(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 909 968**

(51) Int. CI.:

G06Q 20/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.10.2008 E 08290978 (9)**

(97) Fecha y número de publicación de la concesión europea: **30.03.2022 EP 2053553**

(54) Título: **Procedimiento y dispositivo para el intercambio de valores entre entidades electrónicas portátiles personales**

(30) Prioridad:

22.10.2007 FR 0758477

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.05.2022

(73) Titular/es:

IDEMIA FRANCE (100.0%)
2 Place Samuel de Champlain
92400 Courbevoie, FR

(72) Inventor/es:

DELOLME, PIERRICK y
BERTIN, MARC

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Procedimiento y dispositivo para el intercambio de valores entre entidades electrónicas portátiles personales

La presente invención se refiere al intercambio de importes en valores, por ejemplo, de valores monetarios, de puntos de fidelidad, de bonos de compra o de suscripción, y, más particularmente, a un procedimiento y a un dispositivo para intercambiar importes en valores entre entidades electrónicas portátiles, por ejemplo, entre teléfonos móviles.

La evolución de las redes de comunicación, concretamente, Internet, ha contribuido al desarrollo de nuevos modos de distribución de bienes y de servicios, que han conllevado, por su parte, la puesta en práctica de nuevos medios de pago. Por ejemplo, el pago a través de una red de comunicación, también denominado pago en línea, permite a un usuario, tras haber pedido un artículo o un servicio, proporcionar informaciones bancarias, un importe y una autorización a un tercero de confianza, con el fin de que éste transmita una petición de transacción ante el sistema informático del establecimiento bancario en cuestión.

No obstante, aunque los medios de pago entre varias sociedades, o entre individuos y sociedades, son el origen de numerosos desarrollos, pocos sistemas permiten un intercambio de importes en valores, sencillo y protegido, entre varios individuos.

Por un lado, existen monederos electrónicos que permiten que un deudor pague una suma monetaria a un acreedor, estando el deudor y el acreedor físicamente cerca uno de otro en el momento de la transacción. Según estos sistemas, una tarjeta de pago puede memorizar un número que representa un importe monetario. En esta tarjeta puede realizarse un abono, o recargarse, con la ayuda de un dispositivo adaptado. Se realiza un cargo en la misma durante cada pago. Este modo de pago, generalmente, no pone en práctica mecanismos de verificación del consentimiento del titular de la tarjeta mediante su autenticación, se trata, con frecuencia, de un modo de pago anónimo, como un pago en efectivo. No obstante, un medio de pago de este tipo sólo puede usarse para pequeñas transacciones. Por otro lado, el acreedor debe disponer de un dispositivo adaptado a la lectura de la tarjeta, por contacto o sin contacto, para recibir el dinero.

Por otro lado, existen sistemas, tales como el sistema presentado en la solicitud de patente WO 03/023574, que permiten que un deudor pague una suma monetaria a un acreedor, no estando necesariamente el deudor y el acreedor en proximidad uno del otro en el momento de la transacción. Según estos sistemas, puede realizarse una transferencia monetaria entre dos individuos dotados de entidades electrónicas tales como teléfonos móviles. Las transacciones se realizan en este caso por medio de un sistema central en el que están memorizados los perfiles de los usuarios. Tales perfiles permiten memorizar las informaciones bancarias de los usuarios y realizar los controles necesarios. No obstante, una solución de este tipo impone la introducción de la identidad del acreedor, lo cual puede resultar molesto.

La solicitud de patente US-2007/0123215 describe el uso de funcionalidades de redes personales inalámbricas (WPAN) y de tecnologías de identificación inalámbricas en servidores, para mejorar la seguridad de comunicación inalámbrica de datos y permitir la puesta en práctica de nuevas aplicaciones. Conectado a un servidor de autenticación, un adaptador de red inalámbrica autentica a usuarios y les proporciona acceso a datos protegidos. Un servidor de localización indica las ubicaciones de los usuarios y envía informaciones de localización hacia un servidor de control centralizado y al servidor de autenticación. Con estas informaciones, el servidor de control centralizado inicia y optimiza los procesos de intercambio de informaciones y coordina las funciones de los servidores y de los terminales de los usuarios, para permitir, en particular, realizar transacciones.

La solicitud de patente DE 10 2004 046 847 tiene como objetivo un sistema para realizar transacciones a través de Internet usando una tarjeta de microcircuito como medio de firma. Este sistema usa un lector de tarjeta conectado a un ordenador a su vez conectado a Internet. Los datos se reciben por un servidor y se verifican. Se devuelve un acuse de recibo y se realiza la transacción cuando se obtiene una firma digital.

La invención permite resolver al menos uno de los problemas expuestos anteriormente.

Por tanto, la invención tiene por objeto un dispositivo electrónico portátil personal para permitir a un acreedor realizar una transferencia de un importe en valores, comprendiendo este dispositivo los siguientes medios,

- medios de comunicación inalámbrica de corto alcance;
- medios para recibir un mensaje protegido de una entidad electrónica portátil personal de un deudor, comprendiendo dicho mensaje protegido al menos una información de autenticación de dicho deudor y recibiéndose a través de dichos medios de comunicación inalámbrica de corto alcance;
- medios para crear un mensaje de transacción que comprende al menos un dato asociado a dicho importe en valores; y,

- medios para transmitir dicho mensaje de transacción.

Por tanto, el dispositivo según la invención permite realizar sencillamente una transacción de manera protegida con la ayuda de una entidad electrónica portátil personal, tal como un teléfono móvil, sin tener que recurrir a un dispositivo específico, tal como un terminal de pago, ni a un entorno particular.

Dicho mensaje protegido comprende, además, una referencia a dicho deudor, estando dichos medios para recibir un mensaje protegido adaptados para transmitir dicha referencia a dichos medios, para crear un mensaje de transacción, estando dichos medios para crear un mensaje de transacción adaptados para añadir dicha referencia a dicho mensaje de transacción. El mensaje de transacción comprende una referencia al deudor, para permitir que un sistema informático de un tercero realice una operación de cargo correspondiente a la transacción.

Dicho mensaje protegido comprende, además, dicho al menos un dato asociado a dicho importe en valores, estando dichos medios para recibir un mensaje protegido adaptados para transmitir dicho al menos un dato asociado a dicho importe en valores, a dichos medios para crear un mensaje de transacción. Por tanto, el dispositivo según la invención permite a un deudor introducir o validar el importe de la transacción en su entidad electrónica portátil personal.

El dispositivo según la invención comprende, además, preferiblemente, medios de introducción adaptados, por ejemplo, para introducir dicho al menos un dato asociado, a dicho importe en valores. Tales medios de introducción también pueden usarse para introducir un dato que permita la autenticación de dicho deudor, tal como un código personal de identificación.

Dichos medios de comunicación inalámbrica de corto alcance están adaptados para transmitir dicho dato que permita la autenticación de dicho deudor. Por tanto, si el deudor introduce un dato que permita su autenticación en la entidad electrónica portátil personal del acreedor, la autenticación del deudor puede realizarse, no obstante, en la entidad electrónica portátil personal del deudor para proteger la transacción.

Según una realización particular, el dispositivo comprende, además, medios de memorización en los que se almacena al menos una información complementaria, tal como una referencia de una cuenta a abonar o una referencia de dicho acreedor, estando dichos medios para crear un mensaje de transacción adaptados para añadir dicha al menos una información complementaria a dicho mensaje de transacción. Por tanto, el mensaje de transacción puede comprender una referencia para permitir que un sistema informático de un tercero realice una operación de abono correspondiente a la transacción.

El dispositivo comprende, además, medios para añadir al menos una información de autenticación a dicho mensaje de transacción, permitiendo dicha al menos una información de autenticación que un destinatario de dicho mensaje de transacción autentique al menos una parte de dicho mensaje de transacción. Una información de autenticación de este tipo permite autenticar dicho al menos un dato, dicho deudor y/o dicho acreedor.

Dichos medios para añadir al menos una información de autenticación comprenden medios criptográficos para firmar al menos una parte de dicho mensaje de transacción.

El dispositivo comprende, además, medios criptográficos adaptados para encriptar al menos una parte de dicho mensaje de transacción para proteger la transacción.

