(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 607 427**

(21) Número de solicitud: 201531386

(51) Int. CI.:

G06Q 20/04 (2012.01)
G06Q 20/12 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

29.09.2015

(43) Fecha de publicación de la solicitud:

31.03.2017

Fecha de concesión:

02.01.2018

(45) Fecha de publicación de la concesión:

09.01.2018

(73) Titular/es:

MANSO BERNÁRDEZ, José Francisco (100.0%)
Juana Nogueira nº 7 3º C
15702 Santiago de Compostela (A Coruña) ES

(72) Inventor/es:

MANSO BERNÁRDEZ, José Francisco

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

(54) Título: **Método y sistema de telepago electrónico, perfeccionados**

(57) Resumen:
Mejoras introducidas en la solicitud de patente de invención P201300530 ("Método y sistema de telepago electrónico").
La presente invención se refiere a un método de telepago electrónico que comprende: recibir en un dispositivo electrónico del comprador, la identificación de un comprador, de un vendedor, información bancaria del vendedor e identificación de una compra/venta; conectar una memoria externa con unos parámetros de cifrado; recibir un PIN; cifrar la información recibida junto con el PIN de acuerdo a los parámetros de cifrado; enviarla a un módulo de pago; realizar el pago a un módulo de cobro asociado con el usuario vendedor; donde inicialmente se ha enviado un primer mensaje de compra al vendedor identificando el objeto de compra; y sucesiva y simultáneamente se envían un mensaje al comprador identificando al usuario vendedor, información bancaria y de identificación de la compra/venta y otro mensaje al módulo de cobro identificando la compra/venta.

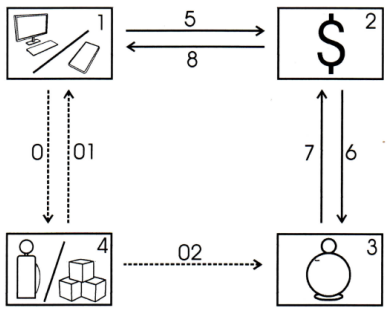

Figura 1

ES 2 607 427 B1

DESCRIPCIÓN

Mejoras introducidas en la solicitud de patente de invención P201300530 (“Método y sistema de telepago electrónico”)

Objeto de la invención

La presente invención se refiere en general al campo técnico de los métodos de comercio electrónico y más específicamente se refiere a una serie de mejoras introducidas en la solicitud de patente P201300530, del mismo titular, denominada “Método y sistema de telepago electrónico” enfocada a realizar pagos seguros entre un comprador y vendedor en transacciones electrónicas.

Antecedentes de la invención

Actualmente, es muy habitual que las operaciones de compra a través de internet se abonen por medio de métodos y sistemas de telepago. Una de las posibilidades es adquirir previamente a la operación de compra, una tarjeta de prepago en una entidad bancaria e introducir los datos que solicite el vendedor a través de la interfaz del vendedor. Esto motiva a menudo una fuerte desconfianza en los compradores debido a que habitualmente desconocen la interfaz utilizada (lo que conlleva que desconozcan los datos que deben aportar) y a que desconocen a que entidad le están proporcionando dichos datos.

Además, en función del sitio web, la forma de solicitar los datos varía y no siempre se solicitan los mismos datos y muchas veces lo único que conoce el comprador de una tienda web, son los datos que aparecen en su página web y nada más.

Es una realidad que las estafas provocadas por robo de datos proporcionados a través de internet hacen que los usuarios no se sientan seguros con los métodos de pago electrónico actuales, lo cual es un grave problema, ya que es fundamental para un método de telepago, no sólo que sea seguro, sino que sea percibido como seguro por el usuario.

Adicionalmente, muchos de los métodos de telepago electrónico existentes en el estado del arte están adaptados para su uso en los dispositivos portátiles de los usuarios, principalmente teléfono móvil, y aunque refuerzan la seguridad con claves personales, esto no es una protección definitiva ante casos de extravío o robo. El mayor riesgo puede considerarse la clonación de los dispositivos, ya que permite a los ciberdelincuentes hacer

un duplicado del sistema y copiar claves sin que el titular tenga conocimiento alguno. De esta forma, el ciberdelincuente no intercepta el contenido del pago realizado por el titular, pero sí le permite hacer pagos posteriormente suplantando su identidad.

Por todo ello, el estado del arte necesita nuevas soluciones en los métodos de telepago electrónico que aporten al usuario la seguridad necesaria tanto para realizar sus pagos, como ante la pérdida, clonación o utilización fraudulenta de sus dispositivos electrónicos.

Descripción de la invención

El presente certificado de adición describe una serie de mejoras introducidas en la solicitud de patente P201300530 “Método y sistema de telepago electrónico”, mediante las cuales se consigue obtener un proceso telepago electrónico que aporta al usuario la seguridad necesaria tanto para realizar sus pagos, como ante la pérdida, clonación o utilización fraudulenta de sus dispositivos electrónicos. Más en particular las mejoras inciden en la simplicidad y agilidad del proceso al simultanear el envío de datos desde el terminal del vendedor tanto al comprador como al módulo de cobro, de forma que si finalmente el comprador decide completar la transacción, el pago y la confirmación se agilizan reduciendo el número necesario de mensajes a intercambiar, a la vez que se mantiene o incluso se aumenta la seguridad del método mediante la comprobación de referencias en el módulo de cobro. El método de telepago electrónico para realizar un pago entre un usuario comprador y un usuario vendedor comprende los siguientes pasos:

a) recibir, en un dispositivo electrónico del usuario comprador, información que comprende al menos información de identificación del usuario vendedor, información bancaria del usuario vendedor e información de identificación de la compra/venta;
b) conectar un módulo de memoria externo al dispositivo electrónico, donde el módulo de memoria externo contiene unos parámetros de cifrado asignados previamente al usuario comprador;
c) recibir, en el dispositivo electrónico, un código PIN de identificación único del usuario comprador;
d) cifrar, en el dispositivo electrónico, la información recibida en el paso a) junto con el código PIN de identificación recibido en el paso c) de acuerdo a los parámetros de cifrado del módulo de memoria externo conectado en el paso b);
e) enviar un mensaje que contiene la información cifrada en el paso d), desde el dispositivo electrónico del usuario comprador, a un módulo de pago, a través de una red de telecomunicaciones;

