(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 648 255**

(21) Número de solicitud: 201630873

(51) Int. CI.:

H04N 1/32 (2006.01)
G06T 1/00 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

28.06.2016

(43) Fecha de publicación de la solicitud:

29.12.2017

(71) Solicitantes:

BANCO SANTANDER, S.A. (100.0%)
Ciudad Grupo Santander Avda. Cantabria, s/n
Edificio Marisma, planta 0
28660 BOADILLA DEL MONTE (Madrid) ES

(72) Inventor/es:

DELGADO ARNAU, Juan Carlos

(74) Agente/Representante:

ZEA CHECA, Bernabé

(54) Título: **Procedimiento, sistema y programa informático para generar y validar un fichero asociado a una transacción electrónica y el fichero generado por dicho procedimiento.**

(57) Resumen:

Procedimiento para generar y validar un fichero asociado a una transacción electrónica, que puede ser un pago o una solicitud de pago, realizándose la transacción de forma segura entre un ordenante y un receptor; el procedimiento puede comprender generar, por parte del ordenante, el fichero asociado a la transacción electrónica incorporando, en un fichero de imagen, una referencia a la transacción electrónica y un criptograma; además el procedimiento también puede comprender recibir, por parte del receptor, el fichero asociado a la transacción electrónica generado; extraer del fichero asociado a la transacción electrónica recibido el fichero de imagen, la referencia a la transacción electrónica y el criptograma; se valida el fichero asociado a la transacción electrónica determinando si el fichero asociado a la transacción electrónica recibido es correcto o incorrecto, en el caso de que sea correcto se puede generar una señal de validación para realizar la transacción.

ES 2 648 255 A1

DESCRIPCIÓN

Procedimiento, sistema y programa informático para generar y validar un fichero asociado a una transacción electrónica y el fichero generado por dicho procedimiento

La presente descripción se refiere a un procedimiento para generar y validar un fichero asociado a una transacción electrónica. Además, se refiere a un sistema y a programa informático adecuados para llevar a cabo el procedimiento.

ESTADO DE LA TÉCNICA ANTERIOR

En la actualidad, el mundo está lleno de personas conectadas en movilidad. Según algunas previsiones, en el año 2020, a nivel mundial, el 90% de las personas mayores de seis años tendrán un teléfono móvil (*Fuente: Ericsson Mobility Report - Junio 2015*).

Por otro lado, claramente el consumo de redes sociales no es una moda pasajera sino que más bien ya se ha convertido en un hábito. De acuerdo con algunas estimaciones, siete de cada diez usuarios de internet móvil se conectan a alguna plataforma social (por ejemplo, *Twitter*, *Facebook*, *Instagram*, *Google+* o *Linkedin*) a través de su dispositivo (por ejemplo, teléfono inteligente o tableta) y el 29% lo hace de forma diaria (*Fuente: sitio web - https://www.territoriocreativo.es/socialholic-introduccion*).

Del mismo modo, el uso de aplicaciones de mensajería instantánea y multimedia por Internet (por ejemplo, *Messenger*, *Whatsapp* o *Telegram*), las cuales pueden formar parte de una red social, ha tenido un crecimiento exponencial. Así, por ejemplo, poniendo como referencia la aplicación *Whatsapp*, se estima que cada día (un día promedio) se comparten 200 millones de notas de voz, 30 mil millones de mensajes (enviados y recibidos) y 700 millones de imágenes (*Fuente: sitio web - http://www.laverdad.com/tecnologia/91360-whatsapp-la-app-de-mensajeria-mas-utilizada-en-el-mundo.html*). Este crecimiento también es aplicable a las aplicaciones cliente de correo electrónico.

A pesar de todo este crecimiento descrito, las transacciones (por ejemplo, pagos o solicitudes de pago) a través de este tipo de aplicaciones (tanto de redes sociales, de mensajería instantánea como de correo electrónico) aún están por explotar.

Existen en el mercado aplicaciones de teléfono móvil o tableta que unen mensajería junto con pagos (por ejemplo, *Pingit*). En algunos casos se utilizan aplicaciones ya extendidas de mensajería para incluir un pago, aunque requieren llegar a un acuerdo de integración con la empresa de mensajería (por ejemplo, *Pingit-Twitter*).

También existe alguna solución que sin llegar a un acuerdo con la red social puede insertar como mensaje de texto un enlace a un pago (por ejemplo, *PayKey*), pero para ello requiere instalarse en el dispositivo móvil un teclado específico que incluye una nueva tecla de pago que dispara el proceso sin salir de la aplicación de la red social. El inconveniente de esta solución está, por un lado, en que requiere cambiar el teclado del teléfono poniendo en compromiso la confianza del cliente sobre la seguridad (*man-in-the-middle*) y, por otro lado, la necesidad de indicar la referencia del beneficiario en el proceso de pago aunque el "chateo" en curso sea con el mismo beneficiario.

En consecuencia, hay una necesidad de un sistema que resuelva al menos parcialmente los problemas mencionados anteriormente.

EXPLICACIÓN DE LA INVENCIÓN

En un primer aspecto, se proporciona un procedimiento para generar un fichero asociado a una transacción electrónica. Este procedimiento puede comprender:

- Recibir datos relativos a la transacción electrónica;
- Obtener una referencia a la transacción electrónica generada a partir de los datos recibidos relativos a la transacción electrónica;
- Recibir un fichero de imagen;
- Generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción electrónica obtenida.

De este modo, con la generación de este fichero asociado a la transacción electrónica, se consigue finalizar esta transacción electrónica (por ejemplo, pagos o solicitudes de pago) a través de, por ejemplo, redes sociales, aplicaciones de mensajería instantánea o correo electrónico de una forma sencilla por presentar compatibilidad natural con la forma de funcionar de estas redes o aplicaciones, dado que no se requiere de ninguna integración

con la red social o la aplicación porque simplemente la usa. Dado que el fichero asociado a la transacción es un fichero de imagen, es posible realizar la transacción mediante el envío de esta imagen entre el emisor de la transacción y el receptor de la misma, es decir, para conseguir el objetivo de realizar una transacción electrónica de forma natural en las redes sociales o a través de las aplicaciones descritas se utiliza la capacidad generalizada de estas de poder compartir imágenes (por ejemplo, fotografías).

En algunos ejemplos, generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción electrónica obtenida puede comprender incorporar, en el fichero de imagen recibido, al menos la referencia a la transacción electrónica obtenida en forma de metadatos de la imagen.

De acuerdo con algunos ejemplos, generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción electrónica obtenida puede comprender incorporar, en el fichero de imagen recibido, al menos la referencia a la transacción electrónica obtenida en forma de código después de la marca de fin de imagen.

Por otro lado, el procedimiento puede comprender:

- Codificar al menos la referencia a la transacción electrónica obtenida;

y en el que generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción electrónica obtenida puede comprender:

- Incorporar, en el fichero de imagen recibido, al menos la referencia a la transacción electrónica codificada.

En algunos ejemplos, codificar al menos la referencia a la transacción electrónica obtenida puede comprender:

- Generar un código representativo de al menos la referencia a la transacción electrónica;

en el que incorporar, en el fichero de imagen recibido, al menos la referencia a la transacción electrónica codificada puede comprender:

- Incorporar, en el fichero de imagen recibido, el código representativo de al menos la referencia a la transacción electrónica de manera visible en la imagen.

Por ejemplo, este código representativo de al menos la referencia a la transacción electrónica puede seleccionarse de entre al menos un código de barras lineal o un código bidimensional, tal como un código de barras bidimensional o un código QR.

En algunos ejemplos, el procedimiento puede comprender:

- Obtener una huella electrónica del fichero de imagen recibido;
- Obtener una huella electrónica del fichero asociado a la transacción electrónica a partir de la huella electrónica obtenida del fichero de imagen recibido, y de la referencia a la transacción electrónica obtenida.

Básicamente, en estos ejemplos, la obtención de la huella electrónica del fichero asociado a la transacción electrónica puede realizarse obteniendo la huella electrónica del fichero de imagen y posteriormente obteniendo la huella electrónica del fichero a partir de la huella electrónica obtenida del fichero de imagen, y de la referencia a la transacción.

Alternativamente, la obtención de la huella electrónica del fichero asociado a la transacción electrónica podría realizarse obteniendo la huella electrónica del fichero de imagen que incorpora la referencia a la transacción.

De acuerdo con algunos ejemplos, el procedimiento puede comprender obtener un criptograma a partir de la huella electrónica obtenida del fichero asociado a la transacción electrónica.

En algunos ejemplos, obtener un criptograma a partir de la huella electrónica obtenida del fichero asociado a la transacción electrónica puede comprender obtener el criptograma mediante el cifrado de la huella electrónica obtenida del fichero asociado a la transacción electrónica. Este cifrado puede realizarse, por ejemplo, con la clave privada asociada al ordenante de la transacción electrónica.

En algunos ejemplos, generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción

electrónica obtenida puede comprender además incorporar, en el fichero de imagen recibido, el criptograma en forma de código después de la marca de fin de imagen, obteniéndose un fichero securizado asociado a la transacción electrónica.

De acuerdo con algunos ejemplos, generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción electrónica obtenida puede comprender además incorporar, en el fichero de imagen recibido, el criptograma en forma de metadatos de la imagen, obteniéndose un fichero securizado asociado a la transacción electrónica.

Por otro lado, codificar al menos la referencia a la transacción electrónica obtenida puede comprender:

- Codificar la referencia a la transacción electrónica obtenida y el criptograma obtenido;

y en el que incorporar, en el fichero de imagen recibido, al menos la referencia a la transacción electrónica codificada puede comprender:

- Incorporar, en el fichero de imagen recibido, la referencia a la transacción electrónica y el criptograma codificados, obteniéndose un fichero securizado asociado a la transacción electrónica.

En algunos ejemplos, codificar la referencia a la transacción electrónica obtenida y el criptograma obtenido puede comprender:

- Generar un código representativo de la referencia a la transacción electrónica y del criptograma;

en el que incorporar, en el fichero de imagen recibido, la referencia a la transacción electrónica y el criptograma codificados puede comprender:

- Incorporar, en el fichero de imagen recibido, el código representativo de la referencia a la transacción electrónica y del criptograma de manera visible en la imagen, obteniéndose un fichero securizado asociado a la transacción electrónica.

Este código representativo de la referencia a la transacción electrónica puede seleccionarse de entre al menos un código de barras lineal o un código bidimensional, tal como un código de barras bidimensional o un código QR.

De este modo, en cualquiera de los casos descritos, el fichero asociado a la transacción electrónica puede comprender o estar formado por el fichero de imagen que incorpora tanto la referencia a la transacción como el criptograma.

Además, la huella electrónica puede comprender un valor de hash criptográfico. Este valor de hash se puede obtener mediante la aplicación de una función hash criptográfica a una versión consistente del fichero asociado a la transacción electrónica. La expresión "versión consistente" se refiere a un formato del fichero que siempre produce el mismo valor hash cuando se aplica la misma función hash criptográfica.

Una función hash criptográfica es un procedimiento determinista que toma un bloque arbitrario de datos y devuelve una cadena de bits de tamaño fijo, el valor hash (de cifrado), de tal manera que un cambio accidental o intencionado en el fichero cambia el valor de hash.

Una función hash que se puede usar es la SHA-256 que pertenece al conjunto de funciones hash criptográficas del estándar SHA-2, aunque se puede utilizar otra función de hash si, por ejemplo, se demuestra en el futuro que SHA-256 no es lo suficientemente segura. La seguridad de una función hash se determina por su resistencia a las colisiones. Así, a pesar de que SHA-256 se utiliza en los presentes ejemplos, podría ser sustituida en el futuro por otra función hash con una mejor resistencia a las colisiones (es decir, más segura), tales como, por ejemplo, SHA-3, que es un nuevo estándar de hash actualmente en desarrollo.

Los datos relativos a la transacción electrónica citados anteriormente pueden seleccionarse de entre al menos uno de las siguientes:

- Datos referentes al concepto de la transacción electrónica;
- Datos referentes a la vigencia de la transacción electrónica;
- Datos referentes al importe de la transacción electrónica;
- Datos referentes al ordenante de la transacción electrónica.

Con referencia al importe, este también puede contemplar el tipo de moneda (euros, dólares, libras, etc.) aunque el tipo de moneda podría considerar como dato relativo a la transacción electrónica de manera independiente.

En algunos ejemplos, la transacción electrónica se selecciona de entre un pago o una solicitud de pago. Adicionalmente, la transacción electrónica también puede referirse, por ejemplo, a una solicitud de colecta (varios receptores del fichero asociado a la transacción pueden hacer un pago), a una solicitud de compra (por ejemplo, seleccionando una imagen de un producto) o a un bono regalo (convenido con un proveedor determinado).

De acuerdo con un segundo aspecto, se proporciona un programa informático. Este programa informático puede comprender instrucciones de programa para provocar que un sistema informático realice un procedimiento para generar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente. Este programa informático puede estar almacenado en unos medios de almacenamiento físico, tales como unos medios de grabación, una memoria de ordenador, o una memoria de solo lectura, o puede ser portado por una onda portadora, tal como eléctrica u óptica.

En un tercer aspecto, se proporciona un sistema para generar un fichero asociado a una transacción electrónica. Este sistema puede comprender:

- Medios para recibir datos relativos a la transacción electrónica;
- Medios para obtener una referencia a la transacción electrónica generada a partir de los datos recibidos relativos a la transacción electrónica;
- Medios para recibir un fichero de imagen;
- Medios para generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción electrónica obtenida.

