

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 865 380**

51 Int. Cl.:

**G06Q 20/02** (2012.01)

**G06Q 20/20** (2012.01)

**G06Q 20/32** (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **08.07.2014 E 14176043 (9)**

97 Fecha y número de publicación de la concesión europea: **17.02.2021 EP 2824625**

54 Título: **Método de realización de una transacción, terminal y programa informático correspondiente**

30 Prioridad:

**11.07.2013 FR 1356839**

**20.12.2013 FR 1363300**

45 Fecha de publicación y mención en BOPI de la  
traducción de la patente:  
**15.10.2021**

73 Titular/es:

**INGENICO GROUP (100.0%)  
28-32, Boulevard de Grenelle  
75015 Paris, FR**

72 Inventor/es:

**LEGER, MICHEL**

74 Agente/Representante:

**ELZABURU, S.L.P**

ES 2 865 380 T3

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

## DESCRIPCIÓN

Método de realización de una transacción, terminal y programa informático correspondiente

### 1. Campo de la invención

La invención se refiere al campo de los instrumentos de pago. Más particularmente, la invención se refiere a un nuevo instrumento de pago.

### 2. Estado de la técnica

La historia del pago es relativamente antigua. Desde que existe el dinero, cómo puede ser intercambiado para realizar un pago ha sido una preocupación crucial. Se crearon de este modo muchos instrumentos de pago: dinero fiduciario, en primer lugar, y después, instrumentos de cambio y crédito, tales como letras de cambio, cheques. Más recientemente, la tarjeta bancaria ha revolucionado gradualmente la forma en que se realizan los pagos. Esta revolución se debe principalmente a las capacidades de miniaturización y procesamiento de los procesadores.

De hecho, se ha pasado del uso de tarjetas simples de banda magnética, que contienen datos, pero no pueden procesar información, a tarjetas inteligentes, que comprenden un procesador y una memoria.

Por el contrario, los principios de pago, en sí mismos, han cambiado relativamente poco en comparación con la evolución de las técnicas utilizadas para realizar estos pagos. Por lo tanto, por ejemplo, en relación con el pago mediante tarjeta bancaria, el usuario dispone de una tarjeta y el comerciante dispone de un terminal de pago que se utiliza para leer datos de la tarjeta y verificar la identidad del portador de la tarjeta (o, como mínimo, que el portador de la tarjeta conoce la información que permite validar el pago). Aunque las técnicas de identificación, reconocimiento y detección de tarjeta han evolucionado, sigue siendo necesario que el usuario disponga de un identificador bancario que presenta al comerciante, estando a cargo de este último el disponer de las infraestructuras necesarias para la autenticación del usuario y la aceptación de las transacciones por parte de los servicios bancarios adecuados. Sin embargo, estas infraestructuras, por un lado, son caras, y por otro, incluyen datos extremadamente confidenciales, tales como, por ejemplo, identificadores bancarios "de todos los usuarios de este terminal", cuya violación de la privacidad puede tener consecuencias mucho más graves que las que están relacionados con el uso no autorizado de datos bancarios de solo un cliente (por ejemplo, un robo de número de tarjeta bancaria). En un intento por protegerse de violaciones de la privacidad o robos a nivel comercial, los terminales utilizados por estos son cada vez más sofisticados y están cubiertos con medidas de seguridad. Sin embargo, aunque estas medidas son efectivas, el hecho es que todavía existen fallos de seguridad.

Por lo tanto, es necesario proponer soluciones que permitan resolver estos problemas vinculados al riesgo de violación de la privacidad de los datos del comerciante.

El documento US 2002/116329 A1 se refiere a un sistema para que un terminal inalámbrico realice transacciones de débito / crédito para una cuenta. Según el documento US 2002/116329 A1, el sistema afecta a tres partes: un comerciante, un cliente y una entidad de autorización (servidor de autorización). Ninguno de los procedimientos dados a conocer por el documento US 2002/116329 A1 explica cómo obtener el identificador de comerciante mediante un código de barras bidimensional, obtenido por el terminal del usuario.

El documento US 2012/136798 A1 se refiere a un sistema de transacciones de pago, en el que la información bancaria del usuario es transmitida a un servidor en lugar de a un comerciante. En efecto, el documento US 2012/136798 A1 da a conocer que el servidor transmite el número de tarjeta bancaria al comerciante para procesar el pedido, y no resuelve los problemas relacionados con el riesgo de violación de la privacidad de los datos del cliente.

El documento EP 2 128 809 A1 se refiere a un método para generar una transacción entre un terminal de un comprador (segunda entidad) y el terminal de un comerciante (primera entidad) bajo el control de una tercera entidad (servidor). La segunda entidad (que corresponde al terminal del comprador) contacta con la primera entidad (el terminal de pago del comerciante o del proveedor de servicios). La segunda entidad transmite un mensaje a la primera entidad. La segunda entidad recibe el código de identificación de la primera entidad a través de una comunicación unidireccional y extrae la información relativa a la transacción a realizar a partir del código. Por el contrario, el documento EP 2 128 809 A1 necesita la transmisión de un mensaje y, por lo tanto, el intercambio bidireccional de información.

### 3. Compendio de la invención

La invención no presenta estos inconvenientes de las soluciones de la técnica anterior. La invención está definida por el objeto de las reivindicaciones.

De este modo, la técnica propuesta permite gestionar la transacción directamente dentro del terminal del cliente. Por lo tanto, no es necesario proporcionar al comerciante los identificadores privados del usuario. Puesto que estos no son proporcionados al comerciante, no hay riesgo de que una violación de la privacidad del dispositivo del comerciante pueda llevar a una violación de la privacidad de los datos del cliente. Por el contrario, no hay riesgo de que el dispositivo del cliente ponga en peligro al comerciante.