Según una realización particular, dichos medios para transmitir dicho mensaje de transacción están adaptados para transmitir de manera aplazada dicho mensaje de transacción. Por tanto, una transacción que hace intervenir un sistema informático de un tercero puede iniciarse en ausencia de una conexión con este sistema informático.

El dispositivo comprende, además, preferiblemente, medios para recibir un mensaje de confirmación de transacción. Por tanto, cuando la transacción hace intervenir un sistema informático de un tercero, es posible verificar que la transacción se ha realizado correctamente. El dispositivo comprende, ventajosamente, medios de memorización para almacenar al menos un mensaje recibido de confirmación de transacción, con el fin de conservar un historial de las transacciones.

Todavía según una realización particular, dichos medios de comunicación inalámbrica de corto alcance están adaptados para transmitir dicho mensaje de confirmación de transacción. Por tanto, es posible transmitir el mensaje de confirmación de transacción a la entidad electrónica portátil personal del deudor.

Según una realización particular, el dispositivo comprende, además, medios para memorizar al menos un primer número y medios para restar o sumar al menos un segundo número a dicho primer número, según dicho al menos un dato. Por tanto, la transacción puede realizarse directamente entre entidades electrónicas portátiles personales, sin recurrir a un sistema informático de un tercero.

El dispositivo comprende, además, medios adaptados para establecer un canal de comunicación protegido entre dichos medios de comunicación inalámbrica de corto alcance, y medios equivalentes de otro dispositivo electrónico portátil para proteger la transacción.

El dispositivo comprende, además, medios de telefonía móvil y/o medios de acceso a una red de comunicación de datos que permiten la transmisión de una petición de transacción a un sistema informático de un tercero.

Por tanto, el dispositivo según la invención permite combinar un intercambio local de información y un intercambio de información a través de una red de telefonía móvil o de datos, para simplificar y proteger una transacción.

De manera ventajosa, el dispositivo comprende, además, medios para indicar el estado de dicha transacción. Por tanto, el dispositivo según la invención permite, en particular, determinar si los dispositivos del deudor y del acreedor deben estar en proximidad uno del otro.

Dichos medios de comunicación inalámbrica de corto alcance son, por ejemplo, según la norma de NFC. Pueden estar integrados en una tarjeta de microcircuito.

Dicho importe en valores es, por ejemplo, un valor monetario, un número de puntos de fidelidad, un bono de compra o de suscripción, un número de puntos de juego, un número de unidades telefónicas o derechos de restitución de grabaciones digitales.

La invención también tiene por objeto un teléfono móvil que comprende el dispositivo tal como se describió anteriormente.

La invención también tiene por objeto un procedimiento para la transmisión de un importe en valores entre un deudor y un acreedor, cada uno dotado de una entidad electrónica portátil personal que comprende medios de comunicación inalámbrica de corto alcance, comprendiendo este procedimiento las siguientes etapas,

- recibir al menos una información de autenticación de dicho deudor a través de dichos medios de comunicación inalámbrica de corto alcance;
- recibir al menos un dato asociado a dicho importe en valores;
- crear un mensaje de transacción que comprende al menos dicho al menos un dato; y,
- transmitir dicho mensaje de transacción.

Por tanto, el procedimiento según la invención permite realizar sencillamente una transacción de manera protegida con la ayuda de una entidad electrónica portátil personal, tal como un teléfono móvil, sin tener que recurrir a un dispositivo específico, tal como un terminal de pago ni a un entorno particular.

Dicho al menos un dato asociado a dicho importe en valores se recibe a través de dichos medios de comunicación inalámbrica de corto alcance. Por tanto, el procedimiento según la invención puede permitir a un deudor introducir o validar el importe de la transacción en su entidad electrónica portátil personal.

El procedimiento comprende, además, una etapa de adquisición de al menos un dato que permita la autenticación de dicho deudor. Por tanto, el deudor puede usar, por ejemplo, un código personal de identificación para autenticarse. También pueden usarse otros datos, tales como una huella dactilar.

El procedimiento comprende, además, una etapa de adición de una información relativa a dicho deudor en dicho mensaje de transacción. El mensaje de transacción comprende una referencia al deudor, para permitir que un sistema informático de un tercero realice una operación de cargo correspondiente a la transacción.

El procedimiento comprende, además, una etapa de adición de una información complementaria relativa a dicho acreedor en dicho mensaje de transacción. El mensaje de transacción comprende una referencia al acreedor, para permitir que un sistema informático de un tercero realice una operación de abono correspondiente a la transacción.

El procedimiento comprende, además, una etapa para añadir al menos una información de autenticación a dicho mensaje de transacción, permitiendo dicha al menos una información de autenticación que un destinatario de dicho mensaje de transacción autentique al menos una parte de dicho mensaje de transacción. Por tanto, es posible autenticar dicho al menos un dato, dicho deudor y/o dicho acreedor. Dicha etapa para añadir al menos una información de autenticación comprende una etapa para firmar al menos una parte de dicho mensaje de transacción.

El procedimiento comprende, además, una etapa de encriptación de al menos una parte de dicho mensaje de transacción, para proteger la transacción.

El procedimiento comprende una etapa de establecimiento de un canal de comunicación protegido entre dichos medios de comunicación inalámbrica de corto alcance de dichas entidades electrónicas portátiles personales, con el fin de proteger la transacción.

El procedimiento se pone en práctica, ventajosamente, en la entidad electrónica portátil personal de dicho acreedor.

De manera ventajosa, el procedimiento comprende, además, una etapa de acercamiento de dichas entidades electrónicas portátiles personales para proteger la transacción.

Dicho mensaje de transacción se transmite por una red móvil de comunicación o por una red de comunicación de datos, por ejemplo, a través de una conexión establecida entre dicha entidad electrónica portátil personal de dicho acreedor y un sistema informático de un tercero.

Por tanto, el procedimiento según la invención permite combinar un intercambio local de información y un intercambio de información a través de una red de telefonía móvil o de datos, para simplificar y proteger una transacción.

Según una realización particular, dicho mensaje de transacción se transmite de manera aplazada. Por tanto, una transacción que hace intervenir un sistema informático de un tercero puede iniciarse en ausencia de una conexión con este sistema informático.

Ventajosamente, el procedimiento comprende, además, una etapa de recepción de un mensaje de confirmación de transacción. Por tanto, cuando la transacción hace intervenir un sistema informático de un tercero, es posible verificar que la transacción se ha realizado correctamente. Además, el procedimiento comprende, preferiblemente, una etapa de memorización de dicho mensaje de confirmación de transacción, con el fin de conservar un historial de las transacciones.

Todavía según una realización particular, el procedimiento comprende, además, una etapa de retransmisión de dicho mensaje de confirmación de transacción a través de dichos medios de comunicación inalámbrica de corto alcance. Por tanto, es posible transmitir el mensaje de confirmación de transacción a la entidad electrónica portátil personal del deudor.

Todavía según una realización particular, el procedimiento comprende, además, una etapa de suma o de resta de dicho al menos un dato a un número previamente memorizado. Por tanto, la transacción puede realizarse directamente entre entidades electrónicas portátiles personales, sin recurrir a un sistema informático de un tercero.

De manera ventajosa, el procedimiento comprende, además, una etapa para indicar el estado de dicha transacción. Por tanto, el procedimiento según la invención permite, en particular, determinar si las entidades electrónicas portátiles del deudor y del acreedor deben estar en proximidad una de la otra.

Dicho importe en valores es, por ejemplo, un valor monetario, un número de puntos de fidelidad, un bono de compra o de suscripción, un número de puntos de juego, un número de unidades telefónicas o derechos de restitución de grabaciones digitales.

Según una realización particular, dicha entidad electrónica portátil personal de dicho acreedor es un teléfono móvil. Asimismo, según una realización particular, dicha entidad electrónica portátil personal de dicho deudor es un teléfono móvil o una tarjeta de microcircuito. Por tanto, el procedimiento según la invención es fácil de poner en práctica y no necesita ningún dispositivo específico, tal como un terminal de pago, ni un entorno particular.

La invención también tiene por objeto un programa de ordenador que comprende instrucciones adaptadas para la puesta en práctica de cada una de las etapas del procedimiento tal como se describió anteriormente.