Básicamente, el sistema para generar un fichero asociado a una transacción electrónica debe ser capaz de reproducir el procedimiento descrito anteriormente, por ejemplo, mediante medios electrónicos y/o informáticos. Dichos medios electrónicos/informáticos se pueden usar indistintamente, es decir, una parte de los medios descritos pueden ser medios electrónicos y la otra parte pueden ser medios informáticos, o todos los medios descritos pueden ser medios electrónicos o todos los medios descritos pueden ser medios informáticos.

Ejemplos de un sistema que comprenden sólo medios electrónicos (es decir, una configuración puramente electrónica) pueden ser un dispositivo electrónico programable tal

como un CPLD (*Complex Programmable Logic Device*), un FPGA (*Field Programmable Gate Array*) o un ASIC (*Application-Specific Integrated Circuit*).

Un ejemplo de un sistema para generar un fichero asociado a una transacción electrónica que comprende medios solamente informáticos puede ser un sistema informático que comprende una memoria y un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, comprendiendo estas instrucciones funcionalidades para ejecutar un procedimiento, tal como el descrito anteriormente, para generar un fichero asociado a una transacción electrónica, es decir, con el fin de generar las diversas acciones y actividades para las que el sistema ha sido programado. Así, por ejemplo, en este caso el sistema puede ser un dispositivo móvil, tal como un teléfono inteligente o una tableta. Este sistema puede ser usado por el ordenante de una transacción electrónica que, por lo tanto, requiere la generación del fichero asociado a la transacción electrónica.

Un sistema para generar un fichero asociado a una transacción electrónica que combine medios electrónicos e informáticos puede comprender un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, comprendiendo estas instrucciones funcionalidades para ejecutar al menos parte de un procedimiento para generar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente. Además, el sistema puede comprende circuitos electrónicos diseñados para ejecutar aquellas partes del procedimiento que no sean implementadas por las instrucciones informáticas.

De acuerdo con otro aspecto, se proporciona un fichero asociado a una transacción electrónica. Este fichero puede comprender:

- Un fichero de imagen;
- Una referencia a la transacción electrónica incorporada en el fichero de imagen.

Además, este fichero puede comprender un criptograma del fichero de imagen que incorpora la referencia a la transacción electrónica, incorporado en el fichero de imagen, así como datos relativos a la transacción electrónica.

En otro aspecto, se proporciona un procedimiento para validar un fichero asociado a una transacción electrónica. Este fichero puede ser generado a partir de un procedimiento para generar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente. Este procedimiento de validación puede comprender:

- Recibir el fichero asociado a la transacción electrónica generado;
- Extraer del fichero asociado a la transacción electrónica recibido al menos el fichero de imagen y la referencia a la transacción electrónica;
- Validar el fichero asociado a la transacción electrónica a partir de al menos el fichero de imagen y la referencia a la transacción electrónica extraídos.

De este modo, cuando el receptor de la transacción electrónica recibe el fichero asociado a la transacción electrónica (es decir, un fichero de imagen que como mínimo incorpora la referencia a la transacción, ya sea por ejemplo como metadatos de la imagen o como código después de la marca de fin de imagen), debe validarlo para que la transacción electrónica se complete. La validación puede depender de los datos contenidos en el fichero de imagen (sólo referencia a la transacción, referencia a la transacción + criptograma, etc.).

En algunos ejemplos, extraer del fichero asociado a la transacción electrónica recibido al menos el fichero de imagen y la referencia a la transacción electrónica puede comprender, cuando el fichero asociado a la transacción electrónica comprende un código visible en la imagen representativo de la referencia a la transacción electrónica:

- Extraer el fichero de imagen;
- Decodificar el código representativo de la referencia a la transacción electrónica visible en la imagen para extraer la referencia a la transacción electrónica.

De acuerdo con algunos ejemplos. el procedimiento de validación puede comprender, cuando el fichero asociado a la transacción electrónica es un fichero securizado que comprende un criptograma:

- Extraer del fichero securizado asociado a la transacción electrónica el criptograma;

en el que validar el fichero asociado a la transacción electrónica a partir de al menos el fichero de imagen y la referencia a la transacción electrónica extraídos comprende:

- Validar el fichero asociado a la transacción electrónica a partir del fichero de imagen, de la referencia a la transacción electrónica y del criptograma extraídos.

Por otro lado, extraer del fichero asociado a la transacción electrónica recibido al menos el fichero de imagen y la referencia a la transacción electrónica puede comprender, cuando el fichero asociado a la transacción electrónica es un fichero securizado que comprende un código visible en la imagen representativo de la referencia a la transacción electrónica y del criptograma:

- Extraer el fichero de imagen;
- Decodificar el código visible en la imagen representativo de la referencia a la transacción electrónica y del criptograma para extraer la referencia a la transacción electrónica y el criptograma;

en el que validar el fichero asociado a la transacción electrónica a partir de al menos el fichero de imagen y la referencia a la transacción electrónica extraídos comprende:

- Validar el fichero asociado a la transacción electrónica a partir del fichero de imagen, de la referencia a la transacción electrónica y del criptograma extraídos.

En algunos ejemplos, el procedimiento de validación puede comprender obtener, a partir del criptograma extraído, una primera huella electrónica.

Además, obtener, a partir del criptograma extraído, una primera huella electrónica puede comprender, cuando el criptograma se obtiene a partir de cifrar la huella electrónica del fichero asociado a la transacción electrónica, descifrar el criptograma extraído. Este descifrado del criptograma puede realizarse a partir de la clave pública del ordenante de la transacción, si es que el cifrado se ha realizado previamente con su clave privada.

De acuerdo con algunos ejemplos, el procedimiento de validación puede comprender además obtener una segunda huella electrónica del fichero asociado a la transacción electrónica a partir del fichero de imagen y de la referencia a la transacción electrónica extraídos.

El procedimiento de validación puede comprender también:

- Obtener una huella electrónica del fichero de imagen extraído;
- Obtener una segunda huella electrónica del fichero asociado a la transacción electrónica a partir de la huella electrónica obtenida del fichero de imagen extraído, y de la referencia a la transacción extraída.

Por otro lado, validar el fichero asociado a la transacción electrónica a partir del fichero de imagen, de la referencia a la transacción electrónica y del criptograma extraídos puede comprender:

- Comparar la primera huella electrónica obtenida del criptograma extraído con la segunda huella electrónica obtenida del fichero asociado a la transacción electrónica;
- Determinar el fichero asociado a la transacción electrónica recibido como correcto, en caso de que la primera huella electrónica y la segunda huella electrónica sean iguales;
- Determinar el fichero asociado a la transacción electrónica recibido como incorrecto, en caso de que la primera huella electrónica y la segunda huella electrónica no sean iguales.

En algunos ejemplos, validar el fichero asociado a la transacción electrónica a partir del fichero de imagen, de la referencia a la transacción electrónica y del criptograma extraídos puede comprender, en caso de determinar el fichero asociado a la transacción electrónica recibido como incorrecto:

- Generar una señal de aviso de fichero asociado a la transacción electrónica incorrecto.

De acuerdo con otro aspecto, se proporciona un programa informático. Este programa informático puede comprender instrucciones de programa para provocar que un sistema informático realice un procedimiento para validar un fichero asociado a una transacción electrónica tal como el descrito anteriormente. Este programa informático puede estar almacenado en unos medios de almacenamiento físico, tales como unos medios de grabación, una memoria de ordenador, o una memoria de solo lectura, o puede ser portado por una onda portadora, tal como eléctrica u óptica.

De acuerdo con aún otro aspecto, se proporciona un sistema para validar un fichero asociado a una transacción electrónica. Este fichero asociado a una transacción electrónica puede ser generado a partir de un sistema para generar un fichero asociado a una transacción electrónica descrito anteriormente. El sistema para validar un fichero asociado a una transacción electrónica puede comprender:

- Medios para recibir el fichero asociado a la transacción electrónica generado;

- Medios para extraer del fichero asociado a la transacción electrónica recibido al menos el fichero de imagen y la referencia a la transacción electrónica;
- Medios para validar el fichero asociado a la transacción electrónica a partir de al menos el fichero de imagen y la referencia a la transacción electrónica extraídos.

Básicamente, el sistema para validar un fichero asociado a una transacción electrónica debe ser capaz de reproducir el procedimiento para validar un fichero asociado a una transacción electrónica descrito anteriormente, por ejemplo, mediante medios electrónicos y/o informáticos. Dichos medios electrónicos/informáticos se pueden usar indistintamente, es decir, una parte de los medios descritos pueden ser medios electrónicos y la otra parte pueden ser medios informáticos, o todos los medios descritos pueden ser medios electrónicos o todos los medios descritos pueden ser medios informáticos.

Ejemplos de un sistema para validar un fichero asociado a una transacción electrónica que comprende sólo medios electrónicos (es decir, una configuración puramente electrónica) pueden ser un dispositivo electrónico programable tal como un CPLD (*Complex Programmable Logic Device*), un FPGA (*Field Programmable Gate Array*) o un ASIC (*Application-Specific Integrated Circuit*).

Un ejemplo de un sistema para validar un fichero asociado a una transacción electrónica que comprende medios solamente informáticos puede ser un sistema informático que comprende una memoria y un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, comprendiendo estas instrucciones funcionalidades para ejecutar un procedimiento, tal como el descrito anteriormente, para validar un fichero asociado a una transacción electrónica, es decir, con el fin de generar las diversas acciones y actividades para las que el sistema ha sido programado. Así, por ejemplo, en este caso el sistema puede ser un dispositivo móvil, tal como un teléfono inteligente o una tableta. Este sistema puede ser usado por el receptor de una transacción electrónica que, por lo tanto, requiere la validación de un fichero asociado a una transacción electrónica.

Un sistema para validar un fichero asociado a una transacción electrónica que combine medios electrónicos e informáticos puede comprender un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador,

comprendiendo estas instrucciones funcionalidades para ejecutar al menos parte de un procedimiento para validar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente. Además, el sistema puede comprender circuitos electrónicos diseñados para ejecutar aquellas partes del procedimiento que no sean implementadas por las instrucciones informáticas.

Según otro aspecto, se proporciona un procedimiento para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica. Esta transacción electrónica puede ser un pago que el ordenante debe realizar al receptor. El procedimiento puede comprender:

- Recibir datos relativos al pago, comprendiendo estos datos al menos el importe del pago a realizar por el ordenante;
- Realizar un cargo en una cuenta del ordenante del pago a partir del importe del pago recibido;
- Abonar el cargo realizado en la cuenta del ordenante en una cuenta intermedia asociada al pago;
- Generar una referencia al pago a partir de datos recibidos relativos al pago y de la cuenta intermedia asociada al pago, siendo esta referencia al pago generada adecuada para generar un fichero asociado al pago de acuerdo con un procedimiento para generar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente;
- Recibir la aceptación del pago por parte del receptor tras la recepción del fichero asociado al pago, a partir de al menos la validación del fichero asociado al pago de acuerdo con un procedimiento para validar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente;
- Traspasar el importe del pago desde la cuenta intermedia a la cuenta del receptor del pago, tras recibir la aceptación del pago por parte del receptor.

En algunos ejemplos, el procedimiento para realizar una transacción electrónica puede comprender:

- Recibir una huella electrónica del fichero de imagen que forma parte del fichero asociado al pago generado;

- Obtener una huella electrónica del fichero asociado al pago a partir de la huella electrónica obtenida del fichero de imagen recibido, y de la referencia al pago generada.

Además, el procedimiento puede comprender obtener un criptograma a partir de la huella electrónica obtenida del fichero asociado al pago.

De acuerdo con algunos ejemplos, obtener un criptograma a partir de la huella electrónica obtenida del fichero asociado al pago puede comprender obtener el criptograma mediante el cifrado de la huella electrónica obtenida del fichero asociado al pago. Este cifrado puede realizarse con una clave privada del ordenante del pago.

En este punto es importante destacar que la validación del fichero asociado al pago puede realizarse automáticamente (por ejemplo, a partir del criptograma) o a partir de la actuación de un usuario.

También es importante destacar que el criptograma obtenido puede ser adecuado para generar un fichero asociado al pago de acuerdo con un procedimiento para generar un fichero asociado a una transacción electrónica (es decir, en este caso un pago), tal como se ha descrito anteriormente.

De acuerdo con algunos ejemplos, el procedimiento para realizar una transacción electrónica puede comprender:

- Obtener una primera huella electrónica a partir del criptograma (este criptograma puede ser obtenido, dependiendo del escenario, por el sistema para generar un fichero asociado a una transacción descrito anteriormente o por el presente sistema);
- Obtener una segunda huella electrónica del fichero asociado al pago;
- Comparar la primera huella electrónica obtenida del criptograma con la segunda huella electrónica obtenida del fichero asociado al pago;
- Determinar el fichero asociado al pago como correcto, en caso de que la primera huella electrónica y la segunda huella electrónica sean iguales;
- Determinar el fichero asociado al pago como incorrecto, en caso de que la primera huella electrónica y la segunda huella electrónica no sean iguales.

En algunos ejemplos, los datos relativos al pago pueden comprender además el número de teléfono móvil del receptor del pago, y el procedimiento puede comprender:

- Enviar un mensaje electrónico al número de teléfono móvil del receptor, comprendiendo este mensaje electrónico al menos una clave OTP;

en el que recibir la aceptación del pago por parte del receptor tras la recepción del fichero asociado al pago puede comprender:

- Recibir la clave OTP.

De este modo, se consigue que el receptor del fichero asociado a la transacción electrónica se autentifique antes de completarse la transacción. Esta medida de seguridad puede ser adecuada, por ejemplo, cuando el importe de la transacción es elevado y se requiere una verificación del receptor del pago.

