(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 770 087**

(51) Int. CI.:

G06Q 20/02 (2012.01)
G06Q 20/20 (2012.01)
G06Q 20/32 (2012.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.07.2016 E 16177645 (5)**

(97) Fecha y número de publicación de la concesión europea: **20.11.2019 EP 3113094**

(54) Título: **Procedimiento de procesamiento de datos transaccionales, dispositivo y programa correspondientes**

(30) Prioridad:

03.07.2015 FR 1556333

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.06.2020

(73) Titular/es:

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

(72) Inventor/es:

QUENTIN, PIERRE y
LEGER, MICHEL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de procesamiento de datos transaccionales, dispositivo y programa correspondientes

1. Campo

La presente técnica se refiere a la problemática del pago en línea. La presente técnica se refiere, más específicamente, a la puesta en práctica de un pago en el ámbito de una transacción de comercio electrónico, también denominado “e-commerce”. La presente técnica se encamina, más en particular, a facilitar el pago.

2. Técnica anterior

Una transacción de e-commerce se caracteriza por el hecho de que es puesta en práctica por mediación de un navegador de Internet que accede a una aplicación servidora (típicamente, una aplicación de comercio electrónico que genera datos con destino al navegador web). La transacción de e-commerce se considera, dentro del ámbito de la presente, como idéntica a la aplicación de comercio electrónico inalámbrico (m-commerce). Con carácter general, una transacción de e-commerce se diferencia de la transacción de m-commerce por el hecho de que la transacción de m-commerce pone en práctica una aplicación particular, instalada en un terminal de comunicación móvil (de tipo teléfono inteligente) y de que es utilizada a la vez para efectuar compras y a la vez para efectuar una transacción de pago.

En cualquier caso, una transacción de e-commerce comprende actualmente un tecleo, por parte del usuario, de datos que permiten realizar un pago. Estos datos son muchas veces datos de tarjeta bancaria. Se trata, por ejemplo, del nombre del portador de la tarjeta, del número de la tarjeta (también denominado PAN), de la fecha de expiración de la misma y de un criptograma visual. La mayor parte del tiempo, estos datos son tecleados por el usuario en la finalización de la compra. Por ejemplo, tras validación de una cesta de compra en la plataforma del vendedor, el usuario es transferido (transferido de una página a otra en el navegador web) hacia un servidor de pago. En la página presentada por este servidor de pago es donde el usuario teclea los datos de su tarjeta bancaria. Eventualmente, a más de estos datos, el servidor de pago puede, en conjunción con un servidor bancario, requerir el tecleo de un dato complementario. Puede tratarse, por ejemplo, de un código generado por el servidor bancario, basándose en el número de tarjeta bancaria tecleado por el usuario. Este código es transmitido al usuario, por ejemplo, por mediación de un mensaje (de tipo SMS) a un dispositivo separado del dispositivo utilizado por el usuario para realizar el pago (típicamente, el teléfono del usuario). Cuando se teclea este código, se pone fin a la transacción entre el servidor de pago, el servidor bancario y el servidor del comercio.

Este sistema general de pago es problemático por dos motivos. El primer motivo surge de la necesidad, para el usuario, de teclear los datos de su tarjeta bancaria para cada pago. Se comprende que, por motivos de seguridad, es preferible que estos datos se tecleen a cada pago. Sin embargo, esto es gravoso y obliga al usuario a sacar su tarjeta bancaria para teclear esta información. Para paliar este problema, existen soluciones de soporte lógico, como los administradores de contraseñas (por ejemplo, DashLane™). Estas soluciones de soporte lógico, instaladas en el dispositivo de comunicación (el ordenador o en la tableta) del usuario, permiten teclear automáticamente, en los campos previstos al efecto, los datos que con anterioridad se han tecleado en el soporte lógico. Sin embargo, por una parte, esto obliga a teclear estos datos en un soporte lógico tercero, que previamente es menester instalar en el dispositivo de comunicación del usuario; por otra parte, esta solución precisa fiarse del editor de este soporte lógico para la conservación de estos datos. Existen, asimismo, soluciones en línea: estas permiten no tener que instalar soportes lógicos en el dispositivo de comunicación del usuario, pero precisan, con todo, fiarse de un editor (por ejemplo, Google™) para la conservación de estos datos. Ahora bien, en los últimos años, se ha visto alterada en gran medida esta confianza. Por otro lado, esta solución de preservación, en el seno del dispositivo de comunicación, de los datos de tarjeta bancaria puede ser problemática en caso de robo o de pérdida del dispositivo de comunicación.

El segundo problema está relacionado con la necesidad de teclear un código suplementario, transmitido, por ejemplo, por SMS. Esta solución se pone en práctica, precisamente, para prevenir los abusos relacionados con los robos o pérdidas de tarjetas bancarias y/o para prevenir los abusos relacionados con los robos o pérdidas del dispositivo de comunicación. Ahora bien, se ha demostrado que esta solución hace que se desplome notablemente el índice de transformación (es decir, la relación entre el número de compras efectuadas respecto al número de visitas). Por lo tanto, esta solución no recibe una buena acogida por parte de los sitios web comerciales.

El documento US 2015/154597 A1 concierne a sistemas y métodos para autenticar transacciones utilizando un dispositivo móvil. Entre las diferentes formas de realización de este documento, se presenta una modalidad de pago por mediación de un terminal de comunicación móvil. Tal modalidad de pago, sin embargo, se realiza poniendo en práctica un terminal de pago en el establecimiento de un comerciante físico, estando el terminal de pago configurado para interaccionar con un servidor de pago. El documento US 015/154597 A1 no enseña, sin embargo, la recepción, por un dispositivo servidor de transacción, la recepción de una petición que comprenda un identificador de un servidor comercial, ni la obtención de un parámetro de pago que permita al terminal de comunicación realizar la transacción de pago con un servidor de pago.