Otras ventajas, objetivos y características de la presente invención se desprenderán de la siguiente descripción detallada, realizada a modo de ejemplo no limitativo, con respecto a los dibujos adjuntos en los que:

- la Figura 1 representa esquemáticamente una entidad electrónica portátil que permite la puesta en práctica de la invención;

- la Figura 2, que comprende las Figuras 2a y 2b, ilustra un primer ejemplo de algoritmo para poner en práctica la invención, con el fin de transferir un importe en valores entre un deudor y un acreedor, cada uno dotado de una entidad electrónica portátil;

- la Figura 3 ilustra un ejemplo de una parte de mensaje que puede transmitirse por la entidad electrónica portátil del deudor a la del acreedor durante la transacción, antes de encriptarse;

- la Figura 4 ilustra un ejemplo de una parte de mensaje transmitido por la entidad electrónica portátil del acreedor a la del deudor, cuando el acreedor ha validado la transacción o una parte de mensaje transmitido a un sistema informático de un establecimiento bancario, de un tercero de confianza o de una persona encargada de la gestión de los valores considerados, en forma de petición de transacción; y,

- la Figura 5, que comprende las Figuras 5a, 5b y 5c, ilustra un segundo ejemplo de puesta en práctica de la invención, con el fin de transferir un importe en valores entre un deudor y un acreedor, cada uno dotado de una entidad electrónica portátil.

La invención permite a un deudor transmitir un importe en valores a un acreedor, con la ayuda de un teléfono móvil y de una entidad electrónica, tal como un teléfono móvil o una tarjeta de microcircuito. Estos dispositivos electrónicos están dotados, en este caso, de medios de comunicación inalámbrica de corto alcance que permiten, por ejemplo, una comunicación a una distancia máxima de un metro, de cincuenta centímetros o de veinte centímetros.

El teléfono móvil también está dotado de medios de comunicación para permitir transferir una petición de transacción a un sistema informático, normalmente, un servidor, de un establecimiento bancario, de un tercero de confianza o de una persona encargada de la gestión de los valores considerados. Tales medios de comunicación son, por ejemplo, medios de comunicaciones telefónicas, concretamente GSM (siglas de *Global System for Mobile Communications,* en terminología inglesa) o GPRS (siglas de *General Packet Radio Service,* en terminología inglesa). Alternativamente, estos medios de comunicación permiten acceder a una red de comunicación de datos a la que está conectado el sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados, para transmitir la petición de transacción a través de la red. Tales medios de comunicación son, a modo de ilustración, compatibles con al menos una de las normas WiFi.

Los importes en valores son, por ejemplo, valores monetarios, puntos de fidelidad, bonos de compra o de suscripción, puntos de juego, unidades telefónicas o derechos de restitución de grabaciones digitales (audio o audio y vídeo).

La Figura 1 representa un teléfono 100 móvil adecuado para poner en práctica la invención. Tal como se ilustra, el teléfono 100 móvil comprende un módulo 110 de telefonía móvil, ventajosamente, conectado a un altavoz 120 y a un micrófono 130. El teléfono 100 móvil también comprende una unidad 140 central de procesamiento, también denominada CPU (siglas de *Central Processing Unit,* en terminología inglesa) y, preferiblemente, una pantalla 150.

El teléfono 100 móvil comprende, además, un módulo 160 de comunicación de corto alcance, ventajosamente, un módulo de comunicación inalámbrica de corto alcance. El módulo 160 es, por ejemplo, del tipo NFC (siglas de *Near Field Communication,* en terminología inglesa). El módulo 160 puede implantarse directamente en el teléfono 100 móvil, por ejemplo, en forma de circuito integrado y de antena, o insertarse en el teléfono 100 móvil, por ejemplo, en forma de tarjeta de microcircuito que comprende una antena integrada.

El teléfono móvil también comprende un dispositivo 170 de introducción, tal como un teclado o un dispositivo equivalente, para introducir caracteres, importes en valores y/o comandos. El dispositivo 170 de introducción forma, en colaboración con la pantalla 150, una interfaz de usuario. El dispositivo 170 de introducción también puede estar integrado en la pantalla 150, en forma de pantalla táctil.

El teléfono 100 móvil también comprende un módulo 180 de memoria adaptado para memorizar al menos una aplicación 190 que permite el intercambio de importes en valores, con la ayuda del módulo 160 de comunicación inalámbrica de corto alcance, con otra entidad electrónica portátil dotada de un módulo de comunicación compatible con el mismo.

La Figura 2, que comprende las Figuras 2a y 2b, ilustra un primer ejemplo de algoritmo para poner en práctica la invención, con el fin de transferir un importe en valores entre dos personas, un deudor y un acreedor, estando uno dotado de un teléfono móvil, por ejemplo, el representado en la Figura 1, y el otro de una entidad electrónica portátil que también puede ser un teléfono móvil. En este caso se considera que el deudor y el acreedor disponen, cada uno, de un teléfono móvil, tal como el representado en la Figura 1. El deudor y el acreedor disponen, por tanto, de teléfonos 100 y 100' móviles, respectivamente.

El deudor es la persona a la que se le retira el importe en valores, por ejemplo, el titular de una cuenta en la que se realiza un cargo, mientras que el acreedor es la persona que recibe el importe en valor, por ejemplo, el titular de una cuenta en la que se abona.

La Figura 2a representa el algoritmo puesto en práctica en el teléfono móvil del deudor, mientras que la Figura 2b representa el algoritmo puesto en práctica en el teléfono móvil del acreedor. Preferiblemente, estos algoritmos están parcialmente integrados en un módulo protegido (autenticación y adición de informaciones que permiten la autenticación) y, parcialmente, en una misma aplicación, por ejemplo, las aplicaciones 190 y 190', que puede usarse para operaciones de cargo y de abono (interfaz de usuario).

En primer lugar, el deudor debe lanzar la aplicación que permita transferir un importe en valores (etapa 200). Esta aplicación es, por ejemplo, la aplicación 190 representada en la Figura 1. El usuario puede introducir, a continuación, un importe en valores (etapa 205) con la ayuda del dispositivo 170 de introducción. Este importe puede visualizarse en la pantalla 150 antes de validarse.

Cuando el usuario ha validado este importe, se le puede invitar a introducir un identificador del acreedor (etapa 210), en particular, si no se ha establecido un canal de comunicación protegido entre las entidades electrónicas portátiles del deudor y del acreedor. El identificador del acreedor es, preferiblemente, corto, tal como iniciales. Puede representarse, por ejemplo, en seis octetos. De nuevo, el identificador del acreedor puede visualizarse antes de validarse. Este identificador se facilita, por ejemplo, verbalmente por el acreedor.

A continuación, se invita al usuario a introducir una indicación que permita su autenticación, tal como un número de identificación personal (etapa 215), también denominado código confidencial o código PIN (acrónimo de *Personnal Identification Number,* en terminología inglesa). Preferiblemente, este código no se visualiza o, ventajosamente, se oculta al menos parcialmente con el fin de que no pueda visualizarlo ninguna persona malintencionada.

Cuando se ha validado el código confidencial, por el usuario o automáticamente si responde a reglas predeterminadas, se realiza una prueba para autenticar al usuario (etapa 220). Para ello, el código confidencial puede transmitirse a un módulo de autenticación que puede estar implantado, por ejemplo, en el módulo 160 de comunicación inalámbrica de corto alcance. El módulo de autenticación compara el código introducido por el usuario con un código previamente grabado. Si el código confidencial introducido por el usuario no corresponde al código previamente grabado, se invita al usuario a introducir de nuevo el código confidencial. El número de intentos para introducir el código confidencial puede estar limitado, por ejemplo, a 3 intentos. Alternativamente, o de manera complementaria, puede introducirse un tiempo de pausa entre cada intento, aumentando el tiempo de pausa entre cada intento.

Si el código confidencial es correcto, el módulo de autenticación envía un acuse de recibo a la aplicación 190 que permite transferir un importe en valores que, preferiblemente, visualiza una indicación de autenticación en la pantalla 150 para avisar de que la transacción puede realizarse.

Se crea un mensaje (etapa 225). El mensaje comprende, concretamente, el importe en valores introducido por el usuario. El mensaje también comprende indicaciones relativas a la identificación del deudor y de la cuenta en la que debe realizarse el cargo. La Figura 3 ilustra un ejemplo de las informaciones contenidas en un mensaje de este tipo. Este mensaje puede crearse por la aplicación 190.