f) descifrar el mensaje recibido en el módulo de pago;

g) realizar el pago, de acuerdo a la información contenida en el mensaje descifrado, desde el módulo de pago a un módulo de cobro asociado con el usuario vendedor;

donde el método está caracterizado por que comprende los siguientes pasos previos al paso a):

i. enviar, desde el dispositivo electrónico del usuario comprador, un primer mensaje de compra al dispositivo electrónico del vendedor, donde dicho primer mensaje de compra comprende información de identificación de un objeto de compra; de esta forma el comprador comunica al vendedor lo que quiere comprar (bien telemáticamente a través de una red de telecomunicaciones, bien personalmente en una tienda física); y

ii. una vez recibido en el dispositivo electrónico del vendedor el primer mensaje de compra:

1. enviar un segundo mensaje desde el dispositivo electrónico del vendedor al dispositivo electrónico del usuario comprador con información al menos de identificación del usuario vendedor, información bancaria del usuario vendedor e información de identificación de la compra/venta;
2. enviar un tercer mensaje desde el dispositivo electrónico del vendedor al módulo de cobro con información al menos de identificación de la compra/venta.

(Por tanto el vendedor, tan pronto recibe el mensaje con lo que quiere comprar el comprador, envía dos mensajes: envía un mensaje a un dispositivo electrónico del usuario comprador, y envía otro mensaje al módulo de cobro.)

Ventajosamente, el vendedor queda de esta manera perfectamente identificado, ya que para poder cobrar tiene que dar todos sus datos bancarios, pues el pago se realiza ingresando el importe en su Entidad de Cobro (banco, caja, etc.) y en su cuenta, lo cual es una garantía para el comprador.

Adicionalmente, la presente invención puede comprender, una vez realizado el pago desde el módulo de pago al módulo de cobro, los pasos de:

- verificar, por parte del módulo de cobro, la coincidencia entre una referencia de cobro contenida en la información de identificación de la compra/venta enviada desde el dispositivo electrónico del vendedor al módulo de cobro, con una referencia asociada al pago de la compra/venta;

- enviar, si las referencias de pago y cobro coinciden un mensaje de confirmación del pago, desde el módulo de cobro al módulo de pago, en cambio, si las referencias no coinciden, el módulo de cobro rechaza el pago;

- una vez recibido en el módulo de pago el mensaje de confirmación del pago, enviar un mensaje adicional que confirma el pago desde el módulo de pago al dispositivo electrónico del usuario comprador.

Adicionalmente, se contempla en una de las realizaciones de la invención que si al verificar la coincidencia entre referencias de pago y cobro en el módulo de cobro dichas referencias no coinciden, eliminar, por el módulo de cobro, la información de identificación de la compra/venta. De esta forma, se añade ventajosamente una medida más de seguridad y si el comprador finalmente no ejecuta una orden de pago no se realizará ningún cobro ni quedará registrado ningún dato (aunque hubiese comenzado los trámites y una orden de cobro haya sido enviada).

Opcionalmente puede incluirse un límite de tiempo para finalizar el pago desde que se recibe la referencia del cobro hasta que el comprador envía la referencia del cobro, que de ser sobrepasado, impedirá finalizar la transacción y el pago será rechazado. Ventajosamente se consigue así aumentar la seguridad del método al introducir una variable de tiempo en la que se puede establecer una ventana de tiempo razonable en la que completar la transacción.

La presente invención contempla la posibilidad de que, realizar el pago de acuerdo a la información contenida en el mensaje descifrado, desde el módulo de pago a un módulo de cobro asociado con el usuario vendedor, además comprenda comprobar que el número PIN de identificación único del mensaje descifrado corresponde con el número PIN de identificación único del usuario comprador, que ha sido almacenado previamente en el módulo de pago.

La presente invención contempla la posibilidad de que, realizar el pago de acuerdo a la información contenida en el mensaje descifrado desde el módulo de pago a un módulo de

cobro asociado con el usuario vendedor, además comprenda comprobar que la información de identificación del usuario vendedor y la información bancaria del usuario vendedor corresponden con un usuario vendedor registrado previamente en dicho módulo de cobro; y también, verificar que los datos del pago concuerdan con los datos de venta previamente recibidos.

Los parámetros de cifrado del usuario comprador son únicos y el cifrado de la información de cada pago utiliza unos parámetros de cifrado diferentes.

De acuerdo a una realización de la invención, se contempla almacenar en el módulo de pago los parámetros de cifrado asignados al usuario comprador. Así, el descifrado del mensaje recibido en el módulo de pago se puede realizar de acuerdo a los parámetros de cifrado asignados al usuario comprador almacenados en el módulo de pago.

La presente invención puede comprender además una interfaz instalada previamente en el dispositivo electrónico, donde la información recibida en el dispositivo electrónico del usuario comprador es introducida por el usuario comprador a través de dicha interfaz.

Los parámetros de cifrado pueden incluir, de acuerdo a una de las realizaciones de la invención, al menos unos parámetros de inicio de cifrado, una clave de cifrado y unos textos clave para el cifrado.