El documento US 2013/304651 A1 propone elementos virtuales seguros en dispositivos móviles. El documento US

2013/304651 A1 da a conocer, en particular, un método para realizar un pago seguro con un dispositivo móvil que comprende un monedero móvil. Así, el dispositivo móvil puede inicializar un pago con un terminal de pago físico, en el establecimiento de un comerciante, con una cuenta de pago registrada con anterioridad en un elemento virtual seguro del dispositivo móvil. Este no enseña, sin embargo, la recepción, por un dispositivo servidor de transacción, la recepción de una petición que comprenda un identificador de un servidor comercial, ni la obtención de un parámetro de pago que permita al terminal de comunicación realizar la transacción de pago con un servidor de pago.

El documento WO 2014/162294 A1 propone métodos y sistemas que permiten efectuar transacciones con un dispositivo móvil que comprende un identificador grabado en una memoria segura. En este documento, el dispositivo peticionario es un terminal de pago el cual, a todas luces, no puede ser considerado como un servidor comercial en el sentido de la reivindicación 1. Adicionalmente, este documento no da a conocer que el servidor de acceso ponga en práctica una etapa de obtención de un dato representativo de un parámetro de pago asociado al servidor comercial.

El documento WO 2009/149164 A2 propone un método de procesamiento de pagos electrónicos. En este documento, habiendo elegido un consumidor utilizar un proveedor de medios de pago alternativo con el fin de abonar sus compras, un servidor comercial transmite información relativa a la transacción de pago que ha de efectuarse a una plataforma comercial universal que procesa esta transacción con el proveedor de medios de pago alternativo seleccionado. El servidor comercial recibe una dirección URL de redirección que a continuación permite al consumidor proporcionar información adicional de pago específica del proveedor de pago alternativo. El documento WO 2009/149164 A2 no enseña, sin embargo, la recepción, por un dispositivo servidor de transacción, la recepción de una petición que comprenda un identificador de un servidor comercial, ni la obtención de un parámetro de pago que permita al terminal de comunicación realizar la transacción de pago con un servidor de pago.

De este modo, estos documentos no están en disposición de aportar una solución a la puesta en práctica directa efectuada por un terminal de comunicación, con un servidor de pago, de una transacción de pago para efectuar el pago de compras realizadas en el servidor de un comercio.

3. Sumario

La presenta técnica no presenta estos inconvenientes del estado de la técnica. Más en particular, la presente técnica se refiere a un procedimiento de procesamiento de datos transaccionales según la reivindicación 1.

De este modo, el dispositivo electrónico de procesamiento de transacciones, también denominado servidor de transacciones o también servidor transaccional, está en condiciones de realizar una gestión optimizada de las transacciones. En efecto, debido a su calidad de receptor de las peticiones de procesamiento de las transacciones con origen en servidores comerciales (se entiende que varios servidores comerciales son susceptibles de apelar al dispositivo de procesamiento de transacciones), el dispositivo de procesamiento de transacciones fácilmente puede verificar y validar las peticiones para detectar eventuales intentos de fraude.

De este modo, el terminal de comunicación queda protegido de los intentos de ataque. En efecto, puesto que se limita a recibir datos paramétricos de manera dinámica (es decir, a la hora de realizar la transacción de pago), no está obligado a almacenar estos datos de manera permanente y puede, cuando se termina la transacción, borrar estos datos. En consecuencia, un intento de ataque que consistiera en tratar de obtener datos de conexión a un servidor de pago estaría abocado al fracaso, ya que el terminal de comunicación (o, *a fortiori*, el componente seguro de este terminal de comunicación) no comprendería ningún dato que permitiera hacerlo. En una forma de realización alternativa, la transmisión de los parámetros de conexión al servidor de pago se realiza por mediación del servidor comercial. En consecuencia, el servidor de transacción queda eximido de una tarea de transmisión al terminal de comunicación. Así, tiene un a modo de cortafuegos que se crea entre el servidor de transacción y el terminal de comunicación.

Al comprender la petición de procesamiento de transacción un dato representativo de un identificador del terminal de comunicación del usuario, por vía de indirección, el servidor de transacción está en condiciones de identificar el terminal de comunicación que desempeña la función de terminal de pago para esta transacción. Subsidiariamente, en una forma de realización específica, el servidor de transacción asimismo puede obtener datos representativos de este terminal de comunicación con el concurso de este identificador. Tales datos pueden, por ejemplo, permitir verificar que el terminal de comunicación no ha sido puesto en una lista negra de terminales de comunicación no autorizados a efectuar transacciones. Puede tratarse, por ejemplo, de terminales de comunicación identificados como presuntos terminales piratas.

Comprendiendo el dato representativo de un identificador del terminal de comunicación del usuario, asimismo, un identificador de un componente de procesamiento de transacciones del terminal de comunicación del usuario, el servidor de transacción asimismo puede verificar, siempre por vía de indirección, el estado del componente de procesamiento de transacciones.

De acuerdo con una característica particular, el procedimiento comprende, además, una etapa de obtención de un dato representativo de un número de transacción.

De este modo, el dispositivo electrónico de procesamiento de transacciones es el planificador de las transacciones, que habrán de realizarse en el servidor de pago. Por lo tanto, gestiona de manera optimizada el procesamiento de las transacciones en función de los diferentes servidores de pago a su disposición. En una forma particular de realización, está en condiciones, por ejemplo, de seleccionar, de entre una pluralidad de servidores de pago, el servidor de pago que es el encargado de procesar una transacción particular. Por otro lado, cuando se encuentra disponible un solo servidor de pago, el servidor de transacción se asegura de que el servidor de pago procese las transacciones en el orden que se le proporciona.

De acuerdo con una característica particular, dicha etapa de obtención de un dato representativo de un parámetro de pago comprende una etapa de búsqueda, en el seno de una estructura de datos, de al menos un parámetro asociado a dicho servidor comercial.

De este modo, la ulterior parametrización del terminal de comunicación no depende de datos proporcionados por el comercio, sino de datos que son obtenidos por el servidor de transacciones. En consecuencia, la modificación de estos datos no puede llevarse a cabo sobre la marcha, por ejemplo interceptando y modificando parámetros que fueran transmitidos directamente por el comercio.