Por lo tanto, a diferencia de otras técnicas, la técnica de la invención garantiza que la transacción (por lo tanto, el pago) se lleva a cabo en el modo de "tarjeta presente", es decir como si una tarjeta bancaria hubiese sido introducida en el terminal del comerciante.

5 Según una implementación, las diferentes etapas de los procedimientos según la invención, son implementadas mediante una o más rutinas o programas informáticos, que comprenden instrucciones de software destinadas a ser ejecutadas por un procesador de datos de un módulo de repetición según la invención, y que está diseñado para controlar la ejecución de las diferentes etapas de los procedimientos.

10 En consecuencia, la invención también está dirigida a un programa, susceptible de ser ejecutado por un ordenador o por un procesador de datos, comprendiendo este programa instrucciones para controlar la ejecución de las etapas de un procedimiento tal como el mencionado anteriormente.

Este programa puede utilizar cualquier lenguaje de programación, y estar en forma de código fuente, código objeto, o código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada, o en cualquier otra forma deseable.

15 La invención también está dirigida a un soporte de información legible mediante un procesador de datos y que comprende instrucciones de un programa tal como el mencionado anteriormente.

El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede comprender un medio de almacenamiento, tal como una ROM, por ejemplo, un CD ROM o una ROM de circuito microelectrónico, o incluso un medio de registro magnético, por ejemplo, un disquete o un disco duro.

20 Por otro lado, el soporte de información puede ser un soporte transmisible, tal como una señal eléctrica u óptica, que puede ser transmitida a través de un cable eléctrico u óptico, por radio o por otros medios. En particular, el programa según la invención puede ser descargado de una red de tipo Internet.

Alternativamente, el soporte de información puede ser un circuito integrado en el que está incorporado el programa, estando el circuito adaptado para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

25 Según una realización, la invención se implementa mediante componentes de software y/o hardware. Desde esta perspectiva, el término "módulo" puede corresponder en este documento tanto a un componente de software, como a un componente de hardware o a un conjunto de componentes de hardware y software.

30 Un componente de software corresponde a uno o varios programas informáticos, una o varias subrutinas de un programa, o, de manera más general, a cualquier elemento de un programa o de un software capaz de implementar una función o un conjunto de funciones, tal como se describe a continuación para el módulo relevante. Dicho componente de un software es ejecutado por un procesador de datos de una entidad física (terminal, servidor, pasarela, encaminador, etc.) y es capaz de acceder a los recursos materiales de esta entidad física (memorias, soportes de grabación, bus de comunicación, tarjetas electrónicas de entradas / salidas, interfaces de usuario, etc.).

35 Asimismo, un componente de hardware corresponde a cualquier elemento de un conjunto de hardware (o hardware) capaz de implementar una función o un conjunto de funciones, tal como se describe a continuación para el módulo en cuestión. Puede ser un componente programable de hardware o con un procesador integrado para la ejecución de software, por ejemplo, un circuito integrado, una tarjeta inteligente, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microprograma (firmware), etc.

Cada componente del sistema descrito anteriormente implementa, obviamente, sus propios módulos de software.

40 Las diversas realizaciones mencionadas anteriormente pueden ser combinadas entre sí para la implementación de la invención.

#### 4. Lista de las figuras

Otras características y ventajas de la invención aparecerán más claramente con la lectura de la siguiente descripción de una realización y de los dibujos adjuntos, entre los cuales:

- la figura 1 presenta un diagrama de bloques de la técnica propuesta;
- 45 — la figura 2 describe un dispositivo para implementar la técnica propuesta;
- la figura 3 describe un servidor de gestión de transacciones.

## 5. Descripción

### 5.1. Recordatorio del principio general de la invención

El principio general de la invención se basa en un cambio de paradigma con respecto al pago. Más particularmente, el pago con tarjeta bancaria de chip (o tarjeta sin contacto, o mediante un teléfono con función de pago), tal como se realiza habitualmente, asume que el comerciante al que se le debe realizar el pago tiene un equipo específico para que pueda ser realizado. Esto supone, asimismo, que el cliente proporciona un identificador (a través de una tarjeta bancaria [de chip, de banda magnética, sin contacto], de un terminal) y que el comerciante se encarga de llevar a cabo una autenticación del cliente en función del material que le presenta el cliente.

En la técnica propuesta, se utiliza un terminal en posesión del cliente (terminal que puede ser un teléfono, un teléfono inteligente, un PDA, una tableta, un ordenador portátil o cualquier otro dispositivo capaz de gestionar una transacción) para generar y transmitir la transacción financiera a un servidor de gestión de transacciones (tal como un servidor bancario o un servidor del proveedor de servicios de pago, por ejemplo). El comerciante ya no utiliza las coordenadas del cliente. Por el contrario, el cliente utiliza las coordenadas del comerciante.

Esto presenta numerosas ventajas, una de las cuales es la garantía de que los datos del cliente no serán robados ni se violará su privacidad. En efecto, en la medida en que se considera que los datos del comerciante pueden ser datos públicos y que la transacción financiera es una operación destinada al comerciante (operación de crédito para el comerciante), no es necesario que el comerciante dé su conformidad para recibir un crédito del usuario. Por consiguiente, los datos del comerciante no se ven comprometidos. Además, puesto que el cliente no proporciona sus propios datos al comerciante, el método propuesto garantiza que los datos del cliente no serán explotados contra su consentimiento (por robo, robo de identidad, etc.). Por lo tanto, ni el comerciante ni el cliente han proporcionado datos confidenciales. Por otra parte, la técnica propuesta tiene la ventaja de utilizar la infraestructura existente a nivel del comerciante. De hecho, este último ya dispone, por regla general, de un terminal que permite recibir datos de uno o varios servidores bancarios. La ventaja del método propuesto es que el terminal del comerciante ya no es responsable de la construcción de la transacción, y que se contenta con recibir datos de un servidor (y/o de otro terminal).