Conviene observar, en este caso, que el mensaje comprende una indicación relativa a la identidad del acreedor, tal como sus iniciales. No obstante, según una realización ventajosa, la transacción está precedida por un intercambio de informaciones preliminares, mediante la interfaz de comunicación inalámbrica de corto alcance, entre los dos teléfonos móviles, con el fin de implementar un canal de comunicación protegido. Este intercambio de informaciones preliminares también se usa para la transmisión de una o de varias claves criptográficas temporales, usadas para encriptar y desencriptar los datos intercambiados.

La comunicación establecida entre los teléfonos móviles se protege, preferiblemente, con la ayuda de un módulo de protección que comprende medios criptográficos conocidos por el experto en la técnica, normalmente, medios para encriptar, desencriptar, firmar y verificar una firma, y medios para memorizar una o varias claves criptográficas.

Tal como se indicó anteriormente, preferiblemente, se establece un canal de comunicación protegido entre los dos teléfonos móviles. Dado que la comunicación mediante la interfaz de comunicación inalámbrica de corto alcance está ahora protegida mediante el uso de claves temporales, no siempre es necesario encriptar específicamente el mensaje con la ayuda de otra clave.

Preferiblemente, se encripta y/o se firma al menos una parte del mensaje. La indicación relativa al acreedor se encripta y se firma, para permitir al acreedor autenticar el mensaje, mientras que las informaciones relativas al importe y al número de cuenta del deudor se encriptan y se firman, para permitir al servidor encargado de realizar la transacción autenticar el mensaje para verificar que se ha presentado correctamente por el deudor. Se usan dos claves diferentes.

Un módulo de protección que comprenda medios criptográficos para encriptar, desencriptar, firmar y verificar una firma, puede estar implantado, por ejemplo, en el módulo 160 de comunicación inalámbrica de corto alcance. El módulo de protección comprende, preferiblemente, un microcontrolador protegido, certificado según los criterios comunes o de acuerdo con las exigencias de FIPS (acrónimo de *Federal Information Processing Standards,* en terminología inglesa). Este módulo se usa para encriptar y desencriptar todos los datos que transitan por el canal de comunicación protegido o, más específicamente, el mensaje. Entonces, se transmite el mensaje al módulo 160 de comunicación inalámbrica de corto alcance, para encriptarse en el mismo. Los medios de encriptación están basados, por ejemplo, en algoritmos convencionales, tales como los algoritmos DES (sigla de *Data Encryption Standard,* en terminología inglesa), AES (sigla de *Advanced Encryption Standard,* en terminología inglesa) y RSA

(iniciales de los autores de este algoritmo: Rivest, Shamir y Adleman), y una clave memorizada. El módulo de protección también puede estar implantado en otra parte, por ejemplo, en una tarjeta SIM (acrónimo de *Subscriber Identity Module,* en terminología inglesa) insertada en la entidad electrónica portátil o en la aplicación 190.

Naturalmente, existen otros sistemas para proteger la transacción y autenticar al autor del mensaje.

A continuación, se transmite el mensaje encriptado al acreedor (etapa 230) mediante el módulo 160 de comunicación inalámbrica de corto alcance.

Si los teléfonos móviles del deudor y del acreedor no están cerca uno del otro, deben acercarse para estar en proximidad uno del otro, por ejemplo, a una distancia inferior a 20 centímetros o a 50 centímetros. La distancia mínima relativa entre los teléfonos móviles está determinada por el alcance de los medios de comunicación inalámbrica de corto alcance. Esta etapa de acercamiento de los teléfonos móviles contribuye a la seguridad del sistema, limitando el riesgo de que las informaciones intercambiadas se intercepten y usen por un tercero.

Por su lado, el acreedor, cuando se pone de acuerdo con el deudor, lanza la aplicación, con la referencia 190', que permite transferir un importe en valores (etapa 235). Alternativamente, la aplicación 190' puede lanzarse automáticamente tras la recepción del mensaje, cuando el mensaje recibido se ha identificado como un mensaje de transacción.

Cuando el teléfono 100' móvil del acreedor recibe el mensaje encriptado emitido por el deudor (etapa 240) con la ayuda de su módulo 160' de comunicación inalámbrica de corto alcance, se pone en práctica una etapa de autenticación (etapa 245). Esta etapa de autenticación, basada, por ejemplo, en el uso de una clave pública, tiene como objetivo controlar el origen del mensaje recibido. Preferiblemente, la autenticación se realiza mediante un módulo de protección implantado, por ejemplo, en el módulo 160'.

Si no se autentica el mensaje, se rechaza.

Si se autentica el mensaje y si el mensaje no se recibe por un canal de comunicación protegido, se realiza una prueba para determinar si el usuario del teléfono 100' móvil es el destinatario de la transferencia (etapa 250), es decir, si el usuario de este teléfono móvil es el acreedor. Para ello, las indicaciones relativas a la identidad del acreedor contenidas en el mensaje recibido se comparan con las indicaciones relativas a la identidad del acreedor, previamente memorizadas en el teléfono 100' móvil, por ejemplo, en el módulo de protección, que puede estar implantado en el módulo 160' de comunicación inalámbrica de corto alcance. Esta prueba permite proteger la transferencia y reducir el riesgo, bajo (el alcance de comunicación es limitado), de que el mensaje se intercepte por otro teléfono móvil.

Si el usuario no es el destinatario de la transferencia, se rechaza el mensaje.

Si el usuario es el destinatario de la transferencia, se transfiere el mensaje recibido a la aplicación 190'. Si una parte del mensaje es confidencial, preferiblemente, sólo se transmite la parte no confidencial a la aplicación 190', que no está necesariamente protegida. Entonces, preferiblemente, algunas informaciones contenidas en el mensaje se visualizan en la pantalla 150', para permitir al acreedor validar la transacción (etapa 255). Las informaciones visualizadas son, por ejemplo, el importe e indicaciones relativas a la identidad del deudor.

El usuario puede usar el dispositivo 170' de introducción para validar o no la transacción. Si el usuario no valida la transacción, se rechaza el mensaje. Por el contrario, si el usuario valida la transacción, se añaden informaciones complementarias al mensaje recibido (etapa 260). Tal como se ilustra en la Figura 4, estas informaciones complementarias son, por ejemplo, datos relativos a la identidad del acreedor y a la cuenta en la que debe abonarse. Estas informaciones complementarias, preferiblemente, encriptadas en el mensaje, pueden añadirse, a petición de la aplicación 190', mediante el módulo de protección. Por tanto, esta petición para añadir las informaciones complementarias se transmite, preferiblemente, con una indicación de validación, al módulo 160', que comprende, por ejemplo, el módulo de protección. El módulo 160' de comunicación inalámbrica de corto alcance transmite (etapa 265), a su vez, una indicación de validación al módulo 160 de comunicación inalámbrica de corto alcance del teléfono móvil del deudor. La indicación de validación transmitida del teléfono móvil del acreedor al del deudor comprende, ventajosamente, las informaciones complementarias añadidas al mensaje.

La indicación de validación recibida por el módulo 160 de comunicación inalámbrica de corto alcance del teléfono móvil del deudor puede memorizarse por este módulo o en el módulo 180 de memoria (etapa 270). La indicación de validación puede visualizarse en la pantalla 150.

Entonces, se emite una petición de transacción por el teléfono móvil del acreedor, al sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados (etapa 275). Esta petición se transmite, en este caso, por la red de telefonía móvil.

La petición de transacción puede contener informaciones que permitan autenticar la petición, concretamente, informaciones de autenticación añadidas por los módulos 160 y/o 160' con la ayuda de claves criptográficas memorizadas en estos módulos (estas claves criptográficas son diferentes de las claves temporales usadas para proteger la comunicación entre las dos entidades electrónicas portátiles). Por tanto, la petición de transacción es, ventajosamente, similar a la indicación de validación transmitida del teléfono móvil del acreedor al del deudor, eventualmente, encriptada con una clave diferente, que permite la autenticación por un tercero de confianza.

Alternativamente, la petición de transacción puede emitirse por el teléfono móvil del deudor, teniendo en cuenta las informaciones complementarias recibidas con la indicación de validación.