Por otro lado, puesto que solo se transmite al servidor de transacción el identificador del comercio, también estaría abocado al fracaso un intento de fraude que consistiera en modificar el identificador del comercio (en vistas a abonar una cuenta bancaria diferente de la cuenta bancaria del comercio), pues sería menester que el actor del fraude dispusiera asimismo de parámetros directamente accesibles por mediación del servidor de transacción. Si esto llegara a producirse, entonces el actor del fraude sería identificable directamente y puesto en lista negra.

De acuerdo con una característica particular, el procedimiento comprende, además, una etapa de transmisión de un dato de confirmación, con destino al servidor comercial.

De acuerdo con otro aspecto, asimismo se describe un sistema de procesamiento de transacciones, apto para efectuar un procesamiento de datos transaccionales según la reivindicación 5.

transacciones. En consecuencia, la modificación de estos datos no puede llevarse a cabo sobre la marcha, por ejemplo interceptando y modificando parámetros que fueran transmitidos directamente por el comercio.

Por otro lado, puesto que solo se transmite al servidor de transacción el identificador del comercio, también estaría abocado al fracaso un intento de fraude que consistiera en modificar el identificador del comercio (en vistas a abonar una cuenta bancaria diferente de la cuenta bancaria del comercio), pues sería menester que el actor del fraude dispusiera asimismo de parámetros directamente accesibles por mediación del servidor de transacción. Si esto llegara a producirse, entonces el actor del fraude sería identificable directamente y puesto en lista negra.

De acuerdo con una característica particular, el procedimiento comprende, además, una etapa de transmisión de un dato de confirmación, con destino al servidor comercial.

De acuerdo con otro aspecto, asimismo se describe un dispositivo electrónico de procesamiento de transacciones, apto para efectuar un procesamiento de datos transaccionales, siendo representativos dichos datos de un pago entre un usuario y un comercio. Tal dispositivo comprende:

- medios de recepción de una petición de procesamiento de transacción con origen en un servidor comercial;
- medios de obtención de un dato representativo de un parámetro de pago asociado a dicho servidor comercial;
- medios de transmisión, a un servidor de pago, de una petición de procesamiento de pago.

Asimismo, comprende, dependiendo de las formas de realización, todos los demás medios para la puesta en práctica de las etapas anteriormente descritas.

De acuerdo con una implementación preferida, las diferentes etapas de los procedimientos según la técnica que se propone se llevan a la práctica mediante uno o varios soportes lógicos o programas de ordenador, que comprenden instrucciones lógicas destinadas a ser ejecutadas por un procesador de datos de un módulo relevador según la técnica que se propone y que está diseñado para regir la ejecución de las diferentes etapas de los procedimientos.

En consecuencia, la técnica que se propone también está encaminada a un programa, susceptible de ser ejecutado por un ordenador o por un procesador de datos, incluyendo este programa instrucciones para regir la ejecución de las etapas de un procedimiento tal como se ha mencionado anteriormente.

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

La técnica que se propone también se encamina a un soporte de información legible por un procesador de datos y que incluye instrucciones de un programa tal y como se ha mencionado anteriormente.

El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD-ROM o una ROM de circuito microelectrónico, o también un medio de grabación magnética, por ejemplo un disquete (floppy disc) o un disco duro.

Por otra parte, el soporte de información puede ser un soporte transmisible, tal como una señal eléctrica u óptica, que se puede conducir a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la técnica que se propone se puede descargar en particular por una red de tipo Internet.

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

De acuerdo con una forma de realización, la técnica que se propone se lleva a la práctica por medio de componentes de soporte lógico y/o de soporte físico. En esta línea, el término "módulo" puede corresponder, en este documento, tanto a un componente de soporte lógico, como a un componente de soporte físico o a un conjunto de componentes de soporte físico y lógico.

Un componente de soporte lógico corresponde a uno o varios programas de ordenador, uno o varios subprogramas de un programa o, de manera más general, a todo elemento de un programa o de un soporte lógico apto para llevar a la práctica una función o un conjunto de funciones, según lo descrito a continuación en relación con el módulo de que se trate. Tal componente de soporte lógico es ejecutado por un procesador de datos de una entidad física (terminal, servidor, pasarela, encaminador, etc.) y está posibilitado de acceso a los recursos de soporte físico de esta entidad física (memorias, soportes de grabación, buses de comunicación, tarjetas electrónicas de entrada/salida, interfaces de usuario, etc.).

De la misma manera, un componente de soporte físico corresponde a todo elemento de un conjunto de soporte físico (o hardware) apto para llevar a la práctica una función o un conjunto de funciones, según lo descrito a continuación en relación con el módulo de que se trate. Puede ser un componente de soporte físico programable o con procesador integrado para la ejecución de soporte lógico, por ejemplo un circuito integrado, una tarjeta inteligente, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microprograma (firmware), etc.

Por supuesto, cada componente del sistema anteriormente descrito pone en práctica sus propios módulos de lógica.

Las diferentes formas de realización antes mencionadas son combinables entre sí para la puesta en práctica de la técnica que se propone.

4. Figuras

Otras características y ventajas de la técnica que se propone se pondrán más claramente de manifiesto con la lectura de la siguiente descripción de una forma preferente de realización, dada a título de mero ejemplo ilustrativo y no limitativo, y de los dibujos que se acompañan, de los cuales:

- la figura 1 presenta un sinóptico de la técnica que se propone, desde el punto de vista del servidor de procesamiento de transacción; y
- la figura 2 describe sucintamente la arquitectura física del servidor de procesamiento de transacción.

5. Descripción

Como se ha expuesto con anterioridad, el objeto de la presente es facilitar el pago, asegurando que el mismo se pueda llevar a cabo de manera simple y segura. Más en particular, el pago se realiza poniendo en práctica, en el seno de un terminal de comunicación, un componente de procesamiento de transacciones, seguro, que actúa como un terminal de pago multicomercio. De este modo, la solución de la invención aporta una seguridad incrementada en las transacciones realizadas, al propio tiempo que evita que el usuario se vea obligado a teclear datos, especialmente de tarjeta bancaria, a la hora de pagar.