De acuerdo con otro aspecto, se proporciona un programa informático que comprende instrucciones de programa para provocar que un sistema informático realice un procedimiento para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica, pudiendo ser esta transacción electrónica un pago que el ordenante debe realizar al receptor, tal como uno de los descritos anteriormente. Este programa informático puede estar almacenado en unos medios de almacenamiento físico, tales como unos medios de grabación, una memoria de ordenador, o una memoria de solo lectura, o puede ser portado por una onda portadora, tal como eléctrica u óptica.

De acuerdo con aún otro aspecto, se proporciona un sistema para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica. Esta transacción puede ser un pago que el ordenante debe realizar al receptor. El sistema puede comprender:

- Medios para recibir datos relativos al pago, comprendiendo estos datos al menos el importe del pago a realizar por el ordenante;
- Medios para realizar un cargo en una cuenta del ordenante del pago a partir del importe del pago recibido;
- Medios para abonar el cargo realizado en la cuenta del ordenante en una cuenta intermedia asociada al pago;
- Medios para generar una referencia al pago a partir de datos recibidos relativos al pago y de la cuenta intermedia asociada al pago, siendo esta referencia al pago

generada adecuada para generar un fichero asociado al pago de acuerdo con un procedimiento para generar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente;

- Medios para recibir la aceptación del pago por parte del receptor tras la recepción del fichero asociado al pago, a partir de al menos la validación del fichero asociado al pago de acuerdo con un procedimiento para validar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente;
- Medios para traspasar el importe del pago desde la cuenta intermedia a la cuenta del receptor del pago, tras recibir la aceptación del pago por parte del receptor.

Básicamente, el sistema para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica, pudiendo ser esta transacción un pago que el ordenante debe realizar al receptor, debe ser capaz de reproducir el procedimiento para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica descrito anteriormente, por ejemplo, mediante medios electrónicos y/o informáticos. Dichos medios electrónicos/informáticos se pueden usar indistintamente, es decir, una parte de los medios descritos pueden ser medios electrónicos y la otra parte pueden ser medios informáticos, o todos los medios descritos pueden ser medios electrónicos o todos los medios descritos pueden ser medios informáticos.

Ejemplos de un sistema para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica que comprende sólo medios electrónicos (es decir, una configuración puramente electrónica) pueden ser un dispositivo electrónico programable tal como un CPLD (*Complex Programmable Logic Device*), un FPGA (*Field Programmable Gate Array*) o un ASIC (*Application-Specific Integrated Circuit*).

Un ejemplo de un sistema para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica que comprende medios solamente informáticos puede ser un sistema informático que comprende una memoria y un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, comprendiendo estas instrucciones funcionalidades para ejecutar un procedimiento, tal como el descrito anteriormente, para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica, es decir, con el fin de generar las diversas acciones y actividades para las que el sistema ha sido programado. Así, por ejemplo, en

este caso el sistema puede ser un sistema informático, tal como un ordenador o un conjunto de ordenadores (por ejemplo, un sistema informático tipo servidor).

Un sistema para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica que combine medios electrónicos e informáticos puede comprender un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, comprendiendo estas instrucciones funcionalidades para ejecutar al menos parte de un procedimiento para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica, tal como el descrito anteriormente. Además, el sistema puede comprende circuitos electrónicos diseñados para ejecutar aquellas partes del procedimiento que no sean implementadas por las instrucciones informáticas.

De acuerdo con otro aspecto, se proporciona un procedimiento para realizar una transacción electrónica entre un ordenante y al menos un receptor de la transacción electrónica. Esta transacción electrónica puede ser una solicitud de pago que el ordenante realiza al receptor. El procedimiento puede comprender:

- Recibir datos relativos a la solicitud de pago, comprendiendo estos datos al menos el importe del pago a realizar por el receptor;
- Generar una referencia a la solicitud de pago a partir de datos recibidos relativos al pago y de la cuenta del ordenante, siendo esta referencia al pago generada adecuada para generar un fichero asociado a la solicitud de pago de acuerdo con un procedimiento para generar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente;
- Recibir la aceptación del pago por parte del receptor tras la recepción del fichero asociado a la solicitud de pago, a partir de la validación del fichero asociado a la solicitud de pago de acuerdo con un procedimiento para validar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente;
- Realizar un cargo en una cuenta del receptor a partir del importe del pago recibido, tras recibir la aceptación del pago por parte del receptor;
- Abonar el cargo realizado en la cuenta del ordenante.

De acuerdo con aún otro aspecto, se proporciona un programa informático. Este programa informático puede comprender instrucciones de programa para provocar que un sistema

informático realice un procedimiento para realizar una transacción electrónica entre un ordenante y al menos un receptor de la transacción electrónica, pudiendo ser esta transacción una solicitud de pago que el ordenante realiza al receptor, tal como el descrito anteriormente. Este programa informático puede estar almacenado en unos medios de almacenamiento físico, tales como unos medios de grabación, una memoria de ordenador, o una memoria de solo lectura, o puede ser portado por una onda portadora, tal como eléctrica u óptica.

Según otro aspecto, se proporciona un sistema para realizar una transacción electrónica entre un ordenante y al menos un receptor de la transacción electrónica. Esta transacción electrónica puede ser una solicitud de pago que el ordenante realiza al receptor, El sistema puede comprender:

- Medios para recibir datos relativos a la solicitud de pago, comprendiendo estos datos al menos el importe del pago a realizar por el receptor;
- Medios para generar una referencia a la solicitud de pago a partir de datos recibidos relativos al pago y de la cuenta del ordenante, siendo esta referencia al pago generada adecuada para generar un fichero asociado a la solicitud de pago de acuerdo con un procedimiento para generar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente;
- Medios para recibir la aceptación del pago por parte del receptor tras la recepción del fichero asociado a la solicitud de pago, a partir de la validación del fichero asociado a la solicitud de pago de acuerdo con un procedimiento para validar un fichero asociado a una transacción electrónica, tal como el descrito anteriormente;
- Medios para realizar un cargo en una cuenta del receptor a partir del importe del pago recibido, tras recibir la aceptación del pago por parte del receptor;
- Medios para abonar el cargo realizado en la cuenta del ordenante.

Básicamente, el sistema para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica, pudiendo ser esta transacción una solicitud de pago que el ordenante realiza al receptor, debe ser capaz de reproducir el procedimiento para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica, pudiendo ser esta transacción una solicitud de pago que el ordenante realiza al receptor, descrito anteriormente, por ejemplo, mediante medios electrónicos y/o informáticos. Dichos medios electrónicos/informáticos se pueden usar indistintamente, es

decir, una parte de los medios descritos pueden ser medios electrónicos y la otra parte pueden ser medios informáticos, o todos los medios descritos pueden ser medios electrónicos o todos los medios descritos pueden ser medios informáticos.

Ejemplos de un sistema para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica que comprende sólo medios electrónicos (es decir, una configuración puramente electrónica) pueden ser un dispositivo electrónico programable tal como un CPLD (*Complex Programmable Logic Device*), un FPGA (*Field Programmable Gate Array*) o un ASIC (*Application-Specific Integrated Circuit*).

Un ejemplo de un sistema para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica que comprende medios solamente informáticos puede ser un sistema informático que comprende una memoria y un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, comprendiendo estas instrucciones funcionalidades para ejecutar un procedimiento, tal como el descrito anteriormente, para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica, es decir, con el fin de generar las diversas acciones y actividades para las que el sistema ha sido programado. Así, por ejemplo, en este caso el sistema puede ser un sistema informático, tal como un ordenador o un conjunto de ordenadores (por ejemplo, un sistema informático tipo servidor).

Un sistema para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica que combine medios electrónicos e informáticos puede comprender un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, comprendiendo estas instrucciones funcionalidades para ejecutar al menos parte de un procedimiento para realizar una transacción electrónica entre un ordenante y un receptor de la transacción electrónica, tal como el descrito anteriormente. Además, el sistema puede comprende circuitos electrónicos diseñados para ejecutar aquellas partes del procedimiento que no sean implementadas por las instrucciones informáticas.

Otros objetos, ventajas y características de realizaciones de la invención se pondrán de manifiesto para el experto en la materia a partir de la descripción, o se pueden aprender con la práctica de la invención.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A continuación se describirán realizaciones particulares de la presente invención a título de ejemplo no limitativo, con referencia a los dibujos adjuntos, en los cuales:

La figura 1 muestra un diagrama esquemático del sistema general de acuerdo con algunos ejemplos;
La figura 2 muestra un diagrama de flujos esquemático de un procedimiento para generar un fichero asociado a una transacción electrónica, de acuerdo con otros ejemplos;
La figura 3a muestra un ejemplo de un fichero de imagen asociado a una transacción electrónica;
La figura 3b muestra un segundo ejemplo de un fichero de imagen asociado a una transacción electrónica;
La figura 4 muestra un diagrama de flujos esquemático de un procedimiento para validar un fichero asociado a una transacción electrónica, de acuerdo con algunos ejemplos;
Las figuras 5a a 5h muestran diagramas esquemáticos de diferentes interfaces gráficas de usuario.

EXPOSICIÓN DETALLADA DE MODOS DE REALIZACIÓN

En los presentes ejemplos, la Figura 1 muestra un primer sistema 10 asociado a un primer usuario 10', que es el ordenante de la transacción electrónica; un segundo sistema 11 asociado a un segundo usuario 11', que es el receptor de la transacción ; y un tercer sistema 12 para realizar la transacción electrónica a partir de datos proporcionados tanto por el primer sistema 10 como por el segundo sistema 11 y/o datos que le han sido proporcionados previamente.

Más concretamente, el primer sistema 10 está configurado para generar un fichero asociado a la transacción electrónica iniciada y para, una vez generado el fichero, enviarlo a través de cualquier red social, correo electrónico o cualquier medio que permita el envío de ficheros informáticos en formato de imagen 13 al segundo sistema 11 para su validación. Una vez validado, el tercer sistema 12 se encarga de completar la transacción.

Por otro lado, el segundo sistema 11 está configurado para validar el fichero asociado a la transacción electrónica iniciada por el primer sistema 10, cuya validación provoca que el tercer sistema 12 complete la transacción electrónica. Esta validación puede realizarse de manera automática o puede requerir la intervención de un usuario.

Con respecto al tercer sistema 12, a partir de la información que recibe del primer sistema 10 con respecto a la transacción electrónica iniciada (importe, moneda, etc.) y de la validación del fichero asociado a la transacción por parte del segundo sistema 11, completa finalmente la transacción.

Cualquiera de los tres sistemas descritos 10,11,12 puede tener, por ejemplo, una configuración puramente informática, una configuración puramente electrónica o una configuración informática/electrónica.

Ejemplos de un sistema con una configuración puramente electrónica pueden ser un dispositivo electrónico programable tal como un CPLD (*Complex Programmable Logic Device*), un FPGA (*Field Programmable Gate Array*) o un ASIC (*Application-Specific Integrated Circuit*).

Ejemplos de un sistema puramente informático puede ser un sistema que comprende al menos una memoria y un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, estando destinadas estas instrucciones a ejecutar las correspondientes funcionalidades del sistema (dependen de cada sistema), es decir, con el fin de generar las diversas acciones y actividades para las que el sistema ha sido programado. Así, por ejemplo, el sistema puede ser un ordenador (por ejemplo, un ordenador portátil o un ordenador de sobremesa), un conjunto o red de ordenadores (por ejemplo, un sistema informático tipo servidor), un dispositivo móvil tal como un teléfono inteligente o una tableta, o un dispositivo portable tal como un reloj inteligente.

El programa informático ejecutado por el procesador puede estar almacenado en unos medios de almacenamiento físico (es decir, por ejemplo la memoria descrita anteriormente), tales como unos medios de grabación, una memoria de ordenador, o una memoria de solo lectura, o puede ser portado por una onda portadora, tal como eléctrica u óptica.

El programa informático puede estar en forma de código fuente, de código objeto o en un código intermedio entre código fuente y código objeto, tal como en forma parcialmente compilada, o en cualquier otra forma adecuada para usar en la implementación de los procedimientos descritos.

El medio portador puede ser cualquier entidad o dispositivo capaz de portar el programa.

Por ejemplo, el medio portador puede comprender unos medios de almacenamiento, tal como una *ROM*, por ejemplo, un *CD ROM* o una *ROM* semiconductora, o un medio de grabación magnético, por ejemplo, un disco duro. Además, el medio portador puede ser un medio portador transmisible tal como una señal eléctrica u óptica que puede transmitirse vía cable eléctrico u óptico o mediante radio u otros medios.

Cuando el programa informático está contenido en una señal que puede transmitirse directamente mediante un cable u otro dispositivo o medio, el medio portador puede estar constituido por dicho cable u otro dispositivo o medio.

Alternativamente, el medio portador puede ser un circuito integrado en el que está encapsulado (*embedded*) el programa informático, estando adaptado dicho circuito integrado para realizar o para usarse en la realización de los procedimientos relevantes.

En el caso de un sistema que combine una configuración electrónica/informática, puede comprender un procesador, en el que la memoria almacena instrucciones de programa informático ejecutables por el procesador, estando destinadas estas instrucciones para ejecutar al menos parte de las funcionalidades del sistema. Por otro lado, el sistema comprende circuitos electrónicos diseñados para ejecutar aquellas funcionalidades que no sean implementadas por las instrucciones informáticas.

En los presentes ejemplos, el primer sistema 10 es un teléfono inteligente del que hace uso el ordenante 10’ de la transacción electrónica; el segundo sistema 11 es también un teléfono inteligente usado por el receptor 11’ de la transacción electrónica; mientras que el tercer sistema 12 es un sistema informático del tipo servidor (que puede estar, por ejemplo, en la nube).

En estos ejemplos, la comunicación entre cada uno de los tres sistemas se realiza mediante sistemas de comunicación inalámbrica, basados en tecnología GSM, GPRS, 3G, 4G o tecnología por satélite (por ejemplo, si la comunicación se realiza a través de una red global de comunicación, tal como Internet). Estos sistemas de comunicación inalámbrica también podrían ser de corto alcance, por ejemplo, Bluetooth, NFC, Wifi, IEEE 802.11 o Zigbee.