La petición de transacción también puede transmitirse por una red de comunicación de datos tal como Internet.

Si la petición de transacción no se rechaza por el sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados, por ejemplo, si la cuenta no tiene crédito suficiente, la transacción se realiza, de manera convencional, por el sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados. Preferiblemente, se envía un mensaje de confirmación de la transacción a los teléfonos móviles del deudor y del acreedor, cuando se ha realizado la transacción (etapas 280 y 285) o, preferiblemente, únicamente al teléfono móvil del emisor de la petición de la transacción. En este caso, el teléfono móvil del emisor de la petición de la transacción transmite, ventajosamente, al otro teléfono móvil el mensaje de confirmación o de rechazo de la transacción.

Las confirmaciones de transacción se memorizan en cada teléfono móvil, preferiblemente, en una memoria no volátil, con fines de archivado.

Alternativamente, la transacción puede iniciarse por el acreedor que transmite un mensaje que comprende las referencias de la cuenta a abonar al deudor, enviando éste un mensaje de validación de la transacción al deudor, con eventuales informaciones complementarias que le incumben.

Conviene indicar, en este caso, que el módulo 160 de comunicación inalámbrica de corto alcance puede presentarse en forma de una tarjeta de microcircuito. Este módulo es, por ejemplo, un monedero electrónico. Alternativamente, el módulo 160 de comunicación inalámbrica de corto alcance puede estar integrado en la unidad 140 central de procesamiento, formando entonces un único circuito integrado. También puede tratarse de un circuito integrado que comprende la antena, o no, montado en el cuerpo de la entidad electrónica portátil. La antena puede estar integrada en el circuito o en otro componente de la entidad electrónica portátil.

Por otro lado, la conexión al sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados y la comunicación de la petición de transacción, puede realizarse a lo largo de la transacción o puede aplazarse en el tiempo. Esta comunicación está, preferiblemente, protegida. En particular, ventajosamente, se autentica la petición de transacción recibida por el sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados.

Si los valores se memorizan y se actualizan directamente en los teléfonos móviles, no es necesario realizar una conexión a un sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados. Por ejemplo, si los módulos 160 y 160' de comunicación inalámbrica de corto alcance son monederos electrónicos y si las aplicaciones 190 y 190' disponen de las funciones que permitan reducir y aumentar los valores memorizados, no se requiere el establecimiento de una conexión. Asimismo, si los valores considerados son de tipo puntos de fidelidad, si se memorizan directamente en los teléfonos móviles y si los módulos de protección o, alternativamente, las aplicaciones 190 y 190', disponen de las funciones que permitan reducir y aumentar los valores memorizados, no es necesario establecer una conexión.

La Figura 3 ilustra un ejemplo de una parte de mensaje que puede transmitirse por el teléfono móvil del deudor al del acreedor, durante la transacción, antes de encriptarse (etapas 225 y 230 de la Figura 2). Tal como se ilustra, el mensaje 300 comprende, en este caso, un primer campo 305 correspondiente al importe de la transacción y un segundo campo 310 correspondiente a la referencia de la cuenta en la que debe realizarse el cargo o a un identificador del deudor que permita recuperar estas referencias. El mensaje 300 también puede comprender un tercer campo correspondiente al identificador del acreedor, por ejemplo, sus iniciales. Tal como se indicó anteriormente, preferiblemente, se encripta el mensaje 300 antes de transmitirlo. Algunos datos del mensaje, tales como la firma y las claves, no se representan en la fFigura 3.

La Figura 4 ilustra un ejemplo de una parte de mensaje transmitido por el teléfono móvil del acreedor al del deudor, cuando el acreedor ha validado la transacción (etapa 265 de la Figura 2) o de una parte de mensaje transmitido a un sistema informático de un establecimiento bancario, de un tercero de confianza o de una persona encargada de la gestión de los valores considerados, en forma de petición de transacción.

Tal como se ilustra, el mensaje 400 comprende los campos 305 y 310 descritos anteriormente, relativos al importe de la transacción y a la cuenta en la que debe realizarse el cargo o a la identificación del deudor. El mensaje 400 comprende, además, un campo 405 correspondiente a la referencia de la cuenta a abonar o a indicaciones relativas al acreedor que permiten recuperar esta referencia. Algunos datos del mensaje, tales como la firma y las claves, no se representan en la Figura 4. Preferiblemente, se encripta el mensaje 400 antes de transmitirlo.

Conviene indicar que, aunque el acreedor puede leer el mensaje 300 y añadir informaciones relativas a la cuenta a abonar, el acreedor no puede modificar los campos 305 y 310 referentes al importe de la transacción y las referencias de la cuenta en la que debe realizarse el cargo debido a la protección usada.

La Figura 5, que comprende las Figuras 5a, 5b y 5c, ilustra un segundo ejemplo de puesta en práctica de la invención, para transferir un importe en valores entre un deudor y un acreedor, estando uno dotado de un teléfono móvil y el otro de una entidad electrónica portátil que puede ser un teléfono móvil. En este caso, se considera que el acreedor dispone de un teléfono móvil, tal como el presentado en la Figura 1, y que el deudor dispone de una simple tarjeta de microcircuito, que comprende medios de comunicación inalámbrica de corto alcance y medios de autenticación, tales como medios criptográficos de autenticación.

La Figura 5a representa el algoritmo puesto en práctica en el teléfono móvil del acreedor, la Figura 5b representa el algoritmo puesto en práctica en la tarjeta de microcircuito del deudor y la Figura 5c representa el algoritmo puesto en práctica por el establecimiento bancario, el tercero de confianza o la persona encargada de la gestión de los valores considerados.

Tras haber lanzado la aplicación 190 de transferencia de valores (etapa 500), el acreedor introduce un importe en valores (etapa 505), preferiblemente, con la ayuda del dispositivo 170 de introducción. El importe puede visualizarse en la pantalla 150.

A continuación, se invita al deudor a introducir su código confidencial en el teléfono móvil del acreedor (etapa 510). El código confidencial se introduce, ventajosamente, con la ayuda del dispositivo 170 de introducción. Preferiblemente, no se visualiza en la pantalla 150.

Entonces, se forma una petición de autenticación por la aplicación 190, que contiene el código confidencial y se transmite al módulo 160 de comunicación inalámbrica de corto alcance. A su vez, el módulo 160 transmite la petición de autenticación a la tarjeta de microcircuito del deudor.

El teléfono móvil del acreedor y la tarjeta de microcircuito del deudor, se acercan para permitir una transmisión de datos entre sí, con la ayuda de los medios de comunicación inalámbrica de corto alcance.

De manera ventajosa, se establece un canal de comunicación protegido entre el teléfono móvil del acreedor y la tarjeta de microcircuito del deudor, con la ayuda de claves temporales de encriptación. Estas claves temporales se memorizan, por ejemplo, en módulos de protección que pueden estar implantados en los módulos de comunicación inalámbrica de corto alcance.

Alternativamente, la petición de autenticación puede encriptarse antes de transmitirse a la tarjeta de microcircuito del deudor.

Tras haber recibido la petición de autenticación (etapa 520), la tarjeta de microcircuito de deudor autentica el código confidencial contenido en la petición, comparándolo, por ejemplo, con un código confidencial previamente memorizado en la tarjeta de microcircuito del deudor (etapa 525).

Si no se valida el código confidencial, se rechaza la petición. Si, por el contrario, se valida el código confidencial, la tarjeta de microcircuito del deudor crea, en respuesta a esta petición, un mensaje de autenticación que se transmite (etapa 530) al teléfono móvil del acreedor, es decir, al módulo 160.

El mensaje de autenticación comprende primeras informaciones que permiten la autenticación de este mensaje por el acreedor y segundas informaciones que permiten la autenticación de este mensaje por un tercero, por ejemplo, por un sistema informático de un establecimiento bancario. Estas informaciones que permiten la autenticación pueden ser una firma. El mensaje de autenticación se encripta al menos parcialmente.

El mensaje de autenticación comprende, en forma encriptada, referencias del deudor, que permiten a un sistema informático de un establecimiento bancario, de un tercero de confianza o de una persona encargada de la gestión de los valores considerados, realizar un cargo en una cuenta.