Recordemos, a todos los efectos útiles, que en una utilización convencional, un terminal de pago se materializa en forma de un dispositivo, instalado físicamente en el establecimiento de un comerciante, dispositivo que permite recibir pagos por parte de los clientes que utilizan una tarjeta de pago. Cada vez más comerciantes disponen de terminales de pago multitecnología, que a la vez admiten un pago con tarjeta inteligente, un pago con tarjeta magnética y un pago con tarjeta sin contacto. El terminal de pago convencional está configurado para funcionar únicamente con un comerciante: esto significa que el terminal de pago comprende una configuración, no modificable por él. Esta configuración comprende cierto número de parámetros que son, por ejemplo, identificadores bancarios (que permiten conectarse o también certificar intercambios con el establecimiento bancario del comerciante) o también parámetros de conexiones a servidores. *De este modo, intrínsecamente, un terminal de pago convencional está relacionado con el comerciante y no con el cliente*.

El enfoque de la técnica que se propone es muy diferente: se trata de disponer de un componente de procesamiento de transacciones, seguro, que desempeña la función de un terminal de pago que es multicomercio. El componente,

que va instalado en el seno del terminal de comunicación del usuario, ofrece capacidades de procesamiento multicomercio, pues es configurable: este componente permite, en cierto modo, transformar el terminal de comunicación del usuario en un terminal de pago mientras dure la transacción de pago. En consecuencia, con la técnica que se propone, es posible realizar transacciones de pago, remotas (es decir, transacciones de e-commerce) sin tener que teclear o grabar previamente en un soporte lógico externo sus datos bancarios.

En una forma de realización, el componente de procesamiento de transacciones (componente seguro) es un componente que dispone de o que utiliza una interfaz de comunicación sin contacto: esta interfaz permite al usuario utilizar una tarjeta de pago sin contacto: desde el punto de vista del usuario, el pago se realiza aplicando o acercando su tarjeta de pago sin contacto en la proximidad de una zona predefinida del terminal de comunicación. La experiencia de pago se ve, por tanto, facilitada en gran manera para el cliente.

Desde el punto de vista del comercio, se maximiza el índice de transformación: en efecto, al facilitarse la experiencia de pago, el riesgo de pérdida de un cliente en la operación de pago disminuye en igual medida.

La técnica que se propone, sea como fuere, no recae sobre un componente seguro destinado a ser utilizado en el seno de un terminal de comunicación, sino en la utilización particular de un conjunto de medios puestos en práctica en el seno de una o varias redes de comunicación para permitir una puesta en práctica de un pago.

Más en particular, la técnica que se propone recae sobre la puesta en práctica del pago mediante un servidor que está en condiciones de configurar, sobre la marcha, el componente seguro del terminal de comunicación, con el fin de permitirle realizar el pago directamente ante el servidor de pago. Desde el punto de vista de este servidor, la técnica puesta en práctica es la siguiente, descrita en relación con la figura 1. Se trata de realizar un procesamiento de datos transaccionales representativos de un pago entre un usuario (U) y un comercio (M). El procedimiento es puesto en práctica por un dispositivo electrónico de procesamiento de transacciones (el servidor) situado en el seno de una red de comunicación. El método, según el dispositivo de procesamiento de transacciones, comprende:

- una etapa de recepción (100) de una petición de procesamiento de transacción (ReqTT) con origen en un servidor comercial (SerMar); esta petición puede comprender, según las condiciones operativas, un dato representativo de un identificador del servidor comercial;

- una etapa de obtención (110) de un dato representativo de un parámetro de pago (ParPai) asociado a dicho servidor comercial (SerMar); estos parámetros se obtienen, por ejemplo, utilizando el identificador del servidor comercial, con el fin de efectuar una búsqueda en el seno de una base de datos de parámetros de pagos;

- una etapa de obtención (120) de un dato representativo de un número de transacción (DRNumTrans); esta etapa es opcional desde el punto de vista del servidor: en efecto, el número de transacción puede venir proporcionado por otras vías, sin que el servidor sea informado necesariamente de este número;

- una etapa de transmisión (130) de un dato de confirmación, con destino al servidor comercial (SerMar); esta etapa es opcional desde el punto de vista del servidor de procesamiento: en efecto, esta confirmación puede ser transmitida asimismo por otras vías, sin que el servidor de procesamiento sea informado necesariamente de ello;

- una etapa de transmisión (140), a un servidor de pago (SerPai), de una petición de procesamiento de pago (ReqTrtPai);

- una etapa de transmisión (150), a un terminal de comunicación del usuario, de un dato representativo de parámetros de conexión (ParCon) al servidor de pago (SerPai); esta etapa, bien es puesta en práctica directamente por el servidor de procesamiento de transacción, o bien puesta en práctica mediante indirección, utilizando el servidor comercial.

Con anterioridad a la puesta en práctica del método, el servidor comercial (Sermar) recibe (E1), por parte del terminal de comunicación (TerCom), une petición de pago (el usuario desea efectuar el pago). Como respuesta a esta petición, el servidor comercial efectúa (E2) una verificación de la presencia de un componente seguro. El terminal transmite (E3) un dato indicativo de la presencia o no del componente seguro en el terminal de comunicación (TerCom).

Se comprende, por supuesto, que la mayoría de los intercambios realizados entre los servidores y el componente seguro están cifrados y que las claves de cifrado simétricas o asimétricas utilizadas son elementos a disposición de estas diferentes entidades.

Como se ha indicado, el servidor comercial transmite la petición de procesamiento de transacción (ReqTT) al servidor de transacción. Tal transmisión es posible porque el servidor comercial es el servidor que efectúa la verificación de la presencia del componente seguro en el terminal de comunicación del usuario. En efecto, en el momento del pago, el servidor comercial, con el concurso de una aplicación de pago específica (“checkout application”), trata de verificar la presencia del componente seguro en el terminal de comunicación del usuario. Cuando este intento culmina en la detección, el servidor comercial transmite la petición de procesamiento de

transacción (ReqTT) al servidor de transacción. Cuando este intento no culmina en la detección del componente, entonces el servidor comercial pone en práctica un proceso de pago convencional consistente en redirigir al usuario a una página web de un servidor bancario con el fin de que el usuario pueda teclear los datos de su tarjeta bancaria.