Dependiendo de la naturaleza de cada uno de los sistemas, alguno o la totalidad de los sistemas de comunicación también pueden ser alámbricos. En este caso, estos sistemas de comunicación podrían estar basados, por ejemplo, en puertos serie, tal como USB, micro USB, mini USB, Firewire o Ethernet.

Dado que en los presentes ejemplos el primer sistema 10 es un teléfono inteligente, el programa informático citado anteriormente es una aplicación (app) que se ejecuta sobre dicho teléfono inteligente. Esta aplicación debe tener como primer objetivo la generación del fichero asociado a la transacción. Para ello, esta aplicación deber ser capaz de ejecutar el siguiente procedimiento para generar el fichero asociado a la transacción electrónica:

- Recibir datos relativos a la transacción electrónica, tales como el importe de transacción, el concepto de la transacción, la vigencia de la transacción (es decir, su fecha de inicio y/o su fecha de expiración) y/o datos relacionados con el ordenante y/o el receptor de la transacción electrónica. Estos datos pueden ser recibidos por la app a través de una interfaz gráfica de usuario mostrada en la pantalla del teléfono inteligente y sobre la que actúa el ordenante de la transacción. Es decir, estos datos pueden ser proporcionados por el ordenante de la transacción, ya sea un única vez cuando se configura la app (por ejemplo, el número de tarjeta de crédito o cuenta bancaria del ordenante 10') o cada vez que se realiza una transacción (por ejemplo, el importe, la fecha de inicio, la fecha de expiración, etc.);
- Obtener una referencia a la transacción electrónica iniciada a partir de al menos los datos recibidos relativos a la transacción electrónica. Esta referencia a la transacción iniciada se genera de forma que permite identificar la transacción iniciada de forma unívoca por ejemplo asignando un número secuencial o un número creciente asociado al instante en que se genera, etc; y así el tercer sistema 12 la puede completar. La referencia puede venir generada por el sistema servidor 12 al iniciarse la transacción a partir de determinados datos relativos a la transacción electrónica proporcionados por el teléfono inteligente 10 del ordenante de la transacción y/o a

partir de datos que previamente ha recibido, tal como se ha descrito en el punto anterior;

- Recibir un fichero de imagen. Este fichero de imagen puede ser siempre el mismo para todas las transacciones o el ordenante 10' puede seleccionar el que desee para que, por ejemplo, esté relacionado con la transacción electrónica. En caso de selección por parte del ordenante, éste puede proporcionar/seleccionar el fichero de imagen a utilizar a partir de una interfaz gráfica de usuario que se le muestra a través de la pantalla del teléfono inteligente 10;
- Generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción electrónica obtenida. De este modo, el fichero generado asociado a la transacción electrónica no es más que un fichero de imagen modificado, pero sigue siendo un fichero de imagen.

Para incorporar la referencia a la transacción en el fichero de imagen, pueden utilizarse diferentes vías. Así, por ejemplo, la referencia a la transacción puede incorporarse en forma de metadatos de la imagen o en forma de código después de la marca de fin de imagen. También es posible codificar la referencia a la transacción (por ejemplo, generando un código representativo de la referencia a la transacción), por ejemplo, en forma de un código de barras lineal o un código bidimensional, tal como un código de barras bidimensional o un código QR, e incorporar en el fichero de imagen este código de manera visible en la imagen. En cualquiera de los casos descritos se consigue incorporar la referencia a la transacción en el fichero de imagen.

Aunque con lo descrito hasta el momento sería suficiente para generar el fichero asociado a la transacción electrónica, con la intención de mejorar la seguridad en el momento de realizar la transacción electrónica (es decir, para securizar el fichero asociado a la transacción), puede ser conveniente incorporar también un criptograma en el fichero de imagen junto con la referencia a la transacción.

Para obtener este criptograma, la app puede seguir diferentes procesos.

Tal como puede verse en la Figura 2, el primer sistema 10 del ordenante 10', por ejemplo una app si se trata de un teléfono inteligente, puede obtener 20 una huella electrónica 21 del

fichero 22 de imagen recibido previamente. Esta huella 21, junto con los datos de la transacción 30, se comunica al tercer sistema 12 para que inicie la transacción y asigne una referencia 25 a la transacción. Posteriormente, el tercer sistema 12 puede obtener 23 una huella electrónica 24 del fichero asociado a la transacción a partir de la huella electrónica 21 del fichero de imagen, y de la referencia 25 a la transacción previamente obtenida. A continuación, esta huella electrónica 24 del fichero asociado a la transacción puede ser cifrada 26 (por ejemplo, a partir de la clave privada del ordenante 10', la cual puede ser asociada al ordenante, por ejemplo, en el momento de su configuración o del registro inicial del ordenante 10' en el primer sistema 10 del ordenante 10' o en el tercer sistema 12, obteniéndose el criptograma 27 descrito.

Alternativamente, la app podría obtener la huella electrónica directamente del fichero asociado a la transacción (es decir, del fichero de imagen que incorpora la referencia a la transacción), para posteriormente ser cifrada mediante, por ejemplo, la clave privada del ordenante 10', obteniéndose el criptograma 27.

Como se comentará más adelante, como el sistema servidor 12 es el que genera la referencia a la transacción, puede ser este sistema servidor 12 (a través de por ejemplo un programa de ordenador configurado para ello) el que obtenga el criptograma 27 citado, para después devolverlo al teléfono inteligente 10 del ordenante 10', para incorporarlo al fichero 22 de imagen y obtener un fichero 29 asociado a la transacción securizado.

En este punto es importante destacar que una huella electrónica puede comprender un valor de hash criptográfico. Este valor de hash se puede obtener mediante la aplicación de una función hash criptográfica a una versión consistente del fichero asociado a la transacción electrónica. La expresión "versión consistente" se refiere a un formato del fichero que siempre produce el mismo valor hash cuando se aplica la misma función de hash criptográfica.

Una función de hash criptográfica es un procedimiento determinista que toma un bloque arbitrario de datos y devuelve una cadena de bits de tamaño fijo, el valor hash (de cifrado), de tal manera que un cambio accidental o intencionado en el fichero cambia el valor de hash.

Una función hash que se puede usar es la SHA-256 que pertenece al conjunto de funciones hash criptográficas del estándar SHA-2, aunque se puede utilizar otra función de hash si, por ejemplo, se demuestra en el futuro que SHA-256 no es lo suficientemente segura. La seguridad de una función hash se determina por su resistencia a las colisiones. Así, a pesar de que SHA-256 se utiliza en los presentes ejemplos, podría ser sustituida en el futuro por otra función hash con una mejor resistencia a las colisiones (es decir, más segura), tales como, por ejemplo, SHA-3, que es un nuevo estándar de hash actualmente en desarrollo.

Sea cual sea el proceso utilizado, una vez obtenido el criptograma 27, éste debe incorporarse 28 en el fichero 22 de imagen, para conseguir un fichero 29 asociado a la transacción securizado. Para ello, el criptograma puede incorporarse en el fichero 22 de imagen, por ejemplo, en forma de código después de la marca de fin de imagen (antes o a continuación de la referencia a la transacción) o en forma de metadatos de la imagen.

Es importante señalar que es posible que tanto la referencia 25 a la transacción como el criptograma 27 se incorporen en el fichero 22 de imagen como metadatos de la imagen. También es posible que ambos se incorporen en el fichero de imagen como código después de la marca de fin de imagen. Pero también es posible que cada uno de ellos se incorpore de manera diferente (la referencia a la transacción como metadatos y el criptograma como código o al revés).

Alternativamente, también es posible codificar la referencia 25 a la transacción junto con el criptograma 27 (por ejemplo, generando un código representativo de la referencia a la transacción junto con el criptograma), por ejemplo, en forma de un código de barras lineal o un código bidimensional, tal como un código de barras bidimensional o un código QR, e incorporar en el fichero 22 de imagen este código de manera visible en la imagen, mediante un proceso reversible, tal como un proceso reversible de inclusión y extracción en una parte de la imagen dada del código representativo, que garantice la integridad tanto de la referencia como de la imagen. Por consiguiente, se incorpora tanto la referencia a la transacción como el criptograma en el fichero de imagen. También es posible codificar únicamente la referencia a la transacción o únicamente el criptograma y utilizar un proceso alternativo (por ejemplo, como metadatos o como código) para el criptograma o para la referencia a la transacción, respectivamente.

Además, la app puede incorporar en el fichero de imagen parte o la totalidad de los datos relativos a la transacción recibidos (por ejemplo, el importe de la transacción, el tipo de moneda y/o el concepto de la transacción) de manera visible en la imagen.

En la Figura 3a se muestra un primer ejemplo de fichero asociado a la transacción electrónica generado, en el que se incorporan datos relativos a la transacción de manera visible en la imagen.

La Figura 3b muestra un segundo ejemplo de fichero parecido al anterior que incorpora además un código QR representativo de la referencia a la transacción y/o del criptograma, tal como se ha descrito anteriormente.

Una vez que el programa informático que se ejecuta sobre el primer sistema 10 del ordenante 10' (por ejemplo una app en un teléfono inteligente) ha obtenido el fichero (ya sea securizado o no) asociado a la transacción electrónica, éste debe estar configurado para enviarlo al receptor de la transacción (más concretamente, en los presentes ejemplos, al teléfono inteligente 11 del receptor 11' de la transacción) para que lo valide a través de su app. En los presentes ejemplos, este envío del fichero asociado a la transacción se realiza a través de un sistema de comunicación inalámbrica, por ejemplo 4G, tal como se ha descrito anteriormente.

Este envío, dado que el fichero asociado a la transacción electrónica no es más que un fichero de imagen, puede realizarse de manera natural a través de cualquier red social o aplicación de mensajería instantánea 13 (por ejemplo, Messenger, Whatsapp, Telegram, etc.) o incluso a través de correo electrónico (por ejemplo, email), a partir de la capacidad de éstas de compartir imágenes. Por lo tanto, no es necesaria la integración o establecer convenios con las diferentes redes sociales o aplicaciones de mensajería; únicamente deben tener la capacidad de compartir imágenes. Más adelante se describirá la interacción entre la app descrita anteriormente que se ejecuta en el teléfono inteligente 10 del ordenante 10' de la transacción y la app de la red social, de mensajería, etc., que también se ejecuta en el teléfono inteligente 10 del ordenante 10' de la transacción.

Sea como sea, cuando el segundo sistema 11 del receptor 11' de la transacción electrónica (por ejemplo, un teléfono inteligente) recibe el fichero asociado a la transacción (securizado

o no, es decir, incorpora o no un criptograma), este fichero puede ser procesado por una app que se ejecuta sobre él, con una funcionalidad destinada a validar el fichero recibido asociado a la transacción.

En este punto es importante señalar que la app para generar el fichero asociado a la transacción y la app para validar el fichero asociado a la transacción pueden ser la misma. Dependiendo de que el usuario del teléfono inteligente sea ordenante o receptor, se utilizará una funcionalidad u otra de la app. También pueden ser app diferentes, una para cada funcionalidad.

Por otro lado, es importante destacar que la validación del fichero está relacionada con el proceso de generación del mismo.

De este modo, si el fichero no ha sido securizado, es decir, no incorpora un criptograma (el fichero asociado a la transacción está formado por un fichero de imagen que incorpora una referencia a la transacción y/o datos relativos a la transacción), la app del teléfono inteligente 11 del receptor 11’ de la transacción únicamente debe mostrar una interfaz gráfica de usuario con un elemento de control configurado para que el receptor 11’ pueda aceptar la transacción. Si el receptor actúa sobre este elemento de control, se genera una señal de control hacia el sistema servidor 12 que dispara la realización de la transacción electrónica.

En otros ejemplos, esta validación puede ser realizada automáticamente por la propia app que se ejecuta sobre el teléfono inteligente 11 del receptor 11’.

En el caso de que el fichero asociado a la transacción esté securizado (es decir, incorpora un criptograma), su validación puede depender de cómo se haya incorporado el criptograma en el fichero de imagen. Básicamente, hay que diferenciar si el criptograma ha sido codificado o no (por ejemplo, mediante un código de barras lineal o un código bidimensional, tal como se ha descrito anteriormente) o si la referencia a la transacción ha sido codificada o no.

En la Figura 4 se muestra un diagrama de flujos de un procedimiento para validar un fichero asociado a una transacción electrónica, en el que ni el criptograma ni la referencia a la

transacción han sido codificados (es decir, se han incorpora al fichero de imagen ya sea como metadatos de imagen o como código después del final de imagen).

Este procedimiento puede comprender:

- Recibir el fichero 40 asociado a la transacción electrónica generado;
- Extraer 41 del fichero 40 asociado a la transacción electrónica recibido el fichero 42 de imagen, la referencia 43 a la transacción electrónica y el criptograma 44;
- Obtener 45 una primera huella electrónica 46 a partir del criptograma 44 extraído (en el caso de que la huella electrónica haya sido cifrada con la clave privada del ordenante 10' de la transacción durante la generación del fichero asociado a la transacción, esta obtención de la primera huella electrónica puede realizarse mediante el descifrado del criptograma con la clave pública del ordenante);
- Obtener 47 una huella electrónica 48 del fichero 42 de imagen extraído;
- Obtener 49 una segunda huella electrónica 50 a partir de la huella electrónica 48 obtenida del fichero 42, y de la referencia 43 a la transacción extraída;
- Comparar 51 la primera huella electrónica 46 obtenida con la segunda huella electrónica 50 obtenida;
- Determinar el fichero asociado a la transacción electrónica recibido como correcto, en caso de que la primera huella electrónica 46 y la segunda huella electrónica 50 sean iguales (sean coincidentes);
- Determinar el fichero 40 asociado a la transacción electrónica recibido como incorrecto, en caso de que la primera huella electrónica y la segunda huella electrónica no sean iguales.