A continuación, se presenta un ejemplo de realización de la invención en el que se implementa el principio presentado. Se comprende que la implementación del principio propuesto no es limitativa y que cualquier otro método que implemente este principio cae dentro del alcance de la presente invención.

### 5.2. Descripción de un ejemplo de realización

En este ejemplo de realización, se describe un procedimiento que permite a un cliente realizar una transacción financiera (por ejemplo, una compra) con un comerciante. El sistema descrito tiene la enorme ventaja, por un lado, de beneficiarse de las infraestructuras existentes y, por otro lado, de garantizar que la operación se lleva a cabo en el modo de "tarjeta presente", puesto que la técnica, en este ejemplo de realización, requiere la entrada, por parte del usuario, de un dato que representa un identificador personal de seguridad (por ejemplo, un código PIN). Este código PIN está asociado, a voluntad, ya sea con una tarjeta de pago, disociada del terminal del usuario, o directamente al propio terminal del usuario (cuando este terminal comprende, por ejemplo, una tarjeta de pago o un módulo de pago integrado en el terminal).

En este ejemplo de realización, el procedimiento comprende, dentro de un terminal propiedad de un usuario (TU) que desea realizar una transacción financiera con un comerciante (que tiene un dispositivo que puede ser comparado con un terminal de comerciante (TC), que comprende funciones posiblemente reducidas):

- una etapa de recepción (100) un identificador de comerciante (IdM);
- una etapa de obtener la recepción (200) de un dato representativo de una monto de transacción (Px);
- una etapa de generación (300), por parte del terminal del usuario, en beneficio de dicho comerciante, de una transacción (TF) destinada a un servidor de gestión de transacciones (Srv);
- una etapa de transmisión (400) de dicha transacción (TF) a dicho servidor de transacciones (Srv).

La recepción del identificador del comerciante y del identificador del precio es posterior bien a una transmisión directa de estos datos desde el terminal del comerciante al terminal, o bien a una transmisión indirecta, involucrando al servidor de gestión de transacciones. En este caso, es el servidor de gestión de transacciones el que transmite directamente estos datos al terminal de usuario TU. En este segundo escenario, el usuario ya está conectado al servidor de gestión de transacciones y valida la transacción con el mismo, por ejemplo, después de la introducción de un código PIN por parte del usuario: la etapa de generación de la transacción comprende, por lo tanto, la introducción de un código PIN por parte del usuario, tal como se explicó anteriormente) y la transacción es transmitida al servidor. Por lo tanto, la transacción (TF) que se transmite al servidor puede ser, en este ejemplo de realización, solamente una confirmación (que es, por ejemplo, una confirmación en forma de un hash de transacción, estando construido dicho hash a partir del identificador del comerciante, del precio y del identificador del cliente).

De este modo, el comerciante proporciona de alguna manera un identificador “público” con el que desea que se realice la transacción de la que es responsable el terminal del cliente. En una realización no cubierta por la invención reivindicada, el identificador proporcionado por el comerciante solo permite realizar transacciones de crédito a una cuenta abierta para el comerciante.

- 5 Una vez que la transacción ha sido transmitida al servidor de gestión de transacciones (servidor bancario o servidor del proveedor de servicios de pago), es validada (500). Esta validación puede adoptar varias formas distintas: una transmisión (501) al terminal del comerciante (TC), que se retransmite al terminal del cliente (502). También puede ser una transmisión directa, por parte del servidor de gestión de transacciones, a los dos terminales (esto hace que sea posible evitar sospechas de fraude que pudieran pesar sobre la transacción): a continuación, el servidor de gestión de transacciones realiza la función de un tercero de confianza para la realización de la transacción. Por supuesto, esta validación no está limitada a estas únicas etapas de transmisión a los terminales, tal como se explicará a continuación.

En función de las realizaciones de la técnica propuesta, la recepción del identificador proveniente del comerciante puede comprender una (o incluso varias) de las fases siguientes:

- 15 – una fase de emparejamiento, por ejemplo, utilizando el protocolo bluetooth, que comprende obtener un dato representativo del identificador del comerciante;
- una fase de lectura de un código de barras, por ejemplo, un código de barras bidimensional, que comprende un dato representativo del identificador del comerciante;
- 20 – una etapa de recepción, proveniente de un servidor remoto, de un dato representativo del identificador del comerciante: puede tratarse, por ejemplo, de un servidor vinculado a una franquicia o un servidor de gestión de transacciones;
- en un ejemplo de realización particular, el identificador se obtiene descifrando un código de barras, por ejemplo, un código de barras bidimensional, (o emparejamiento bluetooth) entregando una dirección desde la cual el terminal del usuario puede obtener un identificador del comerciante;
- 25 – la recepción de este identificador también puede ser realizada, asimismo, mediante una tarjeta sin contacto que, cuando es aproximada al terminal del usuario, entrega el identificador del comerciante. La recepción de este identificador también puede ser realizada por un terminal móvil en posesión del propio comerciante que intercambia datos con el terminal del usuario.

En función de las realizaciones de la técnica propuesta, la obtención de un dato representativo del monto de una transacción puede incluir una (o incluso varias) de las fases siguientes:

- 30 – una introducción por parte del propio usuario del monto de la transacción;
- una fase de emparejamiento, por ejemplo, usando el protocolo bluetooth, que comprende la obtención de un dato representativo de un monto de transacción;
- una etapa de lectura de un código de barras, por ejemplo, un código de barras bidimensional, que comprende un monto de transacción;
- 35 – una etapa de recepción, proveniente de un servidor remoto, de un dato representativo de un monto de transacción: se puede tratar, por ejemplo, de un servidor vinculado a una franquicia o un servidor de gestión de transacciones;
- en un ejemplo de realización particular, el identificador se obtiene descifrando un código de barras, por ejemplo, un código de barras bidimensional, (o emparejamiento de bluetooth) la entrega de una dirección desde la cual el terminal del usuario puede obtener un monto de transacción;
- 40

En función de las realizaciones, las etapas de recepción anteriores pueden ser combinadas en una sola y misma etapa.