La detección de la presencia del componente seguro en el terminal de comunicación del usuario puede venir acompañada de la obtención, por el servidor comercial, de un correspondiente identificador de este componente seguro. Este identificador lo aporta el fabricante del componente seguro. Permite identificar el mismo de manera única de entre el conjunto de los componentes seguros existentes. Permite, por otro lado, como se hace explícito en lo sucesivo, supervisar el estado de funcionamiento de este componente seguro. Por otro lado, la detección de la presencia del componente seguro en el terminal de comunicación del usuario viene precedida o acompañada, eventualmente, de la obtención de una dirección de comunicación en red del terminal de comunicación. Por ejemplo, el servidor comercial puede obtener la dirección IP (del inglés, por “Internet Protocol”). Tal dirección es útil, en el ámbito de la presente técnica, pues permite al servidor de procesamiento de transacción (al que es transmitida esta dirección por el servidor comercial) disponer de una localización (red) del terminal de comunicación. Entonces, el servidor de procesamiento de transacción puede efectuar dos operaciones, eventualmente opcionales (en función de las puestas en práctica operativas de la presente técnica):

- el servidor de procesamiento de transacción puede establecer contacto directamente con el terminal de comunicación, con el fin de verificar, por ejemplo, que el componente seguro funciona correctamente y no ha sufrido o sufre un ataque por parte de un programa, de una persona o de otro componente;

- el servidor de procesamiento de transacción puede proporcionar, al terminal de comunicación, los parámetros de conexión al servidor de pago;

- el servidor de procesamiento de transacción puede verificar la localización real del terminal de comunicación (basándose en la dirección IP, puede obtenerse una localización real con mayor o menor precisión): el servidor puede poner entonces el terminal de comunicación del usuario en una lista negra si la localización del terminal de comunicación del usuario es diferente de una localización esperada por el servidor de procesamiento de transacción;

- el servidor de procesamiento de transacción puede obtener asimismo el identificador del componente seguro (si este identificador no lo ha proporcionado ya el servidor comercial).

En cualquier caso, antes de conducir las operaciones necesarias para la finalización de la transacción de pago, el servidor de procesamiento de transacción puede comunicarse con el servidor comercial con el fin de determinar la fiabilidad del componente seguro y la capacidad de este componente seguro para conducir correctamente una transacción de pago. Las diferentes etapas puestas en práctica con este fin de verificación pueden comprender otras etapas distintas a las explicitadas anteriormente.

Las verificaciones y búsquedas de parámetros efectuadas por el servidor de procesamiento de transacción ponen en práctica estructuras de datos de almacenamiento de parámetros y/o de valores. Tales estructuras pueden materializarse en forma de base de datos o de ficheros.

Cuando el servidor de procesamiento de transacción decide la puesta en práctica de la transacción por mediación del componente seguro, el servidor pone en práctica entonces unas etapas que permiten, por una parte, preparar el componente seguro para que actúe como un terminal de pago del comercio (es decir, un terminal de pago asociado al comercio) y, por otra, informar al servidor bancario de la puesta en práctica de una transacción de pago por venir.

La preparación del componente seguro precisa de la obtención de un dato representativo de un parámetro de pago asociado a dicho servidor comercial. Puede tratarse, típicamente, de datos de identificación del comercio y/o de claves de cifrado asociadas al comercio. Asimismo, puede tratarse de datos relativos a una cuenta bancaria del comercio, cuenta en la que se debe abonar el importe de la transacción. El componente recibe asimismo una dirección IP del servidor bancario al que debe conectarse. Esta dirección IP se puede proporcionar en segunda instancia, una vez que el componente seguro queda en disposición de establecer un enlace seguro con el servidor de procesamiento de transacción o una vez que el servidor de procesamiento de transacción ha seleccionado el servidor de pago que debe efectuar esta transacción.

Recordemos que el componente seguro del terminal de comunicación está virgen de toda información de pago con anterioridad a la recepción de datos con origen en el servidor. Por lo tanto, este componente seguro, antes de cada transacción, debe recibir datos con el fin de que pueda comportarse como un terminal de pago físico. Asimismo, se hace la aclaración de que el final de la transacción de pago (es decir, la confirmación de la toma en consideración del pago por el servidor de pago) lleva consigo la destrucción de los datos recibidos por el componente seguro. En definitiva, finalizada la transacción, el componente seguro recobra su estado inicial. Con objeto de permitir una comunicación segura, el componente seguro dispone, sin embargo, de manera permanente o semipermanente, de una o varias claves (claves públicas y/o claves privadas) que permiten conducir intercambios seguros, ya sea con los servidores comerciales, ya sea con el servidor de procesamiento de transacción.

Dependiendo de las formas de realización y de la puesta en práctica operativa de la presente técnica, la

configuración del componente seguro es puesta en práctica, bien directamente por el servidor de procesamiento de transacción (el cual se hace cargo entonces de esta tarea, prescindiendo de la intervención del servidor comercial), bien por vía de indirección. El servidor de procesamiento de transacción transmite entonces al servidor comercial los datos necesarios para la configuración del componente seguro, el servidor comercial retransmite en lo sucesivo estos datos al componente seguro (utilizando la interfaz física de comunicación del terminal de comunicación).

Ambos enfoques presentan ventajas: en el primer enfoque, se elimina la intervención de un agente (el servidor comercial) y, por tanto, se refuerza la seguridad de la transacción. En el segundo enfoque, se reducen las necesidades de procesamiento del servidor de procesamiento de transacción, que no necesita disponer de los considerables recursos necesarios para la comunicación con un número muy considerable de terminales de comunicación.

Para informar al servidor bancario de que va a procesar una transacción, el servidor de procesamiento de transacción transmite al mismo una petición. Esta petición comprende de manera opcional un identificador de transacción (como, por ejemplo, el número de transacción). Asimismo, esta petición comprende el identificador del componente seguro del terminal de comunicación. Eventualmente, se pueden proporcionar otros datos, como la dirección IP del terminal de comunicación del usuario, con el fin de que el servidor de pago esté en condiciones de aceptar o no una transacción con origen en este terminal de comunicación.