En el caso de la determinación del fichero como correcto, se puede generar automáticamente una señal de validación hacia el sistema servidor 12, para realice la transacción. Alternativamente, en cado de determinación de fichero correcto, la app puede generar una interfaz gráfica de usuario que permita al receptor 11' actuar sobre un elemento de control para validar la transacción. La actuación del receptor sobre este elemento de control puede generar una señal de control (señal de validación) hacia el sistema servidor 12, la cual le autoriza a completar la transacción.

Por otro lado, en caso de determinar el fichero asociado a la transacción electrónica recibido como incorrecto, el procedimiento puede comprender además la generación de una señal de

aviso de fichero asociado a la transacción electrónica incorrecto. Este aviso puede mostrarse a través de la pantalla del teléfono inteligente 11 del receptor 11' de la transacción y/o puede comunicarse también al ordenante 10' a través de su teléfono inteligente 10.

En el caso de que durante la generación del fichero asociado a la transacción el criptograma se haya obtenido en base a una huella digital del fichero de la imagen que incorpora la referencia a la transacción (es decir, el criptograma no se ha obtenido en base a una huella electrónica del fichero de la imagen, y de la referencia a la transacción), la obtención, en el presente procedimiento, de la segunda huella electrónica se realiza mediante la obtención de la huella electrónica del fichero de imagen que incorpora la referencia a la transacción.

En el caso de que la referencia a la transacción se encuentre codificada (por ejemplo, mediante un código de barras lineal o un código bidimensional, tal como se ha descrito anteriormente), para la extracción de dicha referencia a la transacción debe decodificarse el código representativo de la misma, mientras que la huella electrónica del fichero de imagen debe obtenerse con el fichero de imagen original 22, es decir, sin este código (puede realizarse así porque durante la generación del fichero, el código se ha incorporado en el fichero de la imagen mediante un proceso reversible).

Del mismo modo, si el fichero asociado a la transacción incorpora un código que representa tanto la referencia a la transacción como el criptograma, es necesario descodificar este código para extraer tanto la referencia a la transacción como el criptograma, mientras que para obtener la huella electrónica del fichero de imagen es necesario eliminar el código representativo de la referencia a la transacción y del criptograma (recordar que el código se ha incorporado mediante un proceso reversible) de este fichero de imagen.

Es importante destacar que, en determinados casos, alguna las etapas descritas para los diferentes procedimientos (básicamente generación del fichero asociado a la transacción y validación de este fichero) tanto pueden ejecutarse en el primer sistema 10 del ordenante 10' (por ejemplo, un teléfono inteligente) como en el sistema servidor 12, o tanto en el segundo sistema 11 del receptor 11' de la transacción como en el sistema servidor 12, respectivamente.

Así, en el procedimiento de generación del fichero asociado a una transacción electrónica (esté o no la referencia a la transacción y/o el criptograma codificados), la obtención de la huella electrónica del fichero asociado a la transacción puede realizarse tanto en el teléfono inteligente 10 del ordenante 10’ (en este caso el teléfono debe haber recibido previamente la referencia a la transacción) como en el sistema servidor 12. En este último caso, como este sistema servidor 12 es el encargado de generar la referencia a la transacción, ya dispone de ella para generar la huella electrónica del fichero asociado a la transacción. A pesar de ello, sea cual sea el caso, en algún momento el sistema servidor 12 debe proporcionar al teléfono inteligente 10 del ordenante 10’ de la transacción esta referencia a la transacción, para que pueda incorporarla en el fichero de imagen.

En el caso de que el fichero asociado a la transacción comprenda el fichero de imagen que incorpora la referencia a la transacción, la obtención de la huella electrónica de este fichero asociado a la transacción tanto puede realizarse en el teléfono inteligente 10 del ordenante 10’ de la transacción, a través de la app descrita anteriormente, como en el sistema servidor 12, aunque en este caso, es necesario el envío del fichero de imagen que incorpora la referencia a la transacción, al sistema servidor 12.

Básicamente, una buena opción puede ser evitar el envío del fichero al sistema servidor 12 para su procesamiento (obtención de la huella electrónica, etc.), tanto por temas de seguridad de los procesos criptográficos a realizar como por temas de utilización del ancho de banda del sistema de comunicación utilizado.

Lo mismo sucede con la obtención del criptograma, ya que tanto puede realizarse en el teléfono inteligente 10 del ordenante 10’ de la transacción (en este caso la app que se ejecuta sobre el teléfono 12 debe tener acceso a la clave privada del ordenante) como en el sistema servidor 12 (en este caso el sistema servidor es el que debe tener acceso a la clave privada del ordenante de la transacción y debe haber recibido previamente la huella electrónica obtenida del fichero en el teléfono 10 del ordenante 10’).

Con respecto a la validación del fichero asociado a la transacción, la huella del fichero puede obtenerse tanto en el teléfono 11 del receptor 11’ de la transacción como en el sistema servidor 12. En caso de que se realice en el sistema servidor 12, éste debe haber

recibido previamente la referencia a la transacción extraída y la huella electrónica del fichero de imagen, o la huella electrónica del fichero, si este incorpora la referencia a la transacción.

En el caso del descifrado del criptograma, también puede realizarse en el teléfono 11 del receptor 11' de la transacción o en el sistema servidor 12. En cualquiera de los casos es necesario tener acceso a la clave pública del ordenante 10' de la transacción. Si el descifrado se realiza en el sistema servidor, éste previamente debe haber recibido el criptograma extraído en el teléfono 11 del receptor 11'.

Nuevamente en la validación del fichero es deseable evitar el envío del fichero de imagen por temas de seguridad y/o ancho de banda utilizado. A pesar de ello, este envío puede producirse si así se desea.

Por consiguiente, el sistema servidor 12 debe estar configurado para realizar o completar la transacción electrónica. Además debe estar configurado también para ayudar en la generación del fichero asociado a la transacción por parte del teléfono inteligente 10 del ordenante 10' de la transacción. Por ejemplo, este sistema servidor 12 (a través de un programa informático adecuado para ello, en el caso de que se trate de un sistema informático) debe estar configurado para generar la referencia a la transacción, obtener el criptograma, etc. tal como se ha descrito anteriormente.

En este punto es importante destacar que una transacción electrónica básicamente se puede seleccionar de entre, por ejemplo:

- Una orden de pago;
- Una orden de solicitud de pago;
- Una orden de colecta;
- Una orden de compra;
- Un envío de bono regalo.

En el caso de una orden de pago (es decir, el ordenante desea hacer un pago al receptor), el sistema servidor 12 debe ser capaz de:

- Recibir datos relativos al pago, comprendiendo estos datos al menos el importe del pago a realizar por el ordenante. Puede recibir también otros datos relativos al pago, tales como el concepto de la transacción, la fecha de inicio y/o expiración, etc.;

- Realizar un cargo en una cuenta del ordenante del pago (ya sea, por ejemplo, porque dispone de un número de cuenta bancaria o de un número de tarjeta de crédito o débito del ordenante o una referencia de una cuenta de dinero electrónico, etc.) a partir del importe del pago recibido. Esta cuenta del ordenante del pago puede haber sido proporcionada al darse de alta el usuario en el sistema, puede haber sido proporcionada durante la configuración de la app que se ejecuta en el teléfono 10 del ordenante 10' o puede haber sido proporcionada al sistema servidor 12 por parte del teléfono 10 del ordenante 10';
- Abonar el cargo realizado en la cuenta del ordenante en una cuenta intermedia asociada al pago;
- Generar una referencia al pago (referencia a la transacción en general) a partir de datos recibidos relativos al pago y de la cuenta intermedia asociada al pago. Esta referencia al pago puede ser adecuada para generar un fichero asociado al pago de acuerdo con un procedimiento de generación, tal como el descrito anteriormente;
- Recibir la aceptación del pago por parte del receptor 11' (más concretamente, desde su teléfono 11) tras la recepción del fichero asociado al pago, tras su validación de acuerdo con un procedimiento de validación, tal como el descrito anteriormente;
- Traspasar el importe del pago desde la cuenta intermedia a la cuenta del receptor del pago, tras recibir la aceptación del pago por parte del receptor.

En el caso de que, una vez se haya alcanzado la fecha de expiración, no se haya validado de manera manual (por parte del receptor) o automática (por parte de la app) el fichero desde el teléfono 11 del receptor 11' de la transacción, se retrocede la orden, abonando el importe del pago a la cuenta del ordenante.

Por otro lado, en caso de ciertos importes (por ejemplo, para importes elevados), por temas de seguridad, puede realizarse una verificación del receptor antes de realizarse el pago. Para ello, por ejemplo, podría proporcionarse el número de móvil del receptor, para permitir el envío de una clave OTP a través de, por ejemplo, un SMS.

Por consiguiente, el sistema servidor 12 puede comprender una plataforma de pagos (por ejemplo, un servidor *BlockChain*) que permita gestionar cargos y abonos en cuentas bancarias. Adicionalmente, si el cifrado/descifrado descritos anteriormente se realizan en el

sistema servidor 12, también puede comprender un módulo de seguridad (por ejemplo, HSM) que custodie las claves (tanto privadas como públicas) y resuelva la criptografía.

En el caso que este cifrado/descifrado pueda realizarse en el primer sistema 10 del ordenante 10' de la transacción, el módulo de seguridad puede estar comprendido en este primer sistema 10. Del mismo modo, si el cifrado/descifrado se realice en el segundo sistema 11 del receptor 11' de la transacción, el módulo de seguridad puede estar comprendido en este segundo sistema 11. Si este cifrado/descifrado puede realizarse en varios de los sistemas descritos, cada uno de ellos puede comprender el módulo de seguridad.

Si la transacción es una orden de solicitud de pago (es decir, el ordenante requiere al receptor para que le realice un pago), el sistema servidor 12 debe ser capaz de:

- Recibir datos relativos a la solicitud de pago, comprendiendo estos datos al menos el importe del pago a realizar por el receptor;
- Generar una referencia a la solicitud de pago a partir de datos recibidos relativos al pago y de la cuenta del ordenante, siendo esta referencia al pago adecuada para generar el fichero asociado a la solicitud de pago tal como se ha descrito anteriormente;
- Recibir la aceptación del pago por parte del receptor tras la recepción del fichero asociado a la solicitud de pago, a partir de la validación (manual o automática) del fichero asociado a la solicitud de pago, tal como se ha descrito anteriormente;
- Realizar un cargo en una cuenta del receptor a partir del importe del pago recibido, tras recibir la aceptación del pago por parte del receptor;
- Abonar el cargo realizado en la cuenta del ordenante.

Si la transacción es una orden de colecta se puede generar una orden que presente como característica tener asociada una cuenta temporal de recaudación vinculada al ordenante, donde es posible hacer un seguimiento puntual de lo recolectado. En este caso, el fichero asociado a la transacción se puede enviar, por ejemplo, a grupos de redes sociales o a grupos en aplicaciones de mensajería instantánea (o a varios receptores de correo electrónico). Estos a su vez pueden enviar a otros receptores, facilitando así su viralidad. La participación de los receptores de la orden es igual que cuando la transacción es una orden

de solicitud de pago, a excepción de que los receptores, en el caso de colecta, pueden aumentar opcional y voluntariamente el importe del pago mínimo asociado a la orden.

También existe la posibilidad de que la transacción sea una orden de compra. Dado que las empresas poco a poco se van incorporando a las redes sociales, en los ejemplos se contempla la compra de productos. Para ello se parte de un catálogo de productos en imágenes que pueden contener sobreimpreso en la imagen, por ejemplo, el precio y una descripción del producto. El ordenante (en concreto el comprador) puede seleccionar la imagen del producto a comprar, se realiza el pago y se genera un fichero asociado a la compra con la imagen del producto, el cual puede usarse como resguardo de pago de la compra. La comunicación del pedido al receptor puede realizarse de dos formas:

- El ordenante envía al receptor el fichero asociado a la compra del producto a través de una red social, etc. para que el receptor atienda el pedido ya pagado;
- De forma online desde el sistema servidor 12. En este caso no sería necesario enviar el fichero asociado a la compra al receptor, quedando el fichero como justificante de pago. El fichero podría incluir, si fuera necesario, información (en forma de código de barras, QR o incluso información que puede enviarse a través de NFC en el momento de redención del bono) para poder realizar un canje en una tienda presencial.

Por otro lado, la transacción podría tener la forma de un bono regalo. Para ello el ordenante puede seleccionar la imagen de, por ejemplo, un proveedor (Amazon, MediaMarkt, El Corte Inglés, FNAC, etc.) y realizar el pago del mismo modo descrito anteriormente para una orden de pago. Sin embargo, el valor del pago no queda en una cuenta transitoria sino que se abona al proveedor, el cual retorna una referencia que activa el valor del bono regalo en el fichero asociado al bono, de modo que puede ser canjeable por los productos o servicios del proveedor. Así, este fichero de bono regalo puede enviarse a un destinatario como regalo.

En la Figura 5 se muestran posibles ejemplos de interfaces gráficas de usuario generadas tanto por la app que se ejecuta en el teléfono 10 del ordenante 10’ de la transacción como por la app que se ejecuta en el teléfono 11 del receptor 11’ de la misma. Claramente, en caso de que tanto el primer sistema 10 como el segundo sistema 11 no sean dispositivos móviles, estas interfaces podrían ser diferentes ya que, por ejemplo, un ordenador de

sobremesa o un ordenador portátil acostumbra a tener mayor capacidad de procesamiento gráfico y una pantalla con mayores dimensiones.