- 45 Cuando los datos relativos al comerciante y el precio están disponibles para el terminal, este último genera la transacción. Para ello, son posibles varias posibilidades. La primera consiste en generar, con la ayuda de una aplicación particular, un registro específico que comprende, por un lado, los datos obtenidos previamente y un identificador del usuario. Por cierto, este registro se puede cifrar para garantizar la integridad de los datos que se transportarán.

- 50 Durante esta generación, se requiere el código PIN del usuario, por medio de una aplicación específica de introducción de código PIN, que requiere una acción de entrada por parte del usuario. Esto se puede hacer usando un teclado físico o un teclado táctil. Por lo tanto, la transacción se realiza en modo de “tarjeta presente”.

La siguiente etapa consiste en transmitir, desde del terminal del cliente, el registro a un servidor transaccional (servidor de gestión de transacciones). El servidor transaccional (que es ventajosamente un servidor de un proveedor de servicios de pago o un servidor bancario) valida, por lo tanto, la transacción.

5 La validación de la transacción puede comprender un cierto número de etapas, entre las que se encuentran una etapa de débito de una cuenta de un usuario y una etapa de crédito de una cuenta del comerciante.

En un ejemplo de realización específico, además de estas dos etapas (débito / crédito), la validación de la transacción por parte del servidor de gestión de transacciones comprende previamente:

- 10 – una etapa de transmisión, a un terminal en posesión del comerciante, de como mínimo un dato representativo de la transacción, con el fin de que este pueda garantizar el monto de la transacción, y validarlo (en este caso, hay una etapa de validación por parte del comerciante);
- una etapa de recepción, desde un terminal en posesión del usuario cliente, de un dato representativo de una validación de la transacción por parte de dicho comerciante.

Según las realizaciones, el dato representativo de la transacción recibido por el comerciante puede comprender:

- un dato representativo del monto de la transacción;
- 15 – un dato representativo del terminal utilizado por dicho usuario para realizar la transacción, por ejemplo, la marca del terminal;
- un dato representativo del establecimiento de pago seleccionado por el usuario para realizar la transacción en beneficio del comerciante.

20 Cuando el terminal del comerciante (TC) valida la transacción, por ejemplo, pulsando una tecla de validación del terminal del comerciante, el terminal del cliente (TU) recibe, proveniente del terminal del comerciante (TC) (por ejemplo, si una conexión bluetooth ha sido construida) o del servidor transaccional (Serv), un dato representativo de la validación de la transacción. Al mismo tiempo, el servidor transaccional realiza las operaciones de débito y de crédito necesarias.

### 5.3. Otras características y ventajas

25 En relación con la figura 2, se describe un terminal de usuario implementado para realizar las transacciones según el procedimiento descrito previamente.

Por ejemplo, el terminal comprende una memoria 21 constituida por una memoria intermedia, una unidad de procesamiento 22, equipada, por ejemplo, con un microprocesador, y controlada por el programa informático 23, que pone en práctica un procedimiento de construcción de datos representativos de transacción.

30 En la inicialización, las instrucciones de código del programa informático 23 son cargadas, por ejemplo, en una memoria antes de ser ejecutadas por el procesador de la unidad de procesamiento 22. La unidad de procesamiento 22 recibe, como mínimo, en la entrada un dato representativo de un identificador de un comerciante y un dato representativo de un monto de transacción. El microprocesador de la unidad de procesamiento 22 implementa las etapas del procedimiento de construcción de datos representativos de transacciones, según las instrucciones del programa informático 23 para realizar una validación de transacción.

35 Para ello, el dispositivo comprende, además de la memoria intermedia 21, medios de comunicación, tales como módulos de comunicación de red, medios de transmisión de datos posiblemente un procesador de cifrado.

40 En un ejemplo de realización particular de la invención, el terminal de usuario, que puede ser un teléfono inteligente, una tableta, un ordenador portátil o un PDA, integra medios de gestión de transacciones tales como los descritos anteriormente. Estos medios pueden tener la forma de un procesador particular implementado dentro del terminal, siendo dicho procesador un procesador seguro. Según un ejemplo de realización particular, este terminal implementa una aplicación particular que se encarga de gestionar las transacciones, siendo esta aplicación proporcionada por ejemplo por el fabricante del procesador en cuestión para permitir el uso de dicho procesador. Para ello, el procesador incluye medios de identificación únicos. Estos medios de identificación únicos permiten garantizar la autenticidad del

45 procesador.  
En otro ejemplo de realización, la aplicación de gestión instalada en el terminal comprende asimismo identificadores únicos que permiten garantizar la autenticidad de la aplicación o garantizar la identificación del portador del terminal, o ambos.

#### 5.4. Generación de datos de facturación

La técnica descrita se refiere asimismo a la generación y representación de datos destinados al terminal del usuario (identificador del comerciante e identificador del precio). Tal como se explicó anteriormente, esta generación y esta representación pueden formar parte de un pago físico realizado en un comerciante físico.

- 5 Los datos se pueden representar, por ejemplo, en forma de un código bidimensional, tal como un código QR. Los datos también se pueden representar mediante otros tipos de código.

Más particularmente en un ejemplo de realización, los datos se imprimen en papel, por ejemplo, mediante un terminal disponible para el comerciante (terminal de pago que dispone de una impresora, por ejemplo). A continuación, la cámara del terminal del usuario lee estos datos. Son decodificados y, a continuación, interpretados para generar la transacción en beneficio del comerciante, tal como se ha descrito anteriormente.