Un segundo aspecto de la presente invención se refiere a un sistema de telepago electrónico para realizar un pago entre un usuario comprador y un usuario vendedor que comprende:

- un dispositivo electrónico del usuario comprador configurado para enviar un primer mensaje de compra a un segundo dispositivo electrónico del usuario vendedor, donde dicho primer mensaje de compra comprende información de identificación de un objeto de compra; recibir información que comprende al menos información de identificación del usuario vendedor, información bancaria del usuario vendedor e información de identificación de la compra/venta; recibir un código PIN de identificación único del usuario comprador; cifrar la información recibida de acuerdo a unos parámetros de cifrado proporcionados por un módulo de memoria externo conectable al dispositivo electrónico; y enviar un mensaje, que contiene la información cifrada, a un módulo de pago a través de una red de telecomunicaciones;
- un dispositivo electrónico del usuario vendedor configurado para, una vez recibido el primer mensaje de compra:

- enviar un segundo mensaje al dispositivo electrónico del usuario comprador con información al menos de identificación del usuario vendedor, información bancaria del usuario vendedor e información de identificación de la compra/venta;
- enviar un tercer mensaje desde el dispositivo electrónico del vendedor al módulo de cobro con información al menos de identificación de la compra/venta;

- un módulo de memoria externo y conectable al dispositivo electrónico del comprador, que contiene los parámetros de cifrado;
- un módulo de pago configurado para recibir un mensaje enviado desde el dispositivo electrónico del comprador, descifrar el mensaje recibido y realizar el pago, de acuerdo a la información contenida en el mensaje descifrado, a un módulo de cobro asociado con el usuario vendedor;
- módulo de cobro configurado para recibir pagos enviados desde el módulo de pagos.

El módulo de pago, de acuerdo a una de las realizaciones de la presente invención, está además configurado para, una vez descifrado el mensaje recibido, comprobar que el número PIN de identificación único del usuario comprador, incluido en el mensaje descifrado, corresponde con el número PIN identificación único del usuario comprador, que ha sido almacenado previamente en el módulo de pago.

La presente invención, de acuerdo a una realización particular, comprende que:

- el módulo de cobro está además configurado para comprobar que la información de identificación del usuario vendedor y la información bancaria del usuario vendedor corresponden con un usuario vendedor registrado previamente en dicho módulo de cobro y también, verificar la coincidencia entre una referencia de pago de la compra/venta y una referencia de cobro de la compra/venta y además, enviar un mensaje de confirmación del pago al módulo de pago;

- el módulo de pago está además configurado para, una vez recibido el mensaje de confirmación del pago, enviar un mensaje adicional que confirma el pago al dispositivo electrónico del usuario comprador.

El módulo de memoria externo y conectable al dispositivo electrónico, que contiene los parámetros de cifrado, es, de acuerdo a una realización particular de la invención, una memoria de tipo USB de sólo lectura.

El dispositivo electrónico del usuario comprador y/o vendedor es, de acuerdo a una realización particular de la presente invención, un teléfono móvil, una tableta o un ordenador.

La presente invención provoca ventajosamente, a través de las características técnicas divulgadas, los efectos de dar seguridad y confianza al comprador (el que paga) y dar una seguridad integral a todo el sistema de pago (es seguro en la identificación del comprador; es inmune ante la pérdida, robo o utilización fraudulenta de los dispositivos que forman parte del sistema de pago; es inmune a la clonación y pirateo de datos). Además, la presente invención tiene muchas otras ventajas como, por ejemplo, prevenir las estafas a través de páginas web fraudulentas (que suplantan a otra auténtica) porque la presente invención no da “autorización de cobro”, sino que ejecuta una “orden de pago” y si los datos de la orden de pago y el titular de la cuenta no concuerdan, no se produce el pago.

Si nos roban, perdemos el teléfono móvil o nos piratean, un tercero tampoco puede efectuar pago alguno, pues carece de la Tarjeta/USB donde se almacenan los parámetros de cifrado necesarios y el código PIN (número de identificación personal).

1. En el supuesto de que nos roben o perdamos el teléfono móvil y la Tarjeta/USB, tampoco pasa nada, pues un tercero carece del código PIN y no pueden obtener este dato del teléfono móvil ni de la Tarjeta/USB, pues no consta ese dato en dichos soportes.

2. Si nos piratean y duplican una orden de pago, tampoco pueden hacer nada, pues el módulo de pago de nuestra Entidad de Pago no admitirá dos órdenes de pago iguales.

3. Si clonan el teléfono móvil, podrán hacer llamadas y operar en internet al igual que el titular, pero no podrán hacer pagos al carecer de la Tarjeta/USB y desconocer el PIN (aunque tengan y conozcan el programa de cifrado).

4. Incluso en un supuesto de que el empleado de una tienda esté en connivencia con una organización de delincuentes y al tiempo que nos clonan el teléfono móvil y nos

piratean una orden de pago, el empleado le envía una copia de todos los datos de compra con la finalidad de descifrar la clave, tampoco en este supuesto serviría de nada; porque cada orden de pago está perfectamente individualizada y no se pueden reutilizar los parámetros de cifrado, que se almacenan en el módulo externo de memoria y varían en cada módulo de memoria asignado a un comprador, de forma que no existen dos memorias Tarjetas/USB con contenido igual.

Otras ventajas adicionales de la presente invención son que toda la operación del pago se realiza dentro de un circuito propio del comprador, ya que, el Comprador se conecta únicamente con su Entidad de Pago y a través de su propia red de telecomunicación, en lugar de entregar sus datos de pago al Vendedor.

El módulo de memoria con las claves de cifrado tampoco se introduce en ningún dispositivo ajeno al comprador (como sí ocurriría con un tarjeta de crédito), con lo que nunca sale del poder del Comparador.

La presente invención también agiliza el pago en momentos puntuales, en los cuales, una sola persona podría atender perfectamente el pago simultaneo de varias personas. O también en aquellos acontecimientos de masas, en los cuales es necesario atender múltiples pagos en un tiempo muy breve y no se dispone de infraestructuras apropiadas de comunicación. La presente invención solo necesita cobertura por parte de una red de telecomunicaciones y una caja central con conexión a internet y múltiples monitores en los que los usuarios puedan realizar sus pagos de forma simultánea. Además, este sistema, permite un mejor control de todos los pagos.

Descripción de los dibujos

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características del invento, de acuerdo con un ejemplo preferente de realización práctica del mismo, se acompaña como parte integrante de dicha descripción, un juego de dibujos en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

La figura 1.- Muestra un diagrama de bloques que recoge el funcionamiento de la invención.

La figura 2 describe, de acuerdo a una realización de la invención, la relación entre la información cifrada y el módulo de pago.

Descripción detallada de la invención

La presente invención contempla la seguridad de los sistemas de pago electrónicos bajo tres aspectos:

1. La seguridad de la transferencia económica (que viene determinada por la seguridad del sistema de cifra).

2. La seguridad que da el sistema al comprador, desde el punto de vista del propio comprador; es decir, la confianza y seguridad que siente el comprador operando con estos sistemas de pago.