Así, la Figura 5a muestra una interfaz 150 que muestra el momento en el que un posible ordenante está chateando (por ejemplo, mediante una aplicación de una red social o una aplicación de mensajería instantánea, aunque también podría ser a partir de una aplicación de correo electrónico) con un posible receptor. En un momento del chateo, el ordenante decide enviarle una orden de pago (o podría ser cualquiera de las opciones antes comentadas: orden de solicitud de pago, etc.) al receptor del mismo.

La Figura 5b muestra una interfaz 151 en la que el ordenante selecciona, mediante la actuación sobre el elemento de control adecuado de la interfaz, adjuntar una foto.

La Figura 5c muestra una interfaz 152 en la que el ordenante selecciona, mediante la actuación sobre el elemento de control referenciado como “Mis pagos” (es decir, la app que se ejecuta sobre el teléfono 10 del ordenante 10’, la cual ha sido descrita en detalle anteriormente), selecciona la foto a adjuntar a través de la app y no a través de la cámara del teléfono 10. Como se ha comentado anteriormente, esta foto podría ser siempre la misma y no sería necesaria esta etapa de selección del fichero de imagen.

La Figura 5d muestra una interfaz 153, la cual ya ha sido generada por la app que se ejecuta sobre el teléfono 10 del ordenante. En ella pueden ver varios elementos sobre los que puede actuar el ordenante. Así, puede introducir el importe del pago en el elemento 153a de texto o el tipo de moneda a través del elemento 153b de control. También puede introducir en un segundo elemento 153c de texto el número de móvil del receptor 11, principalmente en casos en los que el importe del pago sea elevado y sea necesaria una verificación del receptor previa al pago. De este modo, es posible el envío de una clave OTP a este número de móvil a través de, por ejemplo, SMS, desde el sistema servidor 12 al teléfono 11 (que corresponde al número de móvil introducido) del receptor, para que antes del pago este receptor pueda introducir esta clave OTP en un elemento de texto correspondiente de la interfaz generada en el teléfono 11 del receptor 11’ del pago, tal como se describirá más adelante. En la interfaz 153 también se muestra un elemento 153d de la forma de pago por defecto, la cual puede configurarse en cualquier momento. Finalmente, con la intención de securizar más el pago, el ordenante puede disponer de una tarjeta de

claves o de una contraseña que puede introducir en el elemento 153e de la interfaz 153. Una vez introducida toda la información solicitada, el ordenante puede aceptar la generación del fichero asociado al pago a partir del elemento 153f de control de tipo botón pulsable.

Como se puede ver en la Figura 5e, con esta aceptación por parte del ordenante y mediante el envío de determinada información al sistema servidor 12 (por ejemplo, el importe del pago, el número de la tarjeta de crédito, el número de la cuenta bancaria, etc.) para obtener la referencia al pago y/o un criptograma, la interfaz 154 muestra el fichero 154a asociado al pago, que no es más que un fichero de imagen que incorpora la referencia a la transacción, el importe en formato visible, el criptograma, etc. Por lo tanto, la app del teléfono 10 del ordenante 10', a partir de información de la que dispone y de información recibida desde el sistema servidor 12, genera el fichero asociado al pago, el cual es enviado al teléfono 11 del receptor 11' a través de una aplicación de una red social, de una aplicación de mensajería instantánea, etc.

Por consiguiente, tal como se muestra en la interfaz 155 de la Figura 5f, el receptor 11' recibe, a través de su teléfono 11, el archivo 154a asociado al pago, previamente generado en el teléfono 10 del ordenante 10'.

En la Figura 5g se muestra una interfaz 156 que se genera en el teléfono 11 del receptor del pago, para que éste pueda seleccionar abrir el fichero recibido con la app referenciada como "Mis pagos" (se muestra un elemento 156a que cuando el receptor actúa sobre él, el fichero asociado al pago se abre mediante la app).

Tal como puede verse en la Figura 5h, a partir de la interfaz 157 mostrada, esta app autentifica el fichero (a partir del criptograma que incorpora) y abona el importe indicado previamente en la cuenta bancaria designada por defecto en la app del receptor 11' del pago. Alternativamente, esta validación del fichero asociado al pago podría realizarse de manera manual por parte del receptor del pago (o de la solicitud de pago).

En caso de una validación automática, lo que realiza la app que se ejecuta sobre el teléfono inteligente 11 del receptor 11' de la transacción, es verificar, entre otras posibles cosas, que el hash del fichero asociado a la transacción y el hash del fichero obtenido a partir del criptograma son iguales. En caso de que no sea así, la app no permite que se complete la

transacción, pudiéndolo mostrar a través de la pantalla tanto del teléfono inteligente 11 del receptor como del teléfono inteligente 10 del ordenante 10' de la transacción.

A pesar de que se han descrito aquí sólo algunas realizaciones y ejemplos particulares de la invención, el experto en la materia comprenderá que son posibles otras realizaciones alternativas y/o usos de la invención, así como modificaciones obvias y elementos equivalentes. Además, la presente invención abarca todas las posibles combinaciones de las realizaciones concretas que se han descrito. Los signos numéricos relativos a los dibujos y colocados entre paréntesis en una reivindicación son solamente para intentar aumentar la comprensión de la reivindicación, y no deben ser interpretados como limitantes del alcance de la protección de la reivindicación. El alcance de la presente invención no debe limitarse a realizaciones concretas, sino que debe ser determinado únicamente por una lectura apropiada de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento para generar y validar un fichero asociado a una transacción electrónica, **caracterizado** por el hecho de que el procedimiento comprende:

- Recibir datos relativos a la transacción electrónica;
- Recibir un fichero de imagen;
- Obtener una huella electrónica del fichero de imagen recibido;
- Obtener una referencia a la transacción electrónica generada a partir de los datos recibidos relativos a la transacción electrónica;
- Generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción electrónica obtenida;
- Obtener una huella electrónica del fichero asociado a la transacción electrónica a partir de la huella electrónica obtenida del fichero de imagen recibido, y de la referencia a la transacción electrónica obtenida;
- Obtener un criptograma a partir de la huella electrónica obtenida del fichero asociado a la transacción electrónica;
- Obtener un fichero securizado asociado a la transacción electrónica mediante la incorporación del criptograma en el fichero asociado a la transacción electrónica;
- Recibir el fichero securizado asociado a la transacción electrónica generado;
- Extraer del fichero securizado asociado a la transacción electrónica recibido al menos el fichero de imagen, la referencia a la transacción electrónica y el criptograma;
- Validar el fichero asociado a la transacción electrónica a partir de al menos el fichero de imagen, la referencia a la transacción electrónica y el criptograma extraídos;
- Obtener, a partir del criptograma extraído, una primera huella electrónica;
- Obtener una huella electrónica del fichero de imagen extraído;
- Obtener una segunda huella electrónica del fichero asociado a la transacción electrónica a partir de la huella electrónica obtenida del fichero de imagen extraído y de la referencia a la transacción extraída;

en el que validar el fichero asociado a la transacción electrónica a partir del fichero de imagen, de la referencia a la transacción electrónica y del criptograma extraídos comprende:

- Comparar la primera huella electrónica obtenida del criptograma extraído con la segunda huella electrónica obtenida del fichero asociado a la transacción electrónica;

- Determinar el fichero asociado a la transacción electrónica recibido como correcto, en caso de que la primera huella electrónica y la segunda huella electrónica sean iguales;
- Determinar el fichero asociado a la transacción electrónica recibido como incorrecto, en caso de que la primera huella electrónica y la segunda huella electrónica no sean iguales.

2. Procedimiento según la reivindicación 1, en el que obtener un fichero securizado asociado a la transacción electrónica mediante la incorporación del criptograma en el fichero asociado a la transacción electrónica obtenido, comprende:

- Incorporar, en el fichero de imagen recibido, al menos la referencia a la transacción electrónica obtenida y el criptograma obtenido en forma de metadatos de la imagen.

3. Procedimiento según la reivindicación 1, en el que obtener un fichero securizado asociado a la transacción electrónica mediante la incorporación del criptograma en el fichero asociado a la transacción electrónica, comprende:

- Incorporar, en el fichero de imagen recibido, al menos la referencia a la transacción electrónica obtenida y el criptograma obtenido en forma de código después de la marca de fin de imagen.

4. Procedimiento según la reivindicación 1, que comprende además:

- Codificar al menos la referencia a la transacción electrónica y el criptograma obtenidos;

y en el que obtener un fichero securizado asociado a la transacción electrónica mediante la incorporación del criptograma en el fichero asociado a la transacción electrónica comprende:

- Incorporar, en el fichero de imagen recibido, al menos la referencia a la transacción electrónica y el criptograma codificados.

5. Procedimiento según la reivindicación 4, en el que codificar al menos la referencia a la transacción electrónica obtenida y el criptograma obtenido comprende:

- Generar un código representativo de al menos la referencia a la transacción electrónica y el criptograma obtenido;

en el que incorporar, en el fichero de imagen recibido, al menos la referencia a la transacción electrónica y el criptograma codificados comprende:

- Incorporar, en el fichero de imagen recibido, el código representativo de al menos la referencia a la transacción electrónica y del criptograma de manera visible en la imagen.

6. Procedimiento según la reivindicación 5, en el que el código representativo de al menos la referencia a la transacción electrónica y el criptograma se selecciona de entre los siguientes:

- Un código de barras lineal;
- Un código bidimensional, tal como un código de barras bidimensional o un código QR.

7. Procedimiento según la reivindicación 1, en el que obtener un criptograma a partir de la huella electrónica obtenida del fichero asociado a la transacción electrónica comprende:

- Obtener el criptograma mediante el cifrado de la huella electrónica obtenida del fichero asociado a la transacción electrónica.

8. Procedimiento según la reivindicación 1, en el que la huella electrónica comprende un valor de hash criptográfico.

9. Procedimiento según una cualquiera de las reivindicaciones 1 a 8, en el que generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción electrónica obtenida comprende además:

- Incorporar, en el fichero de imagen recibido, datos recibidos relativos a la transacción electrónica de manera visible en la imagen.

10. Procedimiento según una cualquiera de las reivindicaciones 1 a 9, en el que los datos relativos a la transacción electrónica se seleccionan de entre al menos uno de las siguientes:

- Datos referentes al concepto de la transacción electrónica;
- Datos referentes a la vigencia de la transacción electrónica;
- Datos referentes al importe de la transacción electrónica;
- Datos referentes al ordenante de la transacción electrónica.

11. Procedimiento según una cualquiera de las reivindicaciones 1 a 10, en el que la transacción electrónica se selecciona de entre un pago o una solicitud de pago.

12. Procedimiento según una cualquiera de las reivindicaciones 5 a 11, en el que extraer del fichero asociado a la transacción electrónica recibido al menos el fichero de imagen y la referencia a la transacción electrónica comprende, cuando el fichero asociado a la transacción electrónica es un fichero securizado que comprende un código visible en la imagen representativo de la referencia a la transacción electrónica y del criptograma:

- Extraer el fichero de imagen;

Decodificar el código visible en la imagen representativo de la referencia a la transacción electrónica y del criptograma para extraer la referencia a la transacción electrónica y el criptograma.

13. Procedimiento según la reivindicación 1, en el que obtener, a partir del criptograma extraído, una primera huella electrónica comprende, cuando el criptograma se obtiene a partir de cifrar la huella electrónica del fichero asociado a la transacción electrónica:

- Descifrar el criptograma extraído.

14. Procedimiento según la reivindicación 1, en el que validar el fichero asociado a la transacción electrónica a partir del fichero de imagen, de la referencia a la transacción electrónica y del criptograma extraídos comprende, en caso de determinar el fichero asociado a la transacción electrónica recibido como incorrecto:

- Generar una señal de aviso de fichero asociado a la transacción electrónica incorrecto.

15. Programa informático que comprende instrucciones de programa para provocar que un sistema informático realice un procedimiento según una cualquiera de las reivindicaciones 1 a 14 para generar y validar un fichero asociado a una transacción electrónica.

16. Programa informático según la reivindicación 15, que está almacenado en unos medios de grabación.

17. Programa informático según una cualquiera de las reivindicaciones 15 o 16, que es portado por una señal portadora.

18. Sistema para generar y validar un fichero asociado a una transacción electrónica, **caracterizado** por el hecho de que el sistema comprende:

- Medios para recibir datos relativos a la transacción electrónica;
- Medios para recibir un fichero de imagen;
- Medios para obtener una huella electrónica del fichero de imagen recibido;
- Medios para obtener una referencia a la transacción electrónica generada a partir de los datos recibidos relativos a la transacción electrónica;
- Medios para generar el fichero asociado a la transacción electrónica a partir de la incorporación, en el fichero de imagen recibido, de al menos la referencia a la transacción electrónica obtenida;
- Medios para obtener una huella electrónica del fichero asociado a la transacción electrónica a partir de la huella electrónica obtenida del fichero de imagen recibido, y de la referencia a la transacción electrónica obtenida;
- Medios para obtener un criptograma a partir de la huella electrónica obtenida del fichero asociado a la transacción electrónica;
- Medios para obtener un fichero securizado asociado a la transacción electrónica mediante la incorporación del criptograma en el fichero asociado a la transacción electrónica;
- Medios para recibir el fichero securizado asociado a la transacción electrónica generado;
- Medios para extraer del fichero securizado asociado a la transacción electrónica recibido al menos el fichero de imagen, la referencia a la transacción electrónica y el criptograma;
- Medios para validar el fichero asociado a la transacción electrónica a partir de al menos el fichero de imagen, la referencia a la transacción electrónica y el criptograma extraídos;
- Medios para obtener, a partir del criptograma extraído, una primera huella electrónica;
- Medios para obtener una huella electrónica del fichero de imagen extraído;
- Medios para obtener una segunda huella electrónica del fichero asociado a la transacción electrónica a partir de la huella electrónica obtenida del fichero de imagen extraído y de la referencia a la transacción extraída;

- Medios para comparar la primera huella electrónica obtenida del criptograma extraído con la segunda huella electrónica obtenida del fichero asociado a la transacción electrónica;
- Medios para determinar el fichero asociado a la transacción electrónica recibido como correcto, en caso de que la primera huella electrónica y la segunda huella electrónica sean iguales;
- Medios para determinar el fichero asociado a la transacción electrónica recibido como incorrecto, en caso de que la primera huella electrónica y la segunda huella electrónica no sean iguales.