En otro ejemplo de realización, se muestran los datos, todavía en la forma de un código de dos dimensiones, en una pantalla de un terminal a disposición del comerciante (por ejemplo, el terminal de pago del comerciante, o una caja registradora inteligente). A continuación, la cámara del terminal del usuario lee estos datos. Son decodificados y, a continuación, interpretados para generar la transacción en beneficio del comerciante, tal como se ha descrito anteriormente.

Según las circunstancias y en función de los parámetros de implementación, la obtención de datos se puede realizar en dos etapas: la primera, para la obtención del identificador del comerciante, la segunda, para la obtención del monto de la transacción. Estas dos etapas también se pueden fusionar en una y la misma etapa de obtención, tal como se explicó anteriormente.

#### 20 5.5. Caso de uso

La técnica descrita se puede aplicar a numerosas situaciones diferentes de la vida cotidiana. Permite simplificar las relaciones entre cliente y consumidor, garantizando al mismo tiempo un intercambio de datos mínimo.

Por ejemplo, el método de la invención puede ser aplicado al pago en línea de bienes o servicios a partir de un ordenador: en lugar de solicitar el pago con tarjeta "clásica" del banco, que necesita la introducción de un número de tarjeta bancaria, de una fecha de validez, el sitio de comercio en línea puede mostrar un código QR en pantalla, válido durante un período de tiempo determinado, para que el terminal del usuario tenga tiempo de obtener este código. El resto del pago se realiza de la misma manera que se ha descrito anteriormente. El comerciante recibe una notificación de pago de su banco o de un proveedor de servicios de pago.

Esta técnica puede ser aplicada, asimismo, durante la difusión de programas audiovisuales en televisión: por ejemplo, durante una página de publicidad, se muestra un código QR en la pantalla de televisión, cuando se visualiza el anuncio: una obtención de este código puede ser llevada a cabo por el terminal del usuario para obtener el bien o el servicio en relación con este anuncio. En este caso, la confirmación de pago recibida por el anunciante puede ir seguida de una conexión al sitio de este último para que el usuario pueda introducir información adicional, tal como una dirección de entrega. En este caso, el servidor intermedio (o el servidor del proveedor de pago) es el encargado de transmitir, al terminal del usuario, una solicitud para obtener datos complementarios provenientes del comerciante.

Esta técnica puede ser puesta en práctica, incluso, de manera estática, para permitir la compra directa de un producto o servicio, sin necesidad de intervención del comerciante: para ello, es suficiente mostrar un código QR correspondiente a un producto (por ejemplo, un menú en una tienda de sándwiches). El cliente que desea tomar este menú reconoce directamente el código QR. Estos datos son decodificados y después interpretados para generar la transacción en beneficio del comerciante, tal como se ha descrito anteriormente. Además, el dato representativo del identificador del usuario puede ser completado proporcionando el nombre del usuario, con el fin de que el comerciante (por ejemplo, la sandwichería) pueda conocer la identidad de este último. De manera alternativa, el nombre del usuario también puede ser transmitido por el proveedor de servicios de pago al que se transmite la transacción.

Este tipo de caso de uso se puede aplicar a muchas otras situaciones, tales como el pago en un automóvil, el pago de combustible en una gasolinera, el pago de bebidas dulces y otro sándwich en una máquina expendedora de productos alimenticios, la obtención de los datos a partir de un cartel publicitario, de una pantalla de publicidad en un cine de barrio (por ejemplo, para pagar un helado o dulces, o aún mejor, para obtener bienes físicos de un comerciante al lado del cine - una comida, por ejemplo, en un restaurante). Estos casos de uso pueden corresponder a situaciones en las que el comerciante no se encuentra físicamente presente en el momento de la implementación de la transacción desde el terminal del usuario.

Con el fin de reforzar la seguridad de dichas operaciones, que pueden ser llevadas a cabo sin la presencia física de un comerciante, después de obtener los datos de identificación de comerciante y de identificación del precio, el procedimiento comprende una etapa de emisión, hacia el servidor de gestión (o hacia otro servidor para recoger productos y servicios asociados a comerciantes), de datos obtenidos mediante el código QR escaneado. Estos datos, enviados al servidor de gestión, pueden ser complementados con datos de ubicación disponibles en el terminal (por ejemplo, mediante un GPS) y con una identificación de oferta. Los datos de GPS permiten localizar la oferta mientras

que la identificación de la oferta, que también es un dato del código QR, permite conocer el número de la oferta asociada a este comerciante.

En una realización no cubierta por la invención reivindicada, esta etapa se combina con la etapa de transmisión (400) la transacción (TF) a un servidor de gestión de transacciones (Srv).

- 5 Al recibir estos datos, y antes de la implementación de la transacción, el servidor de gestión verifica que los datos que se le transmiten corresponden realmente a una oferta válida para pagar bienes y/o servicios. En esta realización no cubierta por la invención reivindicada, esto requiere que los comerciantes que deseen realizar ofertas del tipo descrito anteriormente tengan la obligación, a fin de que estas ofertas sean tenidas en cuenta, de declararlas al servidor de gestión (o a otro servidor de recogida de productos y servicios asociados con comerciantes) para que no se consideren sin validez. La validez de la oferta puede ser probada utilizando la ubicación (GPS o red móvil) del terminal. En este caso, la base de datos también incluye una identificación del lugar de la oferta. Para que sea válida, la ubicación registrada en la base de datos debe corresponder sustancialmente a la ubicación del terminal del usuario. El principio asociado con la identificación de la oferta es el mismo. Cuando se tienen en cuenta estos datos, la base de datos incluye un precio asociado a la oferta identificada. En este caso, el precio obtenido del código QR es comparado con el precio registrado en la base de datos. Esto garantiza que no se producirá ningún fraude en el precio.

En caso de validez de la oferta, la transacción continúa, tal como se ha descrito anteriormente. En caso de caducidad de la oferta, la transacción es anulada.