3. La seguridad del sistema ante la pérdida, robo, clonación o utilización fraudulenta del sistema de pago.

En cuanto a “la seguridad de la transferencia económica”, los sistemas de pago ofrecidos por el estado del arte son suficientemente seguros (se basan en sistemas de cifra muy seguros); por lo tanto, no es este el foco de la presente invención, pero en relación a los otros dos aspectos (“seguridad al comprador” y “seguridad ante la posible utilización fraudulenta del sistema”), es donde la presente invención concentra sus principales características.

La presente invención propone una interfaz que es la base de este sistema de pago, ya que la principal característica de la presente invención se centra en cambiar el protagonismo en una compra, del vendedor (como funciona según el estado del arte), al comprador. La operación de pago transcurre según la interfaz de la presente invención, desarrollada sobre un dispositivo electrónico del usuario comprador, ya sea su teléfono móvil, tableta, ordenador personal u otro dispositivo similar. En cuanto a la seguridad ante la pérdida, clonación o cualquier otra utilización fraudulenta del sistema de pago, la presente invención desarrolla un sistema de cifrado que por un lado diversifica las fuentes y, por otro, individualiza el cifrado para cada usuario y operación.

La figura 1 muestra el método de operación de la presente invención de acuerdo a una realización particular, donde asumiendo que, un usuario comprador que decide comprar una

cosa o servicio, para hacer el pago se conecta a través de internet (mediante ordenador, teléfono móvil o dispositivo electrónico con funciones similares) y utiliza como sistema de pago la presente invención, comprende:

- El Comprador (1), una vez seleccionado el producto a comprar, abre la interfaz de la presente invención y pulsa el icono “comprar” (0); es decir, envía un mensaje (0) al vendedor (4), indicándole los objetos que quiere comprar [Nota.- el vendedor, tiene que admitir esta forma de pago].

- El Vendedor (4), al recibir el mensaje de compra (0), envía dos mensajes: uno al comprador (01), con la información de identificación del vendedor, del banco y de la compra/venta; y otro al módulo de cobro (02), con la información de identificación de la compra/venta.

1. El Comprador (1) cumplimenta la “orden de pago” y envía esta orden de pago (5) a su “Entidad de Pago” (2).

2. La Entidad de Pago (2), verifica la orden de pago y emite el pago (6) a la “Entidad de Cobro” (3).

3. La Entidad de Cobro (3), verifica si la referencia del pago -de la compra/venta- (este dato lo recibió el comprador en el mensaje “01”), concuerda con la referencia de venta –de la compra/venta- (este dato lo recibió el módulo de cobro en el mensaje “02”).

4. La Entidad de Cobro (3), si concuerda la referencia de pago y la referencia de venta, ingresa el importe del pago en la cuenta que tiene el Vendedor y acusa recibo del pago (7) a la Entidad de Pago (2).

5. La Entidad de Pago (2), al recibir el acuse del pago (7), comunica el pago (8) al Comprador (1).

6. El Comprador (1), recibe el acuse de pago (8) –lo que le confirma la compra- Fin. Imprimiendo la orden de pago con el acuse de pago, se obtiene el tique o factura.

El Comprador por tanto, independientemente de lo que compre y a quien compre, a la hora de pagar, la orden de pago siempre se la envía a su “Entidad de Pago”.

La Figura 1, muestra que el Comprador (1), para pagar, únicamente contacta con su “Entidad de Pago” (2), por lo que el Comprador, a la hora de pagar, siempre ejecuta las mismas pautas, independientemente de quien sea el Vendedor.

Este hecho da mucha seguridad al Comprador: sabe perfectamente lo que tiene que hacer y siempre es igual.

El Comprador, a la hora de pagar, no tiene que dar ningún dato o referencia de sus datos de pago, ya los tiene su Entidad de Pago; es suficiente con que se identifique a su Entidad de Pago, por ejemplo introduciendo su nombre y/o DNI, y emita la orden de pago. La orden de pago identifica de forma inequívoca al Comprador, ya que “la clave de cifrado” y “la clave propia de cada cifrado”, que se utilizan para cifrar, son exclusivas de cada comprador, es decir, no existen dos compradores con las mismas claves. El Comprador contacta únicamente con su Entidad de Pago, para enviarle la orden de pago; siendo la Entidad de Pago, la que se encarga de ejecutar el pago.

La orden de pago, por tanto, de acuerdo a una de las realizaciones de la invención comprende:

- la identificación del comprador (nombre, apellidos y DNI), que no va cifrada ni necesitan ser introducidos por el comprador, ya que la interfaz los obtiene directamente del módulo de pago (si el comprador prevé utilizar más de un teléfono móvil u ordenador, podrá pagar desde cualquiera de ellos, pero previamente tendrá que contactar con su Entidad de Pago, para incorporar a cada uno de los dispositivos electrónicos la interfaz Ste con el programa de cifra. En todos los dispositivos electrónicos del comprador, el programa de cifra puede ser es el mismo y utilizar la misma tarjeta/USB; o bien, distintos y utilizar distinta tarjeta/USB, por ejemplo: para los dispositivos personales utilizar un primer programa y una misma tarjeta/USB; y para los dispositivos del trabajo, utilizar un segundo programa y otra tarjeta/USB).

- El texto cifrado, donde a su vez se incluyen:

    - la identificación del vendedor, información bancaria del vendedor e información de identificación de la compraventa.

    - El PIN. El PIN, es el único dato que introduce el comprador sobre él mismo, como acto previo a la cifra. Se trata de un dato de identificación “interno” del comprador y únicamente lo conocen el propio comprador y el módulo de

pago, sin que conste en ninguno de los soportes técnicos del comprador (como ordenador o teléfono móvil).

El Comprador, utilizando la presente invención, lo que ejecuta es una “orden de pago” con el contenido comentado anteriormente; mientras que con otros sistemas, lo que se ejecuta en una “autorización de cobro”, porque el Comprador lo que hace es aportar una serie de datos (datos que pertenecen al Comprador), para que el Vendedor pueda con estos datos cobrar.