Tras la recepción del mensaje de autenticación (etapa 535), el módulo 160 transmite el mensaje de autenticación a la aplicación 190. La aplicación forma, entonces, una petición de transacción que comprende el mensaje de autenticación, el importe previamente introducido y referencias del acreedor, tales como su número de cuenta.

La petición de transacción comprende informaciones que permiten la autenticación del deudor, del importe de la transacción y/o del acreedor. La petición de transacción puede comprender una parte del mensaje de autenticación recibido a partir de la entidad electrónica portátil del deudor.

La petición de transacción se encripta al menos parcialmente con la ayuda de medios criptográficos.

A continuación, se transmite la petición de transacción (etapa 540) por el teléfono móvil del acreedor, a un sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados. La petición de transacción se transmite, en este caso, por la red de telefonía móvil.

Cuando se recibe la petición de transacción (etapa 545) por un sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados, éste, o ésta, autentica la petición de transacción. Si no se autentica la petición de transacción, se rechaza. Asimismo, si no puede realizarse la transacción, por ejemplo, si la cuenta del deudor no tiene crédito suficiente, se rechaza la petición de transacción. Si no se rechaza la petición de transacción, el importe en valores se transfiere (etapa 550) de manera convencional. Entonces, se transmite, ventajosamente, un mensaje de confirmación o de rechazo de la transacción por el sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados (etapa 555), al teléfono móvil del acreedor, cuando se ha realizado o rechazado la transacción.

Al recibirse esta confirmación o este rechazo (etapa 560), se visualiza una indicación en la pantalla 150, para indicar que la transacción se ha realizado o rechazado. Esta confirmación puede retransmitirse a la tarjeta de microcircuito del deudor en la que puede memorizarse.

El mensaje de confirmación puede adoptar la forma de un SMS (sigla de *Short Message Service,* en terminología inglesa), transmitiéndose el número de teléfono del acreedor con la petición de transacción o estando memorizado por un sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados en relación con las referencias de la cuenta a abonar.

Alternativamente, la petición y el mensaje de transacción pueden transmitirse por una red de comunicación de datos, por ejemplo, Internet, a la que están conectados el teléfono móvil del acreedor y un sistema informático del establecimiento bancario, del tercero de confianza o de la persona encargada de la gestión de los valores considerados. El teléfono móvil del acreedor puede estar conectado a esta red, por ejemplo, según una de las normas WiFi.

Si puede validarse el acuerdo del deudor mediante la introducción de un código confidencial y la comparación del código introducido con un código previamente memorizado, este acuerdo puede validarse según otras técnicas. En particular, el acuerdo del deudor puede validarse mediante medios biométricos, tales como una comparación de huella dactilar. En este caso, la entidad electrónica portátil del deudor debe estar dotada de medios que permitan la introducción de esta información, por ejemplo, un lector de huella dactilar.

Según otra realización, en primer lugar se transmite un mensaje de transacción por el acreedor al deudor. El teléfono móvil del acreedor y la entidad electrónica portátil del deudor, cada uno dotado de medios de comunicación inalámbrica de corto alcance, disponen, en este caso, cada uno, de una memoria, preferiblemente, protegida, que permite almacenar un saldo en valores con respecto al cual puede abonarse y cargarse el importe en valores de la transacción. Alternativamente, sólo el teléfono móvil del acreedor o la entidad electrónica portátil del deudor dispone de tal saldo, ejecutándose, entonces, parcialmente la transacción por un sistema informático de un tercero.

El teléfono móvil del acreedor transmite a la entidad electrónica portátil del deudor, a través de los medios de comunicación inalámbrica de corto alcance, un mensaje de transacción protegido que comprende el importe en valores de la transacción. El mensaje se protege según una clave criptográfica que puede usarse por un gran número de portadores de entidad electrónica portátil.

Si el teléfono móvil del deudor no está en proximidad de la entidad electrónica portátil del deudor, el teléfono móvil del deudor y la entidad electrónica portátil del deudor deben acercarse uno al otro.

De manera ventajosa, la entidad electrónica portátil del deudor dispone de un botón de activación que permite activar la recepción de mensajes de transacción a través de los medios de comunicación inalámbrica de corto alcance. Por tanto, el deudor controla la recepción de los mensajes de transacción para evitar un cargo sin su consentimiento. En una realización particular, este botón de activación activa los medios de comunicación inalámbrica de corto alcance.

El mensaje de transacción se autentica por la entidad electrónica portátil del deudor, con el fin de verificar que el acreedor está autorizado para emitirle un mensaje de transacción de este tipo.

Tras haber autenticado el mensaje de transacción, la entidad electrónica portátil del deudor realiza un cargo del saldo en valores memorizado del importe en valores de la transacción. A continuación, la entidad electrónica portátil

del deudor transmite, a través de los medios de comunicación inalámbrica de corto alcance, un mensaje protegido al teléfono móvil de acreedor. El mensaje protegido comprende, preferiblemente, el importe en valores de la transacción.

De nuevo, si el teléfono móvil del acreedor no está en proximidad de la entidad electrónica portátil del deudor, el teléfono móvil del acreedor y la entidad electrónica portátil del deudor deben acercarse uno al otro.

Al recibirse el mensaje protegido, el teléfono móvil del acreedor autentica este mensaje. Si se autentica el mensaje, puede abonarse el saldo en valores memorizado.

Si el teléfono móvil del acreedor o la entidad electrónica portátil del deudor no dispone de memoria para almacenar un saldo en valores, transmite una petición de transacción correspondiente a un sistema informático de un tercero, para realizar esta operación.

De manera ventajosa, cuando se pone en práctica un intercambio de datos entre las entidades electrónicas portátiles para proceder a la transacción, por ejemplo, según la última realización descrita, la entidad electrónica portátil del acreedor y/o la del deudor disponen de medios para indicar al usuario que una transacción está en curso y/o que se ha terminado.

En efecto, según la última realización descrita, en caso de corte de la comunicación tras la transmisión del mensaje de transacción y antes de la recepción del mensaje protegido, puede realizarse un cargo en la entidad electrónica portátil del deudor, mientras que no se abonará en el teléfono móvil del acreedor.

A modo de ilustración, el teléfono móvil del acreedor emite una primera señal acústica cuando se transmite un mensaje de transacción y emite una segunda señal acústica, preferiblemente, diferente de la primera, cuando se recibe un mensaje protegido. Alternativamente, o de manera complementaria, puede visualizarse una indicación visual de transacción en la pantalla de la entidad electrónica portátil para indicar que la transacción está en curso o se ha terminado.

En una realización particular, el teléfono móvil del acreedor usa un indicador interno de estado. Según esta realización, el teléfono móvil del acreedor activa un indicador interno de estado cuando se emite el mensaje de transacción. Este indicador interno de estado se desactiva al recibirse el mensaje protegido correspondiente al mensaje de transacción.

Pueden usarse varios indicadores internos de estado cuando el acreedor realiza varias transacciones en un breve intervalo de tiempo.

Si, tras un tiempo predeterminado, el indicador interno de estado sigue estando activo, debe anularse la transacción ante la entidad electrónica portátil de deudor, o debe volver a emitirse el mensaje protegido. Para ello, el teléfono móvil del acreedor puede enviar un mensaje de anulación de transacción o un mensaje de nueva emisión del mensaje protegido.