- 20 Según una característica particular, la invención también se refiere a un código bidimensional, llamado código QR. Según la invención, dicho código QR se diferencia del estado de la técnica en que comprende, por un lado, un identificador de comerciante y, por otro, un identificador relativo a un precio de transacción. Según una característica particular en función de las realizaciones, dicho código también comprende un identificador de producto y/o servicio. Dicho código también puede incluir una ubicación para la venta de producto o de servicio. En una versión alternativa, dicho código también puede incluir una dirección a la que conectarse para obtener dichos datos.

#### 5.6. Servidor de gestión de transacciones

- 25 En función de las realizaciones, el servidor de gestión de transacciones (también llamado servidor transaccional) es considerado como un tercero de confianza para llevar a cabo la transacción.

Más particularmente, el servidor de gestión de transacciones realiza las etapas siguientes:

- *recibe* las transacciones provenientes de los terminales de usuario (o hash de transacciones en función de las realizaciones, véase lo anterior);
- 30 – *controla* la validez de las transacciones recibidas (validez formal, relativa a la constitución de la transacción, la conformidad de las claves de cifrado utilizadas, etc.): esta etapa consiste, por ejemplo, en descifrar la transacción y/o verificar que el contenido de esta corresponde a expectativas formales (longitud de los campos, modo de codificación de datos); el descifrado puede consistir en que se pueda realizar utilizando una clave pública correspondiente al usuario o una clave privada adecuada para el servidor;
- 35 – *opcionalmente, verifica* las autorizaciones de pago (o delega esta verificación a otro servidor). La obtención de dicha autorización hace que sea posible garantizar que el usuario tiene la suma necesaria para el pago (esta verificación solo puede ser llevada a cabo por encima de una cierta cantidad de pago, por ejemplo 150,00 o 300,00 €) y que los datos utilizados para el pago no son robados (es decir, que los datos no han sido colocados en estado de oposición);
- 40 – *realiza* (o hace que se realicen) operaciones de débito y crédito en las cuentas bancarias de usuarios y comerciantes en función de sus respectivos identificadores;
- *transmite* al usuario y/o al comerciante, aserciones de validación de transacciones, ya sea cuando se obtienen las autorizaciones necesarias para realizar las transacciones, o sin estas autorizaciones si no son necesarias.

- 45 En función de las realizaciones, el servidor de gestión de transacciones también puede soportar otros aspectos relacionados. De este modo, por ejemplo, el servidor de gestión de transacciones también puede implementar las etapas siguientes:

- *se comunica* con el comerciante para proporcionar al este el nombre del usuario que realiza una transacción determinada; esto se hace en forma de una etapa de transmisión del nombre del usuario, por ejemplo, al mismo tiempo que se transmite la afirmación de validación de la transacción;
- 50 – *recibe* del comerciante, después de la validación de la transacción, una dirección (por ejemplo, una dirección de tipo URL), con la que el usuario se debe conectar para proporcionar al comerciante datos complementarios;



- *comprueba* la validez de una oferta, en una base de datos de ofertas válidas accesibles desde el servidor, o desde uno o varios servidores se enumeran las ofertas válidas, por medio de la recepción y la transmisión de datos (que implican la transmisión del identificador del comerciante, del precio y, opcionalmente, de un identificador de la oferta y/o de una ubicación del terminal del usuario);

- 5     – *transmite* al terminal del usuario datos provenientes del comerciante.

En relación con la figura 3, se describe un servidor de gestión implementado para realizar las transacciones, desde el punto de vista del servidor, según el procedimiento descrito anteriormente.

- 10    Por ejemplo, el servidor comprende una memoria 31 que consiste en una memoria intermedia, una unidad de procesamiento 32, equipada, por ejemplo, con un microprocesador, y controlada por el programa informático 33, que pone en práctica un procedimiento de construcción de datos representativos de la transacción.

- 15    En la inicialización, las instrucciones de código del programa informático 33 son cargadas, por ejemplo, en una memoria antes de ser ejecutadas por el procesador de la unidad de procesamiento 32. La unidad de procesamiento 32 recibe, en la entrada, como mínimo, un dato representativo de un identificador de un comerciante y un dato representativo de un monto de transacción y un identificador de usuario. El microprocesador de la unidad de procesamiento 32 implementa las etapas del procedimiento del procesamiento de datos representativos de transacciones, según las instrucciones del programa informático 33 para realizar una validación de transacción (control de validez, verificación de las autorizaciones, operaciones de débitos y de crédito, información de los intervinientes).

Para ello, el servidor comprende, además de la memoria intermedia 31, medios de comunicación, tales como módulos de comunicación de red, medios de transmisión de datos y, posiblemente, un procesador de cifrado.

- 20    Estos medios se pueden presentar en forma de un procesador particular implementado dentro del servidor, siendo dicho procesador un procesador seguro. Según un ejemplo de realización particular, este servidor implementa una aplicación particular que se encarga de realizar las transacciones, siendo proporcionada esta aplicación, por ejemplo, por el fabricante del procesador en cuestión, para permitir el uso de dicho procesador. Para ello, el procesador incluye medios de identificación únicos. Estos medios de identificación únicos garantizan la autenticidad del procesador.

- 25    Por otra parte, el servidor comprende, además, los medios para identificar y validar las ofertas de productos y de servicios. Estos medios también se presentan como interfaces de comunicación que permiten intercambiar datos a través de redes de comunicación, medios para consultar y actualizar la base de datos, medios para comparar datos de ubicación.