Con anterioridad a la transmisión de estos datos, en forma de una petición, al servidor de transacción, el servidor de procesamiento de transacción obtiene un número de transacción que ha de procesarse. El número de transacción es un identificador que permite asociar conjuntamente los datos de la transacción. Se trata de un identificador perenne: el identificador y los datos asociados son conservados, por ejemplo en una o varias bases de datos, para una ulterior explotación de estos datos (por ejemplo, a título comprobatorio). El identificador de transacción, bien es generado directamente por el servidor de procesamiento de transacción, o bien obtenido ante otro servidor o servicio. Esta puesta en práctica depende de las condiciones operativas y no se detalla.

Una vez provisto de estos datos, el servidor bancario queda en disposición, por una parte, de aceptar o no una conexión con origen en el terminal de comunicación (efectuando, por ejemplo, una verificación de la dirección de origen de las peticiones transmitidas por el terminal de comunicación) y, por otra, de verificar que el componente seguro que desea validar la transacción realmente se corresponde con el componente seguro identificado con anterioridad. El servidor de pago prepara las instancias de soporte lógico necesarias para el procesamiento de la transacción y queda en espera de la petición con origen en el componente seguro.

Con anterioridad a la transmisión de esta petición, el servidor de procesamiento de transacción, asimismo, puede efectuar una elección de un servidor de pago cuando están disponibles varios servidores de pago para procesar la petición. De este modo, el servidor de procesamiento de transacción está en condiciones de repartir eficientemente la carga que gravita sobre estos servidores de pago.

Cuando se efectúa la preparación del componente seguro y del servidor de pago, el servidor de procesamiento de transacción queda en espera de la (eventual) recepción (E5) de una confirmación de pago con origen en el servidor de pago.

El acto de pago (E4), figura 1, propiamente dicho, lo realiza el usuario, quien aplica su tarjeta de pago sin contacto en una ubicación especificada de su terminal de comunicación, con el fin de que el componente seguro pueda recuperar los datos de la tarjeta de pago y transmitir estos datos al servidor de pago para que efectúe el pago.

Con anterioridad o con posterioridad a la recepción de tal información, asimismo, puede transmitir (E6) por sí mismo una confirmación de final de procesamiento de transacción al servidor comercial, con el fin de que este último pueda, por ejemplo, redirigir (E7) el navegador web del terminal de comunicación hacia una página de final de transacción, sinónimo para el usuario de que el procesamiento de pago está terminado.

Se describe, en relación con la figura 2, un dispositivo que comprende medios que permiten la ejecución del procedimiento descrito con anterioridad. Tal dispositivo adopta la forma, por ejemplo, de un servidor de procesamiento de transacción.

Por ejemplo, el dispositivo comprende una memoria 21 constituida a partir de una memoria intermedia, poniendo en práctica una unidad de procesamiento 22 equipada, por ejemplo, con un microprocesador y pilotada por el programa de ordenador 23, las etapas necesarias para el procesamiento de las transacciones, en indirección, entre el servidor comercial, el componente seguro y el servidor de pago.

Con la inicialización, las instrucciones de código del programa de ordenador 23 se cargan, 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 entrada, por ejemplo, una petición de procesamiento de transacción con origen en un servidor comercial. El microprocesador de la unidad de procesamiento 22 pone en práctica las etapas del procedimiento de procesamiento, según las instrucciones del programa de ordenador 23, para efectuar una preparación de la transacción ante el componente seguro, una preparación de un servidor de pago.

Comprende para ello el dispositivo, aparte de la memoria intermedia 21, unos medios de obtención de datos de configuración, eventualmente un procesador de cifrado y medios de comunicación, tales como módulos de comunicaciones en red, que permiten la transmisión y la recepción de datos. Estos medios pueden estar pilotados por el procesador de la unidad de procesamiento 22 en función del programa de ordenador 23. Estos medios se materializan asimismo en forma de módulos, de soporte lógico o físico, dedicados específicamente o no a la puesta en práctica de la presente técnica. Por otro lado, el procesador a cargo puede ser un procesador seguro que permite precaverse contra un ataque durante las fases de cifrado o de descifrado.

Asimismo, la técnica se refiere a un terminal de pago multicomercio, tal como se ha descrito anteriormente. Tal terminal de pago multicomercio se materializa en diversas formas. En una forma simple, tal terminal comprende una interfaz de comunicación en red. Esta interfaz permite al terminal de pago recibir datos con origen en servidores, entre ellos el servidor comercial y el servidor de transacción. Tal interfaz puede ser una interfaz independiente o una interfaz gestionada por un dispositivo en cuyo seno está instalado o conectado el terminal de pago. En esta misma forma simple, el terminal de pago comprende una interfaz de comunicación sin contacto. Tal interfaz de comunicación sin contacto permite transmitir una señal con destino a una tarjeta de pago (o a un terminal de comunicación NFC), con el fin de que esta última, como respuesta, emita los datos necesarios para el pago. Esta interfaz de comunicación sin contacto puede ser una interfaz independiente o una interfaz gestionada por un dispositivo en cuyo seno está instalado o conectado el terminal de pago. En una forma de realización distribuida, que es la que anteriormente se ha descrito, el terminal de pago multicomercio se compone, por tanto, de un conjunto que comprende el componente seguro e interfaces de comunicación prestadas del terminal de comunicación en cuyo seno va instalado el componente seguro.

Asimismo, la técnica se refiere a un procedimiento de gestión de un pago, puesto en práctica por un terminal de pago multicomercio tal como se ha descrito anteriormente. Tal procedimiento comprende, desde el punto de vista de este terminal, una etapa de transmisión, al servidor comercial, de una petición de pago (el usuario desea efectuar el pago). Como respuesta a esta petición, el servidor comercial efectúa una verificación de la presencia de un componente seguro (es decir, de la presencia del terminal de pago multicomercio): el terminal de comunicación recibe una petición de verificación de la presencia del componente seguro. El terminal (de comunicación o de pago) transmite un dato indicativo de la presencia del componente seguro en el terminal de comunicación.