En cambio, al ejecutar el Comprador una “orden de pago”, es el Vendedor quien tiene que proporcionar todos sus datos (el Vendedor queda plenamente identificado) y lo que hace el Comprador, es ordenar a su Entidad de Pago (banco, caja, etc.) que ingrese el pago en la Entidad de Cobro (banco, caja) y en cierta cuenta de la cual es titular el Vendedor. Comparando esta forma de actuar, con un pago en el mundo mercantil clásico, se diría que la “orden de pago” equivale a un “cheque nominativo barrado” (este cheque, únicamente lo puede cobrar el titular del cheque e ingresándolo en su entidad bancaria).

Además, de acuerdo a la realización preferente de la invención, las fuentes para el cifrado de información se diversifican para aumentar la seguridad ante la utilización fraudulenta del sistema por terceras personas (robo, pérdida, pirateo, clonación, etc.).

Para hacer la cifra, o cifrado, se requieren distintas fuentes, lo que en sí mismo no aumenta la seguridad de la cifra, pero la finalidad de usar distintas fuentes, es la seguridad del sistema de pago ante la pérdida, robo, clonación o utilización fraudulenta de los dispositivos del sistema.

Las fuentes de cifra pueden ser, por ejemplo:

- Un ordenador, teléfono móvil, tableta o dispositivo electrónico con funciones similares, donde está el programa de cifrado.
- Una Tarjeta de memoria o memoria USB, donde están los parámetros de cifrado.
- El comprador, que conoce el código PIN.

Cualquier programa de cifra puede ser utilizado por la presente invención siempre que cumpla tres condiciones:

1. Que el programa de cifra esté en el ordenador o teléfono móvil.

2. Que el programa de cifra, para que pueda cifrar, necesite los parámetros de cifrado de un módulo de memoria externo como puede ser una tarjeta o un USB.

3. Y para que la cifra sea válida, necesite un código de identificación único, como un código PIN (Personal Identification Number; en español: Número de Identificación Personal).

Para que la cifra sea válida, necesita el código PIN correcto. El PIN va cifrado, por lo que aunque el PIN sea incorrecto, el cifrado se genera igual, pero la Entidad de Pago no lo dará por válido.

El módulo de memoria externo, utilizado para proveer al dispositivo electrónico de los parámetros de cifrado puede ser, de acuerdo a diferentes realizaciones de la invención, una tarjeta de memoria o una memoria USB. Preferiblemente se escoge una memoria de tipo USB por considerar que se ajusta mucho mejor a las necesidades de la presente invención (las memorias USB tienen una gran capacidad de almacenamiento de datos y son fácilmente conectables al ordenador, teléfono móvil, tabletas, etc.). Estas memorias vienen con toda la información preestablecida y no es posible ampliar, modificar o variar dato alguno, ya que son de “sólo lectura”. El contenido de la Tarjeta/USB de acuerdo a la presente invención, son los parámetros de cifrado.

En cuanto al código de identificación único o código PIN, no consta en la memoria (Tarjeta o USB), ni en el ordenador, ni en el teléfono móvil; el PIN sólo lo conocen el comprador y el módulo de pago. La finalidad del PIN es confirmar que, quien compra y paga es el comprador y evitar el uso fraudulento realizado por terceras personas. De acuerdo a una de las realizaciones de la invención, el código PIN consiste en un código alfanumérico con un mínimo de 7 caracteres, aunque es el comprador quien determina el número de caracteres que considere conveniente.

Por tanto, siguiendo un ejemplo de funcionamiento de una realización particular, la diversificación de fuentes de la presente invención opera del siguiente modo:

A.- La persona que desea hacer un pago para pagar una compra con este sistema, abre la interfaz del Sistema de telepago electrónico “Ste” de la presente invención utilizando un dispositivo electrónico.

B.- Después, comunica al vendedor qué compra y que quiere pagar lo comprado.

C.- El vendedor, al tener conocimiento de la compra y que la forma de pago es mediante el Sistema “Ste”, envía dos mensajes: uno al comprador con los datos suyos, del banco y de la compra/venta; y otro al módulo de cobro, con los datos de la compra/venta.

D.- El comprador, al recibir el mensaje del vendedor con los datos, ya puede hacer la orden de pago. Y es aquí, en esta fase donde se aplica el método y sistema de cifrado de diversificación de fuentes.

Para hacer la orden de pago, todos los datos los proporciona el Vendedor. Y una vez hecha, se envía al módulo de pago.

Ahora bien, si se envía la orden de pago tal cual se confecciona, es decir, sin cifrar, cualquier persona podría tener acceso a los datos de identificación y en consecuencia, dar órdenes de pago suplantando la identidad del comprador. Por lo que, para evitar esto, está el cifrado de los datos de la orden de pago, que tiene más bien una función de identificación, que de privacidad.

E.- El cifrado de la orden de pago de acuerdo a una realización concreta de la invención, cumple los siguientes pasos:

1. Una vez cumplimentados los datos de la orden de pago, se hace clic en un icono mostrado por la interfaz del dispositivo electrónico “continuar”.
2. En la pantalla del dispositivo electrónico se muestra un mensaje requiriendo introducir una memoria externa, por ejemplo “introduzca Tarjeta/USB”.
3. Al introducir la Tarjeta/USB en el dispositivo electrónico, la pantalla del dispositivo electrónico muestra un mensaje que requiere introducir un código PIN de identificación único del usuario comprador, por ejemplo: “escriba código PIN”. Una vez recibido el código PIN, el dispositivo electrónico cifra la información en base a los parámetros de cifrado almacenados en la Tarjeta/USB y, cuando finaliza el cifrado, la pantalla del dispositivo electrónico muestra un mensaje autorizando la extracción del módulo de memoria conectado, por ejemplo: “Retire Tarjeta/USB”.

4. Al retirar la Tarjeta/USB, la pantalla del dispositivo electrónico ofrece una opción de enviar el mensaje cifrado (la orden de pago) al módulo de pago para que efectúe el pago: por ejemplo, la interfaz puede estar configurada para mostrar un simple icono que recite “enviar” (obviamente hay que pulsarlo para continuar). El código PIN está incluido y cifrado en la propia orden de pago.