## REIVINDICACIONES

1. Procedimiento de realización de una transacción financiera con un terminal de un comerciante (TC), procedimiento implementado dentro de un terminal de un usuario que desea realizar una transacción con un comerciante, siendo realizado el procedimiento por el terminal de un usuario, y estando caracterizado por que comprende:

- 5 - una etapa de recepción (100) de un identificador de comerciante (IdM):
    - mediante la lectura de un código de barras por medio de una cámara del terminal de un usuario; o
    - mediante la recepción de un mensaje a través de una interfaz Bluetooth del terminal de un usuario; o
    - mediante la recepción de un mensaje a través de una interfaz sin contacto del terminal de un usuario; o
    - la recepción, desde un servidor remoto, de un dato que representa el identificador del comerciante;
  - 10 - una etapa de recepción (200) de un dato que representa un monto de transacción (Px), que comprende:
    - la lectura de un código de barras por medio de una cámara del terminal de un usuario; o
    - la recepción de un mensaje a través de una interfaz Bluetooth del terminal de un usuario; o
    - la recepción, proveniente de un servidor remoto, de un dato que representa un monto de transacción;
  - 15 - una etapa de generación (300) por parte del terminal del usuario, para dicho comerciante de una transacción (TF), que comprende:
    - la obtención de datos de ubicación del terminal de un usuario por medio de un GPS o de una red móvil;
    - la creación de un registro que comprende por un lado dicho identificador de comerciante (IdM), el dato que representa un monto de transacción (Px), un dato que representa un identificador del usuario, los datos de ubicación de dicho terminal de usuario;
  - 20 - una etapa de transmisión (400) de dicha transacción (TF) hacia un servidor de gestión de transacciones (Srv), para realizar la transacción con el terminal del comerciante en una cuenta bancaria del usuario, en el que el servidor de gestión de las transacciones al cual se transmite la transacción verifica la validez de la transacción por medio de una base de datos, mantenida por dicho servidor de gestión de transacciones (Srv), que comprende un dato que representa el monto de transacción y una identificación de una ubicación de venta;
  - 25 - una etapa de recepción de, como mínimo, una afirmación de validación de la transacción transmitida por el servidor de gestión de transacciones (Srv), después de que este haya verificado la validez de la transacción e implementado la transacción.
2. Procedimiento, según la reivindicación 1, caracterizado por que dicha etapa de generación (300) de dicha transacción (TF) comprende una etapa para la introducción, por parte de dicho usuario, como mínimo, de un dato que
- 30 representa un identificador personal de seguridad.
3. Procedimiento, según la reivindicación 1, caracterizado por que dicho procedimiento comprende, posteriormente a dicha etapa de transmisión, una etapa de recepción de un dato que representa una validación de dicha transacción proveniente de un terminal de dicho comerciante (TC).
- 35 4. Procedimiento, según la reivindicación 1, caracterizado por que dicha etapa de recepción (100) de un identificador de comerciante (IdM) comprende una fase de emparejamiento con un terminal de dicho comerciante (TC) que comprende una etapa de obtención de dicho dato que representa el identificador de comerciante (IdM).
5. Procedimiento, según la reivindicación 1, caracterizado por que dicha etapa de generación (300) de una transacción (TF) comprende:
- una etapa de creación del registro que comprende dicho dato representativo de un identificador del usuario;
- 40 - una etapa de cifrado de dicho registro con la ayuda de dicho terminal de dicho usuario, entregando dicha transacción (TF).
6. Dispositivo de realización de una transacción financiera con un terminal de un comerciante (TC), el dispositivo implementado dentro del terminal de un usuario, el dispositivo caracterizado por que comprende:
- como mínimo, una de las siguientes interfaces: una cámara, una interfaz Bluetooth o una interfaz sin contacto;

- medios de recepción (100) de un identificador de comerciante (IdM) mediante:
  - la lectura de un código de barras por medio de la cámara; o
  - la recepción de un mensaje a través de la interfaz Bluetooth del terminal de un usuario; o
  - la recepción de un mensaje a través de la interfaz sin contacto del terminal de un usuario; o
- 5       – la recepción, proveniente de un servidor remoto, de un dato que representa el identificador del comerciante;
- medios de recepción (200) de un dato que representa un monto de transacción (Px) que comprende:
  - la lectura de un código de barras por medio de una cámara del terminal de un usuario; o
  - la recepción de un mensaje a través de una interfaz Bluetooth del terminal de un usuario; o
- 10       – la recepción, proveniente de un servidor remoto, de un dato que representa un monto de transacción;
- medios de generación (300), por parte del terminal del usuario, de una transacción (TF) para dicho comerciante que permite:
  - la obtención de datos de ubicación de dicho terminal de usuario por medio de un GPS o de una red móvil;
  - la creación de un registro que comprende por un lado dicho identificador del comerciante (IdM), el dato que representa un monto de transacción (Px), un dato que representa un identificador del usuario, los datos de ubicación del terminal de un usuario;
- 15
- medios de transmisión (400) de dicha transacción (TF) hacia un servidor de gestión de transacciones (Srv), para realizar la transacción con el terminal del comerciante en una cuenta bancaria del usuario, en el que el servidor de gestión de las transacciones al que se transmite la transacción verifica la validez de la transacción por medio de una base de datos, mantenida por dicho servidor de gestión de transacciones (Srv), que comprende un dato que representa el monto de transacción y una identificación de una ubicación de venta;
- 20
- medios de recepción, como mínimo, de una aserción de validación de la transacción transmitida por el servidor de gestión de transacciones (Srv), después de que este haya verificado la validez de la transacción e implementado la transacción.
- 25       7. Producto de programa informático descargable desde una red de comunicaciones y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador, caracterizado por que comprende instrucciones de código de programa para la ejecución de un procedimiento de realización de transacciones según la reivindicación 1, cuando es ejecutado en un ordenador.