El terminal de pago (o el terminal de comunicación) recibe a continuación un dato representativo de parámetros de conexión (*ParCon*) al servidor de pago (*SerPai*). Esta recepción desencadena la autoconfiguración del terminal de pago multicomercio. En el momento de esta autoconfiguración, el terminal de pago multicomercio pasa a ser un terminal dedicado únicamente al comercio para el cual debe realizarse el pago. Las interfaces de comunicación en red y sin contacto se hallan entonces bajo control exclusivo del procesador seguro, con el fin de poner en práctica el pago. Cuando estas interfaces de comunicación en red y sin contacto son compartidas con un terminal de comunicación, la autoconfiguración comprende un proceso de bloqueo de estas interfaces en favor del procesador seguro.

El procesador seguro recibe a continuación, con origen en la interfaz sin contacto, unos datos necesarios para el pago (número de tarjeta bancaria, nombre, fecha de expiración, etc.) y transmite esta información, así como datos complementarios propios de la transacción de pago, al servidor de pago. En estas etapas de recepción de los datos de la interfaz NFC y de construcción y de transmisión de la transacción al servidor de pago, el terminal de pago utiliza los parámetros de conexión y de configuración recibidos anteriormente.

Cuando se valida la transacción, el terminal de comunicación recibe a continuación los datos de confirmación con origen en el servidor comercial. El procesador seguro se separa entonces de los datos de configuración y readquiere la posibilidad de realizar un pago para otro comercio en una próxima transacción.

INSTANCIA PRINCIPAL - REIVINDICACIONES

1. Procedimiento de procesamiento de datos transaccionales (SerTran) representativos de un pago entre un usuario (U) y un comercio (M), procedimiento puesto en práctica por un dispositivo electrónico de procesamiento de transacciones situado en el seno de una red de comunicación, dispositivo que se constituye en interfaz entre un servidor comercial (SerMar) y un servidor de pago (SerPai), comprendiendo el procedimiento:

- una etapa de recepción (E1) de una petición de pago con origen en el terminal de comunicación del usuario,
- una etapa de verificación (E2) de una presencia de un componente de procesamiento de transacciones del terminal de comunicación del usuario,
- una etapa de transmisión (E3), por parte del terminal de comunicación del usuario, de un dato indicativo de la presencia del componente de procesamiento de transacciones, que comprende un identificador de dicho componente de procesamiento de transacciones; y cuando está presente el componente de procesamiento de transacciones;
- una etapa de recepción (100) de una petición de procesamiento de transacción (ReqTT) con origen en el servidor comercial (SerMar), comprendiendo dicha petición de procesamiento un identificador del servidor comercial (SerMar) y el identificador del componente de procesamiento de transacciones del terminal de comunicación del usuario;
- una etapa de obtención (110) de un dato representativo de un parámetro de pago (ParPai) asociado a dicho servidor comercial (SerMar), en función del identificador del servidor comercial (SerMar);
- una etapa de transmisión (140), al servidor de pago (SerPai), de una petición de procesamiento de pago (ReqTrtPai) que comprende el identificador de dicho componente de procesamiento de transacciones;
- una etapa de transmisión (150), a dicho componente de procesamiento de transacciones del terminal de comunicación del usuario, de datos de configuración que comprenden dicho dato representativo de un parámetro de pago (ParPai) asociado a dicho servidor comercial (SerMar) y de un dato representativo de parámetros de conexión al servidor de pago (SerPai);
- una etapa de realización de la transacción de pago entre el componente de procesamiento de transacciones del terminal de comunicación y el servidor de pago (SerPai), en función de los datos recibidos a lo largo de la etapa de transmisión, que comprende una etapa de verificación de que el componente de procesamiento de transacciones que desea validar la transacción se corresponde con el componente de procesamiento de transacciones identificado con anterioridad ante el servidor de pago.

2. Procedimiento de procesamiento según la reivindicación 1, caracterizado por que además comprende una etapa de obtención (120) de un dato representativo de un número de transacción (DRNumTrans).

3. Procedimiento de procesamiento según la reivindicación 1, caracterizado por que dicha etapa de obtención (110) de un dato representativo de un parámetro de pago (ParPai) comprende una etapa de búsqueda, en el seno de una estructura de datos, de al menos un parámetro asociado a dicho servidor comercial.

4. Procedimiento de procesamiento según la reivindicación 1, caracterizado por que además comprende una etapa de transmisión (130) de un dato de confirmación con destino al servidor comercial (SerMar).

5. Sistema electrónico de procesamiento de transacciones, apto para efectuar un procesamiento de datos transaccionales, que comprende un dispositivo que se constituye en interfaz entre un servidor comercial (SerMar) y un servidor de pago (SerPai), siendo representativos dichos datos de un pago entre un usuario (U) y un comercio (M), sistema caracterizado por comprender:

- medios de recepción (E1) de una petición de pago con origen en el terminal de comunicación del usuario,
- medios de verificación (E2) de una presencia de un componente de procesamiento de transacciones del terminal de comunicación del usuario,
- medios de transmisión (E3), por parte del terminal de comunicación del usuario, de un dato indicativo de la presencia del componente de procesamiento de transacciones, que comprende un identificador de dicho componente de procesamiento de transacciones;

y cuando está presente el componente de procesamiento de transacciones, la puesta en práctica:

- de medios de recepción (100) de una petición de procesamiento de transacción (ReqTT) con origen en el servidor comercial (SerMar), comprendiendo dicha petición de procesamiento un identificador del servidor comercial (SerMar) y el identificador del componente de procesamiento de transacciones del terminal de comunicación del usuario;

- medios de obtención (110) de un dato representativo del parámetro de pago (ParPai) asociado a dicho servidor comercial (SerMar), en función de un identificador del servidor comercial (SerMar);

- medios de transmisión (140), al servidor de pago (SerPai), de una petición de procesamiento de pago (ReqTrtPai) que comprende el identificador de dicho componente de procesamiento de transacciones,

- medios de transmisión (150), a dicho componente de procesamiento de transacciones del terminal de comunicación del usuario, de datos de configuración que comprenden dicho dato representativo de un parámetro de pago (ParPai) asociado a dicho servidor comercial (SerMar) y de un dato representativo de parámetros de conexión al servidor de pago (SerPai);

- medios de realización de la transacción de pago entre el componente de procesamiento de transacciones del terminal de comunicación y el servidor de pago (SerPai), en función de los datos recibidos a lo largo de la etapa de transmisión, en función de los datos recibidos a lo largo de la etapa de transmisión, que comprenden medios de verificación de que el componente de procesamiento de transacciones que desea validar la transacción se corresponde con el componente de procesamiento de transacciones identificado con anterioridad ante el servidor de pago.