5. El mensaje enviado, que es la orden de pago, es recibido por el módulo de Pago, donde es descifrado de forma automática y, si todo es correcto, la da por válida.

Si el módulo de pago recibe dos órdenes de pago iguales, la segunda no es válida. Cada cifrado, utiliza una clave de cifrado propia y diferente a las demás y sólo se puede utilizar una única vez. Por lo tanto, no pueden existir dos cifrados iguales, aunque el contenido del texto a cifrar sea idéntico. La “clave de cifrado propia de cada cifrado”, es independiente y distinta de las “clave de cifrado del texto”; lo que significa, que cada cifrado emplea simultáneamente dos claves de cifrado distintas.

Gracias a la diversificación de fuentes y la individualización del cifrado, la presente invención garantiza la seguridad para los pagos del comprador incluso en los supuestos de robo de su dispositivo electrónico, pérdida o uso fraudulento. Incluso en el supuesto hipotético de que un tercero consiga descifrar las claves de una orden de pago, tampoco en este supuesto le sería de ninguna utilidad, puesto que cada orden de pago, al estar perfectamente individualizada, no permite reutilizar los parámetros de un cifrado para otro cifrado posterior.

La figura 2 describe, de acuerdo a una realización de la invención, la relación entre la información cifrada y el módulo de pago, donde se evidencia la diversificación de fuentes, lo que implica, que ningún módulo dispone de la totalidad de la información:

- El Comparador (1) emite una orden de pago (5) al módulo de pago (2) de su Entidad de Pago.
- La orden de pago (5) es recibida directamente en un “módulo de cifrado” (2-A) del módulo de pago (2) de la Entidad de Pago.
- En el “módulo de cifrado” (2-A), están los programas de cifrado/descifrado y lo primero que se hace es determinar si la identificación del Comprador está operativa. Si está operativa, continúa con el proceso y para ello empieza a recabar a los distintos módulos los datos que se necesitan para descifrar la orden de pago y poderla dar por válida:
- Se pone en contacto con el “módulo de claves de cifrado” (2-B) y le pide las claves de cifrado de la Tarjeta/USB del usuario comprador, previamente almacenadas.
- Se pone en contacto con el “módulo de códigos PIN” (2-C) y le pide el PIN de la Tarjeta/USB del usuario comprador, previamente almacenado.
- Se pone en contacto con los “módulos de textos clave”, hay 3 módulos (2-D, 2-E y 2-F) y le pide los textos clave de la Tarjeta/USB del comprador, almacenados previamente”.

- Si el texto descifrado es válido, comunica al “módulo de pago” (2-G) la orden de pago y este último departamento (2-G) es el que emite el pago (6) al módulo de cobro (3) de la Entidad de Cobro.
- La Entidad de Cobro verifica si la referencia del pago -de la compra/venta-, concuerda con la referencia de venta –de la compra/venta- (este dato lo recibió el módulo de cobro en el mensaje “02”).

Distintos tipos de cifrado pueden emplearse de forma satisfactoria en la presente invención, siempre y cuando permitan individualizar cada cifrado y cumplan los criterios anteriores para diversificar las fuentes. A continuación se presentan, a modo de ejemplo, dos tipos de cifrado que se utilizan en distintas realizaciones particulares de la invención: “cifrado por valor de los caracteres” y “cifrado por mezcla de caracteres en uno”.

Para explicar estos dos tipos de cifrado de una forma clara y práctica, en lugar de mostrar el cifrado de una orden de pago completa se utilizarán únicamente un par de palabras, ya que el proceso es el mismo.

- Caso práctico: Un caso típico de compra por internet, es comprar un libro; y ese libro hay que pagárselo al Vendedor: “Librería ABC”; en los dos casos que se detallan a continuación, se cifrará únicamente el nombre del Vendedor: “Librería ABC” (por simplicidad de la explicación, no se distingue entre mayúsculas y minúsculas).
- En los métodos de cifrado que permiten individualizar la cifra, es necesario dar el dato de individualización del cifrado. En los dos casos de cifrado que se detallan, se requieren dos datos para individualizar la cifra: Texto de inicio y Carácter de inicio.
  - Texto de inicio: en los casos mostrados, por ejemplo el párrafo de inicio es el 320.
    - Al decir: “el párrafo de inicio es el 320”, significa que el párrafo que sirve de referencia para el inicio de la cifra, es el 320
    - El párrafo de inicio (en este caso concreto, el 320), una vez utilizado como párrafo de inicio, ya no se puede volver a utilizar como párrafo de inicio; de ahí, que la cifra quede perfectamente individualizada.
    - Por motivos de seguridad, cada Tarjeta/USB debe contener un número mínimo de párrafos y cada párrafo debe contener un número mínimo de caracteres y un número máximo.

- Carácter de inicio: en los casos mostrados, por ejemplo el carácter de inicio es el 753.

    - Al decir: “el carácter de inicio es el 753”, significa que, empezando a contar los caracteres en el párrafo 320, la cifra empieza en el carácter 753 y continúa con los siguientes caracteres.

    - Si cada párrafo tiene, por ejemplo, entre 70 y 230 caracteres, aun suponiendo que los párrafos 320, 321, 322 y 323 tengan el máximo de caracteres (es decir, 230), el inicio de la cifra comenzaría en el carácter 123 del párrafo 323, de esta forma nadie puede identificar los textos clave.

- Para ambos casos se supone que el carácter 753 y siguientes son: “**casaxy32xbf532zap3hxf hs074axzrpo st …**” (texto clave).

- Por último, es de destacar aquí que, en los dos casos que se exponen a modo de ejemplo, **los “textos clave”** son los que **permiten individualizar la cifra**. De los “textos clave” sale la “clave de cifrado propia de cada cifrado” (el “texto clave” varía en cada cifrado y no se repite).