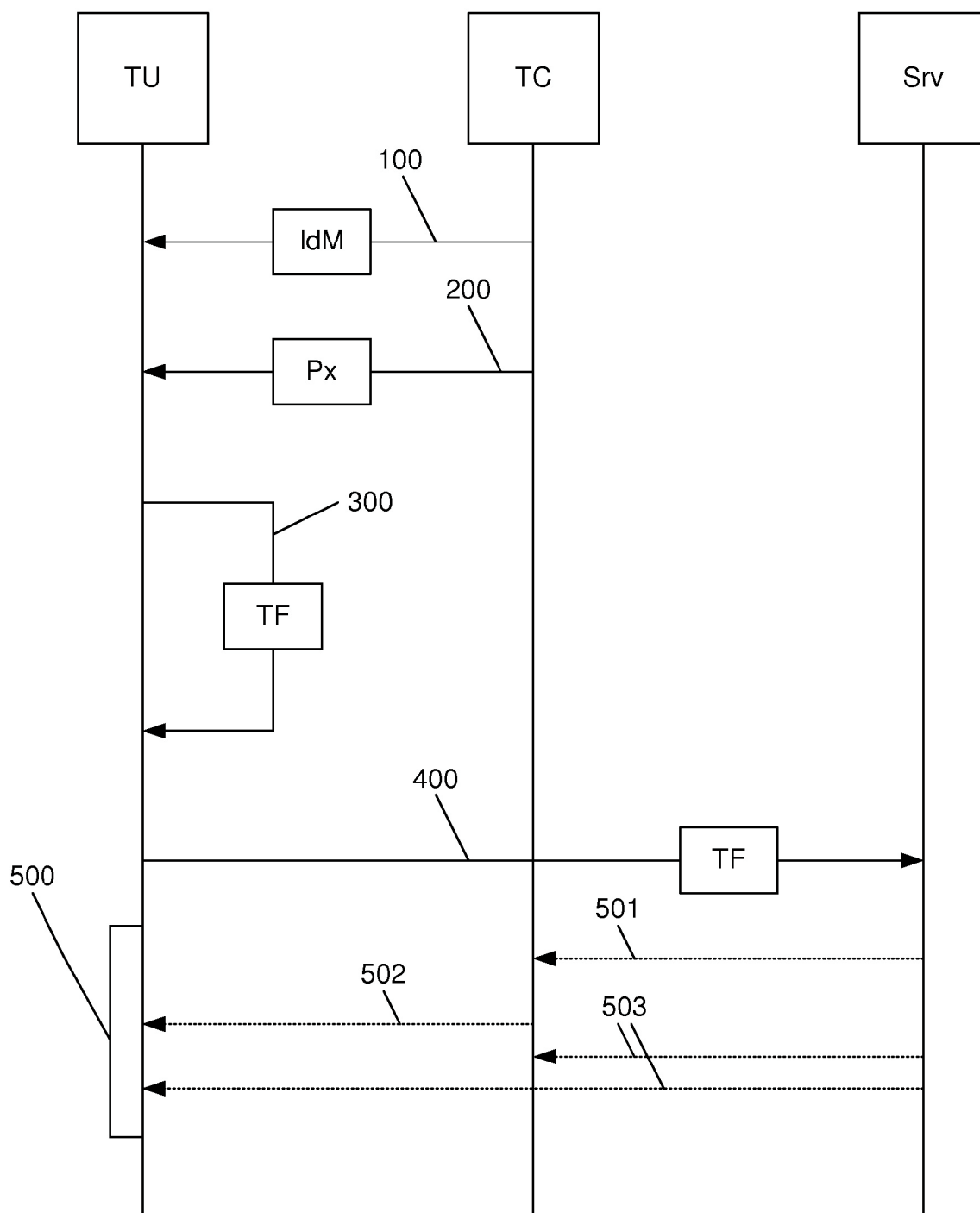


Figura 1

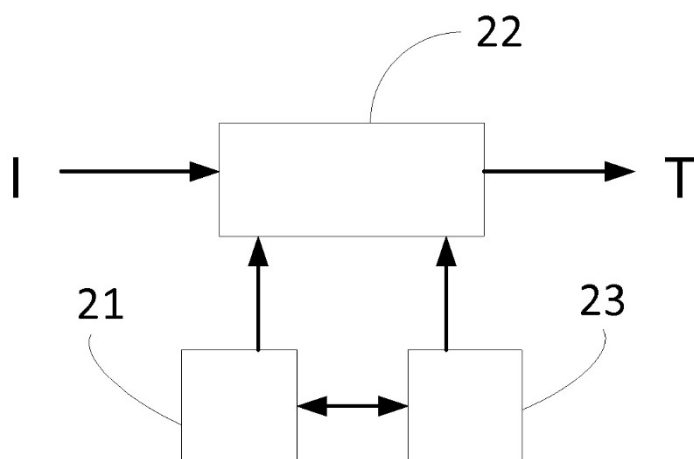


Figura 2

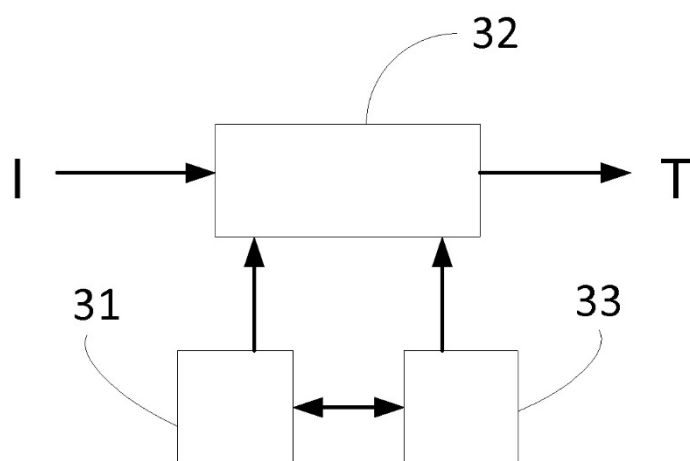


Figura 3