REIVINDICACIONES

1. Procedimiento para la transmisión de un importe en valores entre un deudor y un acreedor, cada uno dotado de una entidad electrónica portátil personal que comprende medios de comunicación inalámbrica de corto alcance, transfiriéndose dicho importe en valores de una cuenta de dicho deudor a una cuenta de dicho acreedor mediante un sistema informático encargado de la gestión de los valores considerados, estando este procedimiento **caracterizado por que** comprende las siguientes etapas,

   - introducir (210) en dicha entidad electrónica portátil de dicho deudor, un identificador de dicho acreedor;
   - recibir (240, 535) por dicha entidad electrónica portátil de dicho acreedor, al menos una información de autenticación de dicho deudor, recibiéndose dicha al menos una información de autenticación a partir de dicha entidad electrónica portátil de dicho deudor, a través de dichos medios de comunicación inalámbrica de corto alcance, transmitiéndose dicho identificador de dicho acreedor a dicha entidad electrónica portátil de dicho acreedor con dicha al menos una información de autenticación;
   - recibir (240, 505) al menos un dato asociado a dicho importe en valores;
   - crear por dicha entidad electrónica portátil de dicho acreedor, un mensaje de transacción, que comprende al menos dicho al menos un dato, dicha al menos una información de autenticación y datos relativos a la identidad de dicho acreedor y de dicha cuenta a abonar; y,
   - transmitir (275, 540) dicho mensaje de transacción a dicho sistema informático encargado de la gestión de los valores considerados, a través de una red de telefonía móvil o una red de comunicación de datos, aplazándose dicha transmisión de dicho mensaje de transacción, en ausencia de una conexión con dicho sistema informático, que comprende, además, una etapa de encriptación, por dicha entidad electrónica portátil de dicho deudor, de dicha al menos una información de autenticación y una etapa de encriptación, por dicha entidad electrónica portátil de dicho deudor, de dicho identificador de dicho acreedor, usando dicha encriptación de dicha al menos una información de autenticación y la encriptación de dicho identificador de dicho acreedor, claves diferentes.

2. Procedimiento según la reivindicación 1, que comprende, además, una etapa de acercamiento de dichas entidades electrónicas portátiles personales.

3. Procedimiento según la reivindicación 1 o la reivindicación 2, que comprende, además, una etapa de introducción (205), en dicha entidad electrónica portátil de dicho deudor, de dicho al menos un dato asociado a dicho importe en valores, transmitiéndose dicho al menos un dato asociado a dicho importe en valores a dicha entidad electrónica portátil de dicho acreedor con dicha al menos una información de autenticación.

4. Procedimiento según la reivindicación 1 o la reivindicación 2, que comprende, además, una etapa de introducción (505), en dicha entidad electrónica portátil de dicho acreedor, de dicho al menos un dato asociado a dicho importe en valores.

5. Procedimiento según la reivindicación 1, que comprende, además, una etapa de recepción (280, 560) de un mensaje de confirmación de transacción y una etapa de retransmisión (280) de dicho mensaje de confirmación de transacción, a través de dichos medios de comunicación inalámbrica de corto alcance.

6. Procedimiento según una cualquiera de las reivindicaciones anteriores, que comprende, además, una etapa de introducción (215), en dicha entidad electrónica portátil de dicho deudor, de un número de identificación personal de dicho deudor y una etapa de comparación de dicho número de identificación personal con un código previamente registrado, transmitiéndose dicha al menos una información de autenticación, en respuesta a dicha comparación.

7. Procedimiento según una cualquiera de las reivindicaciones anteriores, según el cual dicha entidad electrónica portátil personal de dicho deudor y/o de dicho acreedor, es un teléfono móvil.

8. Programa de ordenador que comprende instrucciones adaptadas para la puesta en práctica de cada una de las etapas del procedimiento según una cualquiera de las reivindicaciones anteriores.