Comenzando con el primer caso, correspondiente a un cifrado por valor de los caracteres, una vez planteados los supuestos con los que se cuenta, el cifrado por valor de los caracteres, se basa en dar a cada carácter un valor y este valor sustituye al carácter (por ejemplo:, la “a” tiene un valor “1”, lo que significa que se sustituye la “a”, por un “1”); ahora bien, una mera sustitución de un carácter por un valor, no es suficiente para garantizar el cifrado (sería fácilmente descifrable). Por ello, en el “cifrado por valor de los caracteres”, a los caracteres a cifrar, se les añaden otros caracteres (estos caracteres que se añaden, es lo que se denominan “textos clave” y se encuentran en la Tarjeta/USB), ejecutándose entre unos y otros caracteres, una serie de operaciones matemáticas (ya que los caracteres han sido sustituidos por valores), cuyo resultado es el cifrado.

En este caso práctico, por simplicidad, a los caracteres se les asigna un valor correlativo del “1” al “38” de acuerdo a la siguiente tabla que relaciona la clave de cifrado con el valor de los caracteres para este ejemplo:

Caracteres	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**ñ**	**o**	**p**	**q**	**r**
Valoración	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Caracteres	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**		**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Valoración	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38

No obstante, los valores pueden ser otros (por ejemplo: la “a” un valor de “536”, la “b” un valor de “189”, la “c” un valor de “725”, etc.)

A continuación, el programa de cifrado, antes de comenzar a cifrar, lo primero que hace es contar el número de caracteres que tiene el texto a cifrar. En este caso concreto, el texto “Librería ABC” contiene 12 caracteres, contando también los espacios entre palabras como un carácter. Así que, teniendo en cuanta que el texto a cifrar tiene 12 caracteres, el programa de cifra selecciona de los textos clave que están en la Tarjeta/USB, el triple de caracteres y los divide en 3 grupos de 12 caracteres. Siguiendo con el supuesto expuesto anteriormente el resultado es el siguiente: “casaxy32xbf5”, “32zap3hxf hs” y “074axzrpo st”.

Cada carácter tiene, por tanto, un valor y en este caso concreto, el valor esta determinado en la relación de valores, tal y como se ha mostrado en la tabla anterior. Según esta relación de valores, el texto a cifrar “Librería ABC” tiene los siguientes valores: 12, 09, 02, 19, 05, 19, 09, 01, 28, 01, 02, 03.

Texto a cifrar	**L**	**i**	**b**	**r**	**e**	**r**	**i**	**a**		**A**	**B**	**C**
Valor de los caracteres	12	9	2	19	5	19	9	1	28	1	2	3

Y para cifrar el texto, en este supuesto, se realizan las siguientes operaciones para evitar que una tercera persona pueda descifrar el valor de los caracteres aunque tenga pleno conocimiento del contenido de la orden de pago:

A los valores citados de “Librería ABC”….:12, 09, 02, 19, 05, 19, 09, 01, 28, 01, 02, 03
se suman los valores de “casaxy32xbf5”: 03, 01, 20, 01, 25, 26, 32, 31, 25, 02, 06, 34
y de “32zap3hxf hs”……..: 32, 31, 27, 01, 17, 32, 08, 25, 06, 28, 08, 20
y se restan los valores de “074axzrpo st”: 29, 36, 33, 01, 25, 27, 19, 17, 16, 28, 20, 21
el resultado son los siguientes valores: 18, 05, 16, 20, 22, 50, 30, 40, 43, 03, -04, 36

Texto a cifrar	**L**	**i**	**b**	**r**	**e**	**r**	**i**	**a**		**A**	**B**	**C**
Valor de los caracteres	12	9	2	19	5	19	9	1	28	1	2	3
Texto clave - grupo 1º	c	a	s	a	x	y	3	2	x	b	f	5
Valor de los caracteres (sumar)	3	1	20	1	25	26	32	31	25	2	6	34
Texto clave - grupo 2º	3	2	z	a	p	3	h	x	f		h	s
Valor de los caracteres (sumar)	32	31	27	1	17	32	8	25	6	28	8	20

Texto clave - grupo 3º	0	7	4	a	x	z	r	p	o		s	t
Valor de los caracteres (restar)	29	36	33	1	25	27	19	17	16	28	20	21
Texto cifrado (resultado operaciones)	18	5	16	20	22	50	30	40	43	3	-4	36

Para descifrar lo cifrado, hay que hacer el proceso inverso:

A los valores cifrados recibidos…...: 18, 05, 16, 20, 22, 50, 30, 40, 43, 03, -04, 36;
se restan los valores de “casaxy32xbf5”: 03, 01, 20, 01, 25, 26, 32, 31, 25, 02, 06, 34;
se restan los valores de “32zap3hxf hs”: 32, 31, 27, 01, 17, 32, 08, 25, 06, 28, 08, 20;
se suman los valores de “074axzrpo st”: 29, 36, 33, 01, 25, 27, 19, 17, 16, 28, 20, 21.
El resultado de estas operaciones es: 12, 09, 02, 19, 05, 19, 09, 01, 28, 01, 02, 03.
Si pasamos los valores a caracteres, sale: Librería ABC.

Texto cifrado para descifrar	18	5	16	20	22	50	30	40	43	3	-4	36
Texto clave - grupo 1º	c	a	s	a	x	y	3	2	x	b	f	5
Valor de los caracteres (restar)	3	1	20	1	25	26	32	31	25	2	6	34
Texto clave - grupo 2º	3	2	z	a	p	3	h	x	f		h	s
Valor de los caracteres (restar)	32	31	27	1	17	32	8	25	6	28	8	20
Texto clave - grupo 3º	0	7	4	a	x	z	r	p	o		s	t
Valor de los caracteres (sumar)	29	36	33	1	25	27	19	17	16	28	20	21
Resultado operaciones	12	9	2	19	5	19	9	1	28	1	2	3
Sustitución de los valores por caracteres	**L**	**i**	**b**	**r**	**e**	**r**	**i**	**a**		**A**	**B**	**C**

Por tanto, la clave de cifrado, en este ejemplo concreto está determinada así: la “a” vale 1; la “b” vale 2; la “c” vale 3; etc. En cambio la clave propia de cada cifrado, viene dada por los textos clave; así, en este ejemplo concreto son: “casaxy32xbf532zap3hxf hs074axzrpo st”.