6. Producto de programa de ordenador descargable desde una red de comunicación y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador, caracterizado por comprender instrucciones de código de programa para la ejecución de un procedimiento de procesamiento de datos transaccionales según la reivindicación 1, cuando se ejecuta en un ordenador.

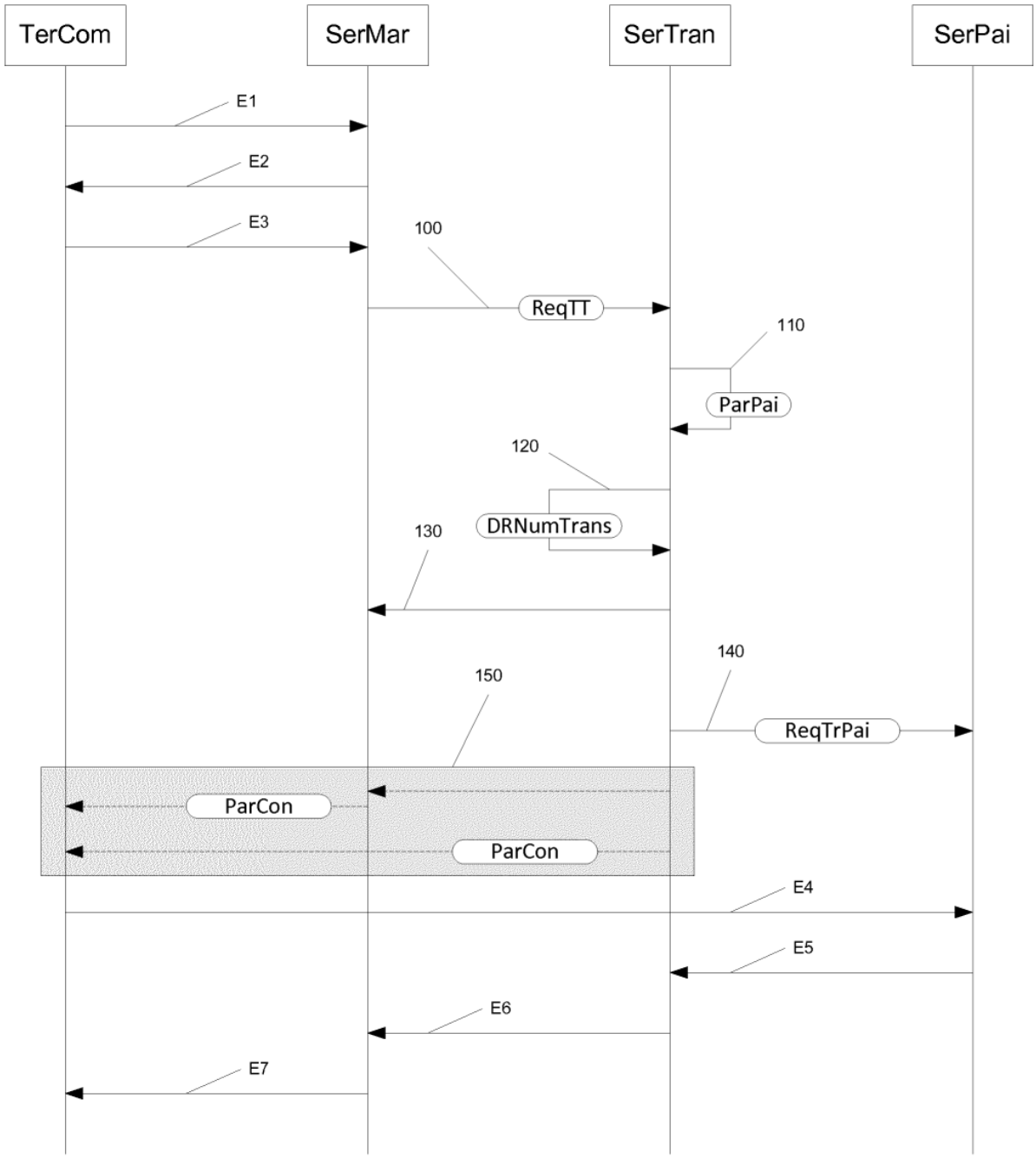
TerCom
SerMar
SerTran
SerPai
E1
E2
E3
100
ReqTT
110
ParPai
120
DRNumTrans
130
140
150
ReqTrPai
ParCon
ParCon
E4
E5
E6
E7

Figura 1

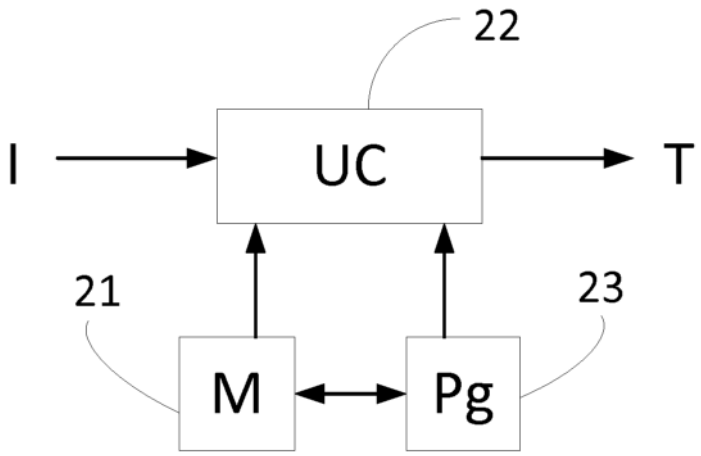

Figura 2