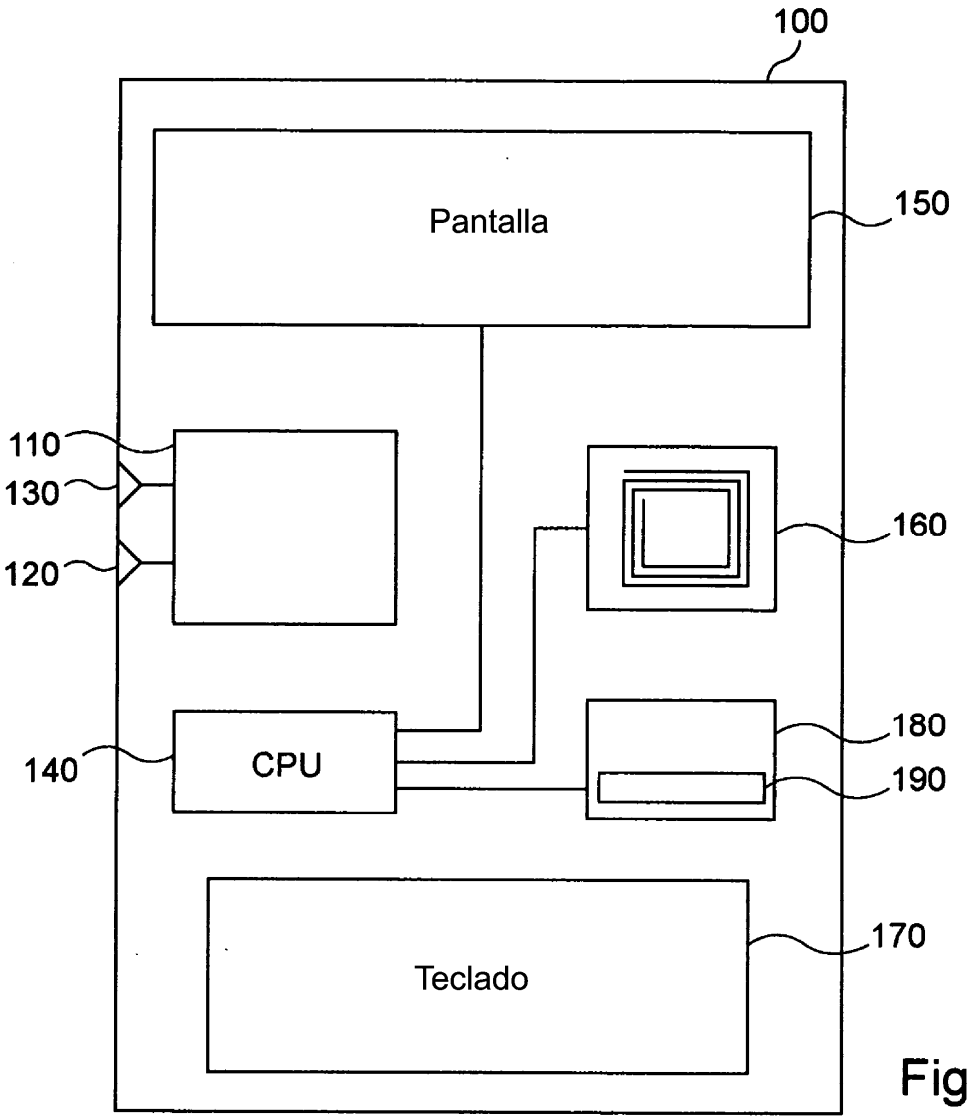

Fig. 1

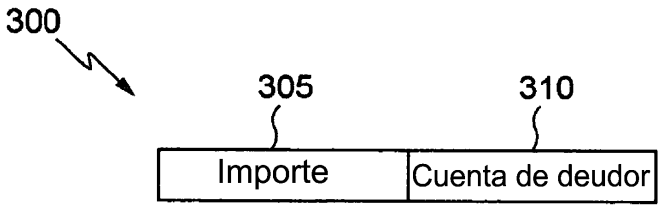

Fig. 3

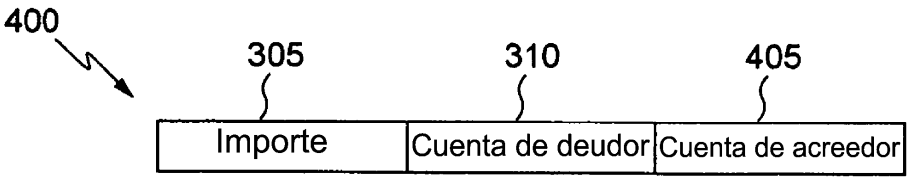

Fig. 4

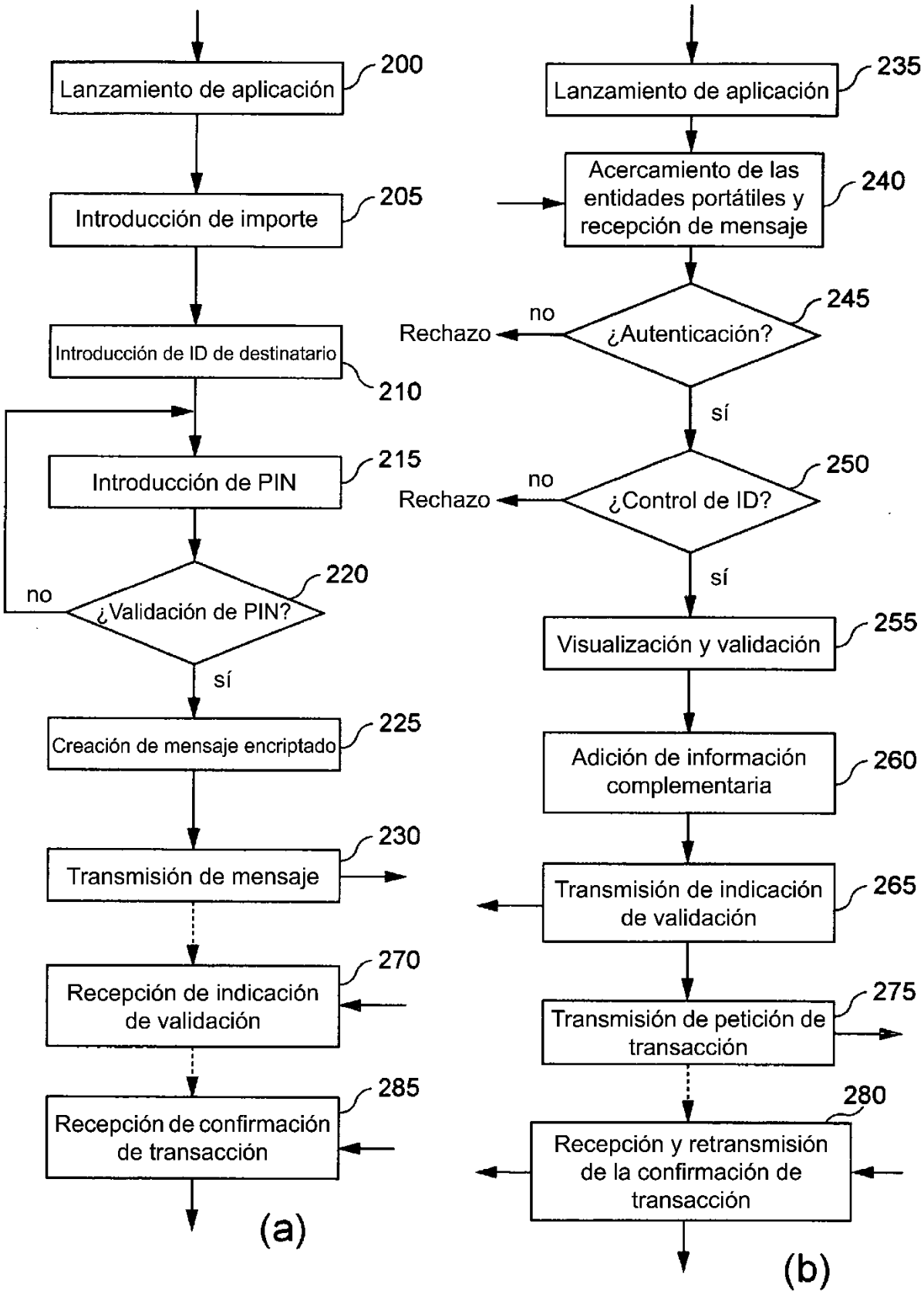
Lanzamiento de aplicación
200
Introducción de importe
205
Introducción de ID de destinatario
210
Introducción de PIN
215
¿Validación de PIN?
220
no
sí
Creación de mensaje encriptado
225
Transmisión de mensaje
230
Recepción de indicación de validación
270
Recepción de confirmación de transacción
285
(a)
Lanzamiento de aplicación
235
Acercamiento de las entidades portátiles y recepción de mensaje
240
¿Autenticación?
245
no
Rechazo
sí
¿Control de ID?
250
no
Rechazo
sí
Visualización y validación
255
Adición de información complementaria
260
Transmisión de indicación de validación
265
Transmisión de petición de transacción
275
Recepción y retransmisión de la confirmación de transacción
280
(b)

Fig. 2

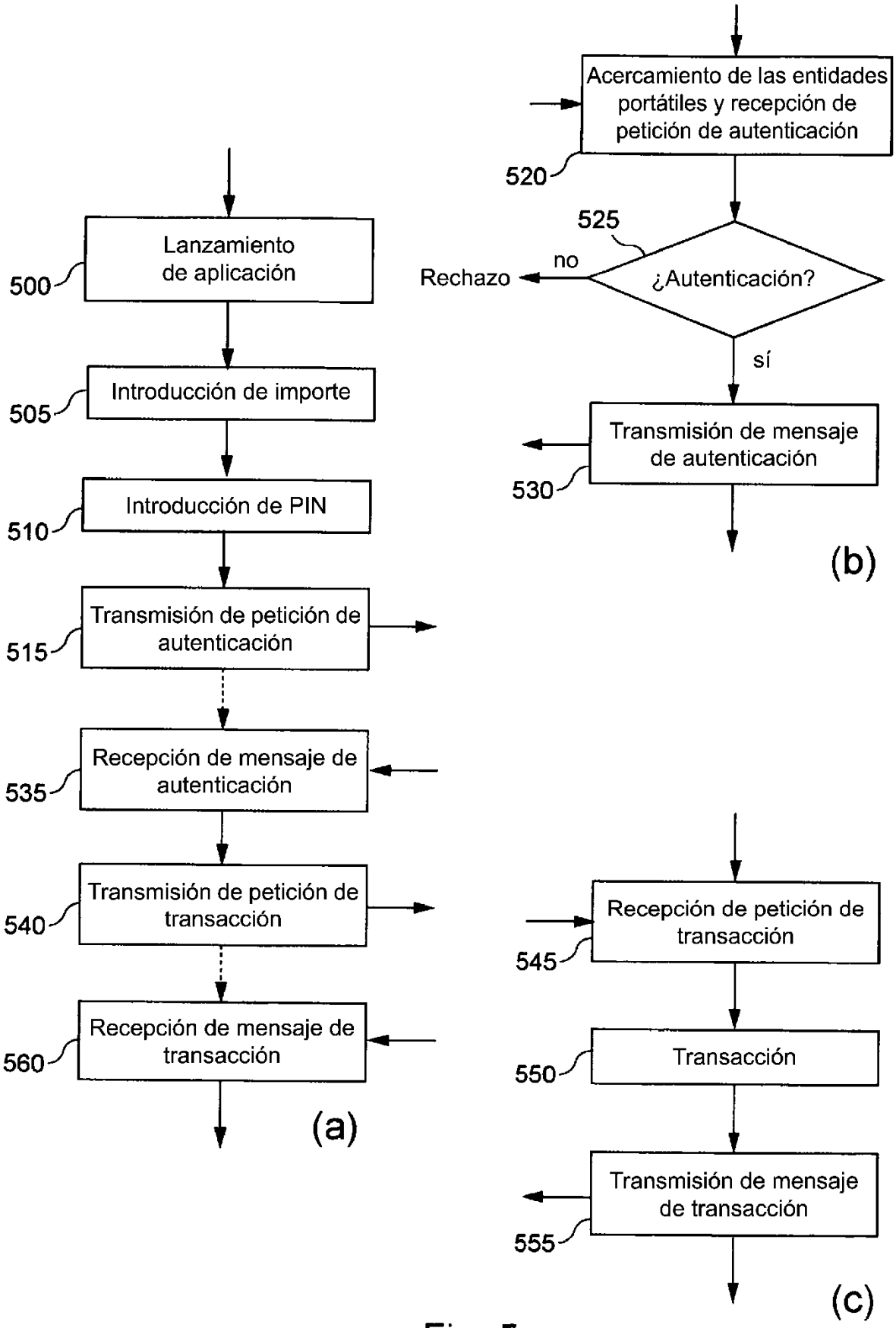
Lanzamiento de aplicación
500
Introducción de importe
505
Introducción de PIN
510
Transmisión de petición de autenticación
515
Recepción de mensaje de autenticación
535
Transmisión de petición de transacción
540
Recepción de mensaje de transacción
560
(a)
Acercamiento de las entidades portátiles y recepción de petición de autenticación
520
525
¿Autenticación?
no
Rechazo
sí
Transmisión de mensaje de autenticación
530
(b)
Recepción de petición de transacción
545
Transacción
550
Transmisión de mensaje de transacción
555
(c)

Fig. 5