19. Fichero asociado a una transacción electrónica generado mediante un procedimiento para generar y validar según una cualquiera de las reivindicaciones 1-14, **caracterizado** por el hecho de que comprende:

- Un fichero de imagen;
- Una referencia a la transacción electrónica incorporada en el fichero de imagen.
- Un criptograma del fichero de imagen que incorpora la referencia a la transacción electrónica, incorporado en el fichero de imagen.

20. Fichero según la reivindicación 19, que comprende además:

- Datos relativos a la transacción electrónica.

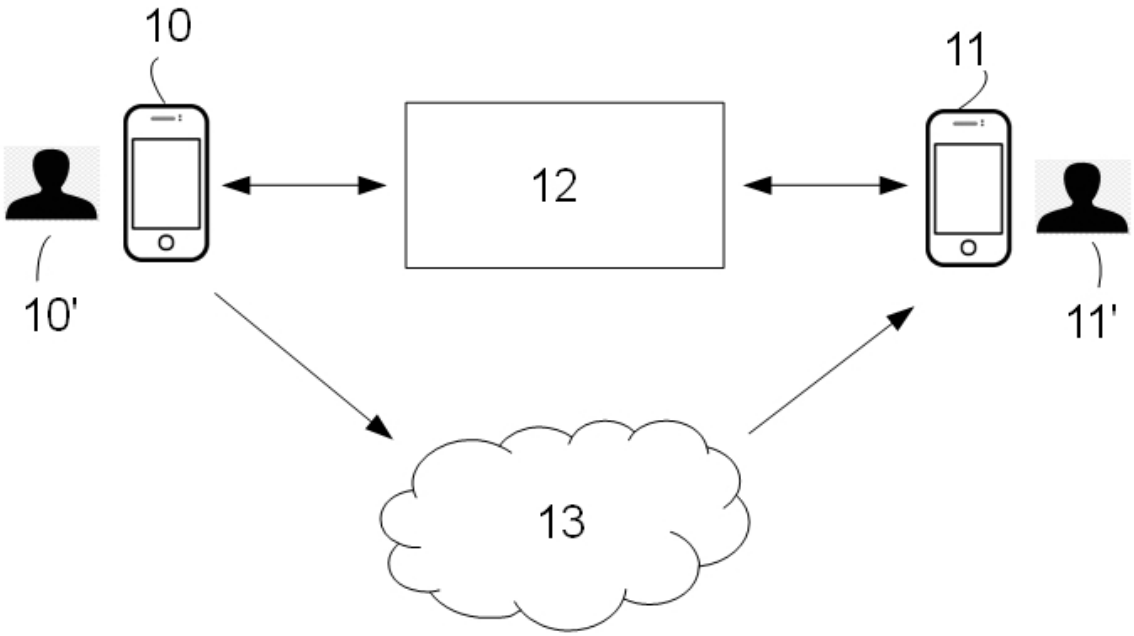

Fig. 1

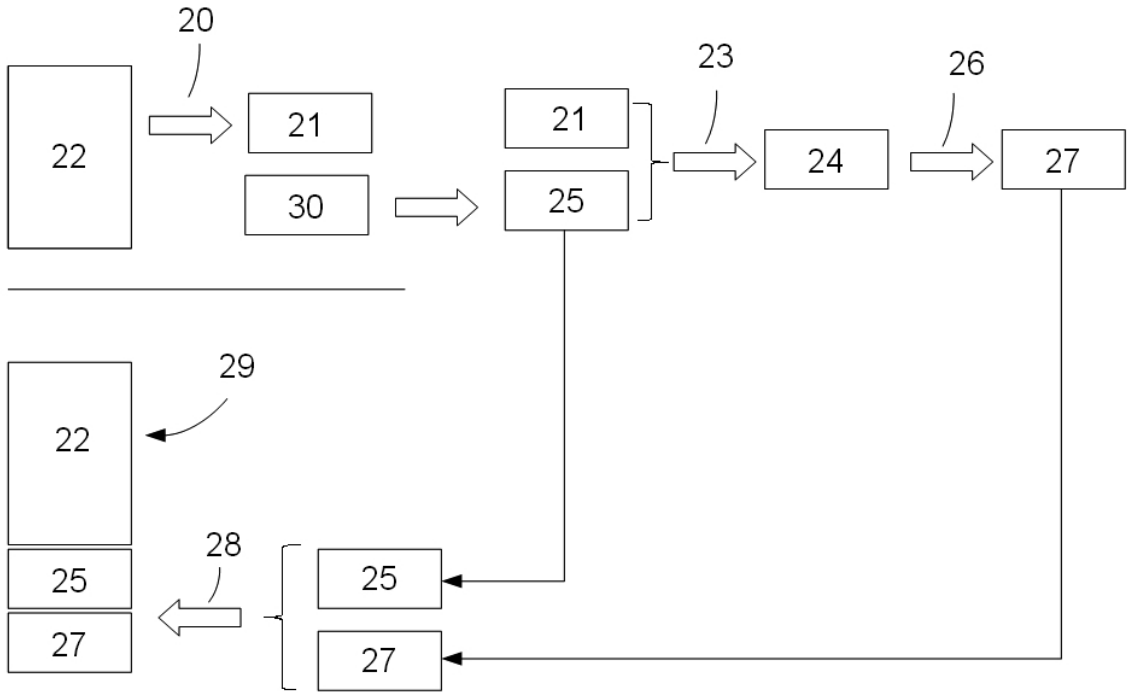

FIG. 2

FIG. 3a

FIG. 3b

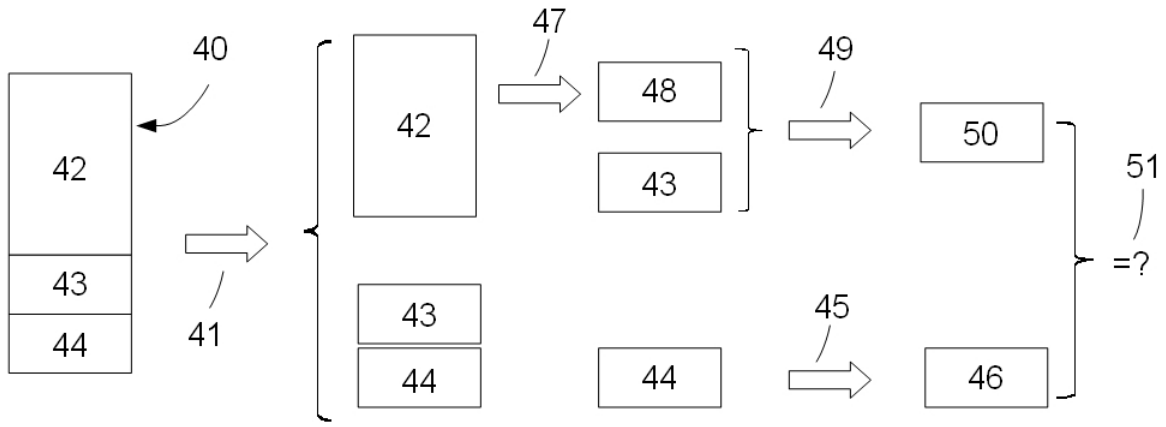

FIG. 4

Fig. 5a


151
55%
06:39 PM
Galería
Foto
Vídeo
Audio
Ubicación
Contacto
Escribir mensaje

Fig. 5b


152
Seleccionar una acción
Cámara
Mis pagos
Escribir mensaje

Fig. 5c

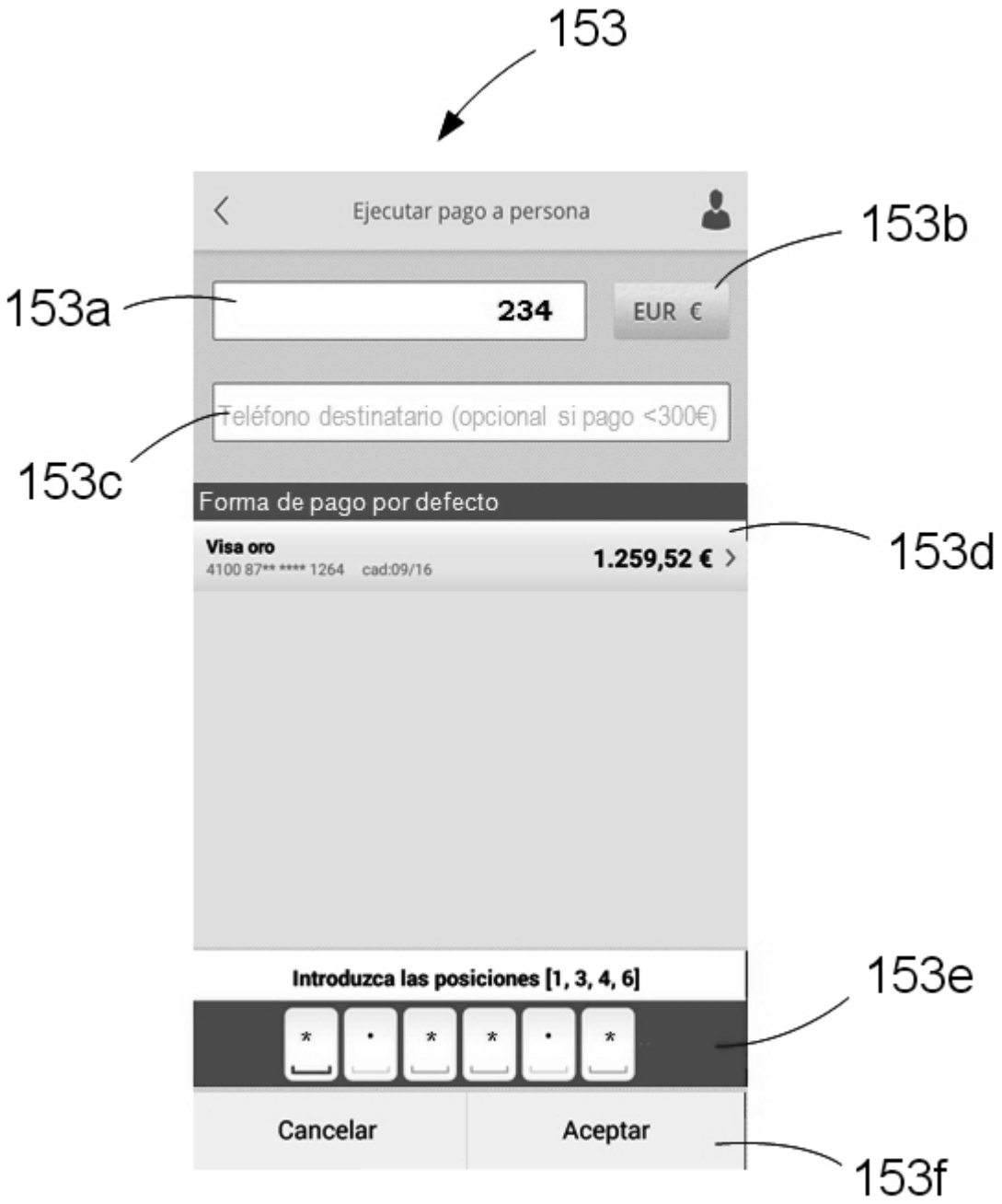
153
Ejecutar pago a persona
153b
153a
234
EUR €
Teléfono destinatario (opcional si pago <300€)
153c
Forma de pago por defecto
Visa oro
4100 87** **** 1264 cad:09/16
1.259,52 €
153d
Introduzca las posiciones [1, 3, 4, 6]
153e
Cancelar
Aceptar
153f

Fig. 5d

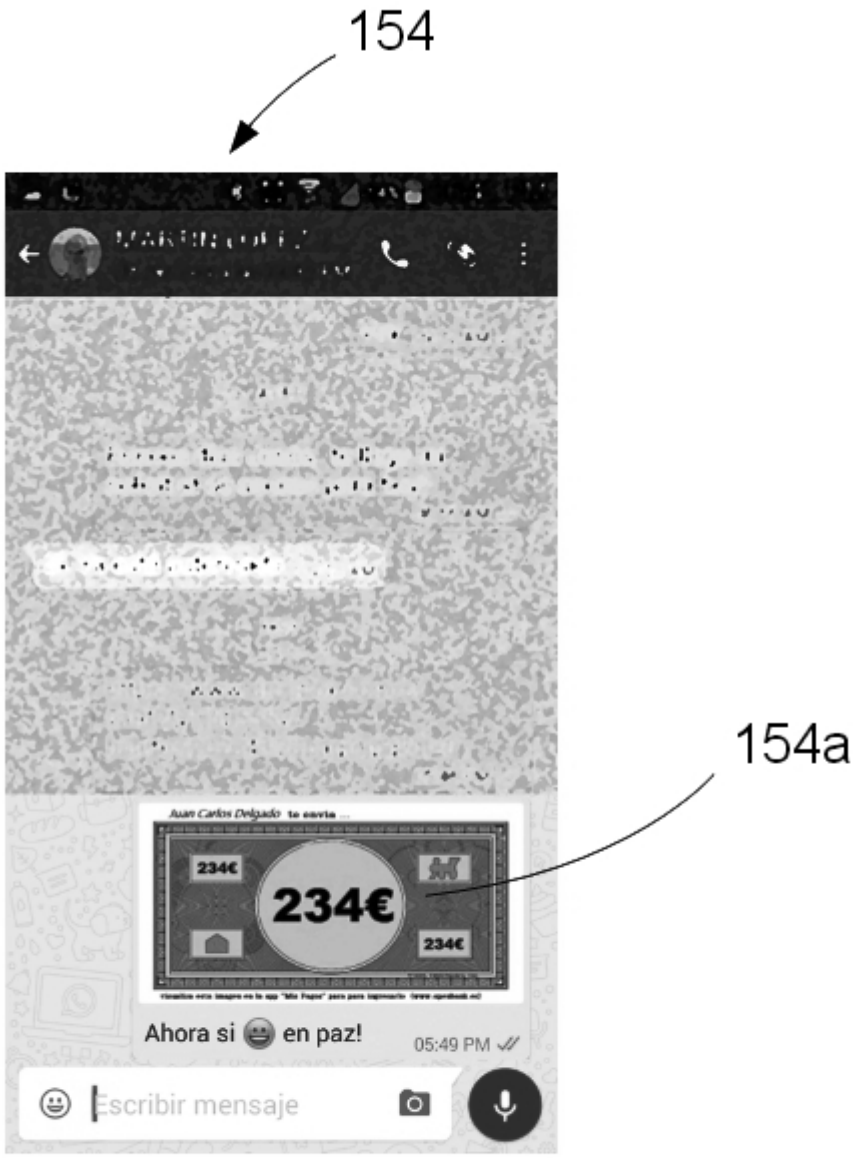

Fig. 5e

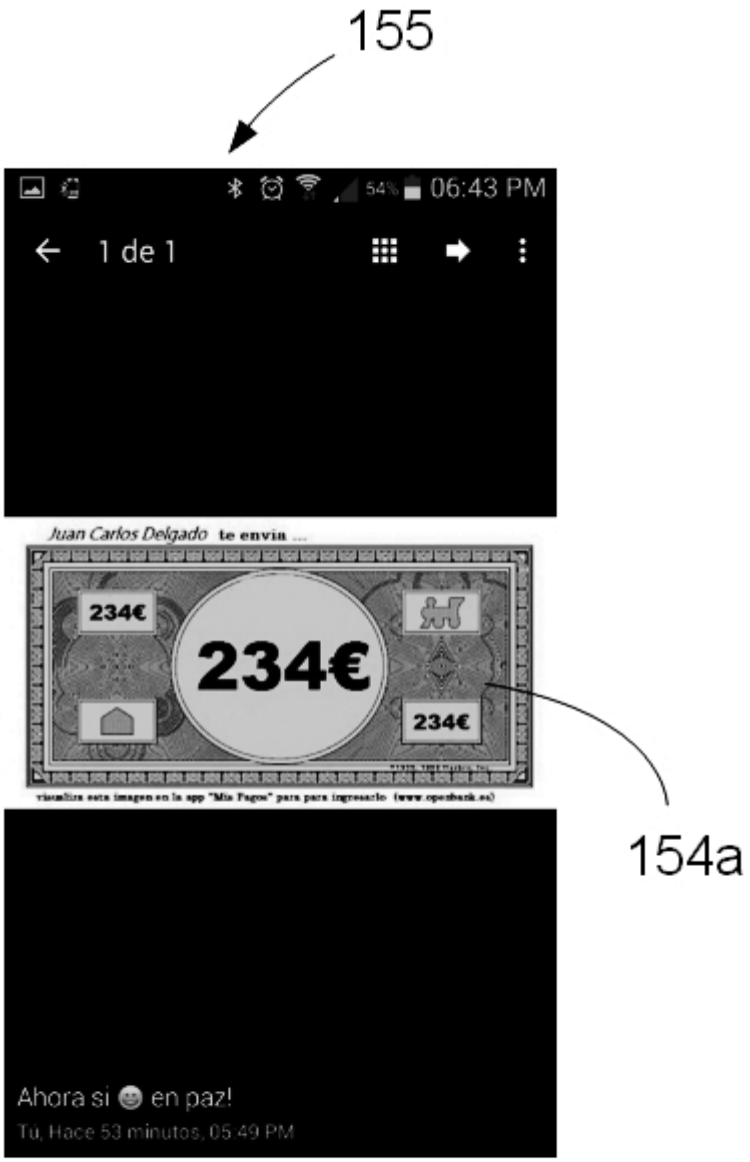
155
06:43 PM
1 de 1
Juan Carlos Delgado te envia ...
234€
234€
234€
visualiza esta imagen en la app "Mis Pagos" para para ingresarlo (www.openbank.es)
Ahora si en paz!
Tú, Hace 53 minutos, 05:49 PM
154a

Fig. 5f


156
06:43 PM
Seleccionar una acción
Add to Yammer
Mis pagos
156a
Añadir a Dropbox
Bluetooth
Compartir como código QR
Copiar a
Correo electrónico
Decodificar código QR

Fig. 5g


157
Registro
CLAVE DE ACCESO A SUPERNET (8 dígitos)
Registro realizado correctamente
Ahora puede acceder a realizar operaciones con la aplicación
Aceptar
DNI
514787889 H
Dirección
Pintor Miguel Angel 26
Aceptar

Fig. 5h

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201630873

(22) Fecha de presentación de la solicitud: 28.06.2016

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04N1/32*** (2006.01)
G06T1/00 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	US 7216232 B1 (COX INGEMAR J et al.) 08/05/2007, resumen; columna 1, líneas 8 - 12; columna 1, líneas 54 - 65; columna 5, línea 32 - columna 6, línea 9; columna 6, líneas 32 - 56; columna 8, líneas 6 - 29; columna 10, líneas 51 - 53; figuras 2A -2B.	1-3, 7-8, 10-11, 13-20
Y		4-6, 9, 12
Y	US 2005067487 A1 (BRUNDAGE TRENT J et al.) 31/03/2005, párrafo [0008]; párrafos [0019-0023] párrafo [0027]; párrafos [0033 - 0039];	4-6, 9, 12

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	**Examinador**	**Página**
26.10.2017	M. L. Alvarez Moreno	1/6

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

H04N, G06T, G06Q

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: 26.10.2017

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-20	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-20	**NO**

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 7216232 B1 (COX INGEMAR J et al.)	08.05.2007
D02	US 2005067487 A1 (BRUNDAGE TRENT J et al.)	31.03.2005

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 1

D01 (columna 1, líneas 8-12) divulga un procedimiento para generar y validar un fichero de imagen, permite insertar y autenticar firmas digitales y datos asociados en una imagen digital.

D01 (resumen; columna 5, línea 32 - 58; figura 2A) ejecuta las siguientes acciones para generar un fichero de imagen.
- Se reciben datos digitales que definen una imagen (fichero de imagen)
- Se obtiene una primera huella electrónica del fichero de imagen.
- Se obtiene un criptograma a partir de la huella electrónica anterior
- Se obtiene un fichero securizado mediante la incorporación del criptograma en el fichero de imagen

D01 (resumen, columna 5, línea 59 - columna 6, línea 9; figura 2B) ejecuta las siguientes acciones para validar el fichero anterior:
- Se recibe el fichero securizado generado (datos digitales de imagen firmados y cifrados);
- Se extraen del fichero el fichero recibido los datos digitales (imagen) y el criptograma;
- Se valida el fichero a partir de al menos los datos digitales y el criptograma extraídos;
- Se obtiene, a partir del criptograma extraído, una primera huella electrónica;
- Se obtiene una huella electrónica de los datos digitales (imagen) extraídos;
- Se valida el fichero (autentican los datos) comparando ambas huellas electrónicas, siendo correcto si son iguales e incorrecto si no son iguales.

El documento D01 (columna 6, líneas 32-56; columna 8, líneas 6-29) muestra la posibilidad de incorporar información adicional a la imagen. Dicha información puede incorporarse tanto antes de la generación de la huella electrónica de la imagen como posteriormente a dicha generación. En este último caso, el procedimiento incorpora la generación de una segunda huella electrónica sobre la base de la primera huella electrónica y los nuevos datos a incorporar (p.ej., marca de tiempo en D01). En este caso, el cifrado se aplicaría sobre esta segunda huella electrónica. Esta nueva información (p.ej., marca de tiempo) es incorporada, junto con el criptograma, en los datos de imagen. D01 también indica que es decisión del diseñador la forma de adjuntar la información adicional en la imagen, parte puede estar cifrada y parte no. Aunque D01 no detalla el procedimiento de validación en el caso de cifrar esta segunda huella electrónica, es evidente que la comparación de la información obtenida del criptograma debe realizarse con la información recibida y que se tomó como base para el cifrado. La huella electrónica obtenida del criptograma recibido se debe comparar con la huella electrónica generada sobre la huella electrónica de la imagen recibida y los datos adicionales.

D01 usa una marca de tiempo como ejemplo particular de datos adicionales a incorporar. La reivindicación 1 cita la utilización de datos referidos a una transacción financiera. La selección del tipo de información que se desea asociar a la imagen se considera una decisión de diseño que no contribuye a la superación de ningún problema técnico.

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

Reivindicaciones dependientes 2 y 3

D01 (columna 1, líneas 54-58) muestra que una solución obvia para adjuntar la información deseada puede ser su concatenación en la cabecera del formato de imagen (lo que afecta a su capacidad de conversión entre formatos). También muestra (columna 1, líneas 59-65) que existen fórmulas para insertar esta información dentro de la imagen misma, de forma que no se necesite ningún tipo de metadatos. D01 ya muestra que es conocida la incorporación de la información deseada en forma de metadatos o en ubicaciones específicas de los archivos de imagen.

Las reivindicaciones 2 y 3 no definen características particulares de dicha incorporación que puedan contribuir a solucionar un problema técnico específico. Las reivindicaciones 2 y 3 no cumplen el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

Reivindicaciones dependientes 4 a 6

D01 (columna 8, líneas 6-29) muestra que se codifica la información que se desea incorporar en la imagen. D01 no muestra de forma expresa que una de las posibilidades de codificación consista en generar un código que sea posteriormente incorporado en forma visible en la imagen en forma de código de barras o código bidimensional.

D02 proporciona este tipo de alternativa. D02 (párrafos 0008; 0019-0023; 0027) muestra que se dispone de información que desea asociar a un objeto. Se transforma dicha información en una referencia en formato apropiado para ser incorporado como marca de agua, y se incorpora en el objeto (p.ej., imagen digital) por cualquiera de los mecanismos ya conocidos. D02 (párrafos 0033-0039) muestra que es ampliamente conocida la utilización de códigos de barras y de códigos bidimensionales como formas de codificar una cantidad de información relativamente pequeña. D02 incluso muestra la posibilidad de utilizar simultáneamente ambos métodos (marca de agua y códigos de barras visibles) para incorporar el tipo de información deseada en el objeto (imagen).

Las reivindicaciones 4 a 6 no cumplen el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

Reivindicaciones dependientes 7 y 8

D01 (columna 5, líneas 46-54) ya muestra que el criptograma se obtiene a partir de la huella electrónica de los datos deseados, comprendiendo dicha huella electrónica valor hash criptográfico.

Las reivindicaciones 7 y 8 no cumplen el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

Reivindicación dependiente 9

Como se ha indicado al analizar las reivindicaciones 4 a 6, D02 divulga la incorporación de información en forma visible en la imagen.

La reivindicación 9 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

Reivindicaciones dependientes 10 a 11

Anteriormente ya se ha indicado que la selección del tipo de información que se desea asociar a la imagen se considera una decisión de diseño que no contribuye a la superación de ningún problema técnico.

Las reivindicaciones 10 a 11 no cumplen el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

Reivindicación dependiente 12

Al analizar las reivindicaciones 4 a 6 ya se ha mostrado que D02 divulga la incorporación de información codificada en forma visible en la imagen. Ello implica la existencia de una decodificación de la información contenida en el código visible para proceder a su procesamiento.

La reivindicación 12 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

Reivindicación dependiente 13

D01 (columna 5, líneas 64-65) ya divulga que la obtención de la huella electrónica a partir del criptograma extraído se realiza mediante el descifrado del mismo.

La reivindicación 13 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

Reivindicación dependiente 14

De la lectura de D01 (columna 10, líneas 51-53) se deduce la generación de un aviso al usuario sobre el resultado del análisis del fichero recibido. La reivindicación 14 no define características particulares de dicha generación de señal de aviso que puedan contribuir a conferir actividad inventiva.

La reivindicación 14 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

Reivindicaciones independiente 15 y dependientes 16 a 17

Por referirse a un programa que contienen instrucciones para realizar un procedimiento según cualquiera de las reivindicaciones 1 a 14, se aplican las mismas consideraciones indicadas anteriormente en la reivindicación 1.

Las reivindicaciones 15 a 17 no cumplen el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

Reivindicación independiente 18

Al estar definida por disponer de los medios para efectuar las mismas acciones del procedimiento de la reivindicación 1, se aplican las mismas consideraciones indicadas en la reivindicación 1.

La reivindicación 18 no cumple el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.

Reivindicaciones independiente 19 y dependiente 20

D01, tal y como se muestra en la argumentación realizada para la reivindicación 1, divulga un fichero (datos digitales) que comprende datos de imagen, datos adicionales incorporados en la imagen y un criptograma asociado incorporado en la imagen. Aunque no se cita de forma expresa que los datos adicionales se correspondan con una transacción electrónica financiera, ya se indicó anteriormente que la selección del tipo de información que se desea asociar a la imagen se considera una decisión de diseño que no contribuye a la superación de ningún problema técnico.

Las reivindicación 19 y 20 no cumplen el requisito de actividad inventiva según el artículo 8 de la Ley de Patentes.