Por lo tanto, en el hipotético supuesto de que un delincuente consiguiese descifrar la “clave de cifrado” y la “clave propia de un cifrado concreto” de una orden de pago, ello no permitiría hacer posteriormente ningún cifrado válido, porque para hacer un cifrado posterior válido se requiere, además de “la clave de cifrado” (que ya la sabe), de una nueva “clave propia para ese cifrado posterior” que requiere toda orden de pago y esta clave propia de cada cifrado, la componen los textos clave que se encuentran en la Tarjeta/USB.

En cuanto al segundo caso de ejemplo, el cifrado por mezcla de caracteres en uno, se basa en la sustitución de dos caracteres por uno solo (por lo que a este tipo de cifra se le denomina en este documento como “cifrado por mezcla de caracteres en uno”); esto implica, que el texto a cifrar se mezcla o combina con otro texto y de esta mezcla, sale un tercer texto; ahora bien, teniendo en cuenta que existe la posibilidad de que de forma fraudulenta se conozcan los datos a cifrar, para evitar que nadie pueda descifrar ninguna de las clave de cifra , esta operación se realiza dos veces. Los textos de mezcla, son los “textos clave” que se encuentran en la Tarjeta/USB.

En el caso práctico que se muestra de ejemplo, la combinación o mezcla de caracteres se hace siguiendo el patrón del siguiente diagrama, aunque puede tener diversas combinaciones, por lo tanto la variedad de diagramas es amplísima; lo que da una gran seguridad al sistema:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9
a	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b
b	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e
c	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h
d	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l
e	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p
f	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w
g	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	
h	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0
i	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2
j	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5
k	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9
l	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g
m	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ
n	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u
ñ	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4
o	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f

p	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q
q	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1
r	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i
s	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v
t	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8
u	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o
v	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6
w	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r
x	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a
y	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t
z	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d
	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y
0	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n
1	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j
2	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c
3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3
4	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x
5	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s
6	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m
7	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k
8		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
9	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z		0	1	2	3	4	5	6	7

El programa de cifrado instalado en el dispositivo electrónico, antes de comenzar con el cifrado, lo primero que hace es contar el número de caracteres que componen el texto a cifrar (en este caso en concreto, como ya se ha dicho, son 12 caracteres).Teniendo en cuenta que el texto a cifrar tiene 12 caracteres, el programa de cifrado selecciona de los textos clave (que están en la Tarjeta/USB), el doble de caracteres y los divide en 2 grupos de 12 caracteres. Siguiendo con los supuestos planteados al inicio de los casos prácticos, el resultado es el siguiente: “casaxy32xbf5” y “32zap3hxf hs”.

Para cifrar el texto, hay que tener en cuenta que el texto “Librería ABC”, corresponde a las filas y los caracteres del texto clave “casaxy32xbf5”, corresponden a las columnas. A continuación se procede con las siguientes operaciones:

1. Primero nos situamos en la fila “l” del diagrama anteriormente mostrado (esta “l”, se corresponde con la letra “L” de Librería) y después en la columna “c” (esta “c”, se corresponde con la letra “c” de “casaxy32xbf5”) y donde confluyen la fila con la columna está la letra “j”;

2. Continuando con el siguiente carácter , nos situamos en la fila “i” (esta “i”, se corresponde con la primera “i” de Librería) y después en la columna “a” (esta “a”, se corresponde con primera “a” de “casaxy32xbf5”) y donde confluyen la fila con la columna está el número “3”;
3. Y así sucesivamente. El resultado es: “j3xjdqx4mdkd”

Fila	L	i	b	r	e	r	i	a		A	B	C	Texto a cifrar
Columna	c	a	s	a	x	y	3	2	x	b	f	5	Texto clave (primer grupo)
Resultado	**j**	**3**	**x**	**j**	**d**	**6**	**x**	**4**	**m**	**d**	**k**	**d**	Que pasa a ser fila en la siguiente fase

A continuación, se realiza la misma operación con este resultado de “j3xjdqx4mdkd” y con el texto clave “32zap3hxf hs”, donde el resultado “j3xjdqx4mdkd” corresponde a las filas y los caracteres del texto clave “32zap3hxf hs” corresponden a las columnas:

- Primero nos situamos en la fila “j” del diagrama (esta “j”, se corresponde con la primera “j” de “j3xjdqx4mdkd”) y después en la columna “3” (este “3”, se corresponde con el primer “3” de “32zap3hxf hs”) y donde confluyen la fila con la columna está un espacio “[espacio]”;
- Continuamos con el proceso y nos situamos en la fila “3” (este “3”, se corresponde con el “3” de “j3xjdqx4mdkd”) y después en la columna “2” (este “2”, se corresponde con el “2” de “32zap3hxf hs”) y donde confluyen la fila con la columna está la letra “x”;
- Y así sucesivamente. El resultado es: “ x 60wiltbh3”.

Fila	**j**	**3**	**x**	**j**	**d**	**6**	**x**	**4**	**m**	**d**	**k**	**d**	Resultado de la primera combinación
Columna	3	2	z	a	p	3	h	x	f		h	s	Texto clave (segundo grupo)
Resultado		**x**		**6**	**0**	**w**	**i**	**l**	**t**	**b**	**h**	**3**	Mensaje cifrado que recibe el módulo de pago de la Entidad de Pago

El descifrado se hace siguiendo el proceso inverso. El texto a cifrar junto con el texto clave producen el cifrado, por lo tanto, sabiendo el texto clave y el cifrado, se puede conocer el texto cifrado: Librería ABC. Para descifrar el texto se tiene en cuenta que se comienza por el segundo grupo de textos clave (“32zap3hxf hs”), el cual ocupa las columnas, ya que el proceso inverso va del final al principio; y se empieza por las columnas, porque para cifrar se empieza por las filas. Y el texto cifrado recibido “ x 60wiltbh3”, es el carácter clave de la columna. Se realizan las siguientes operaciones:

1. Primero nos situamos en la columna “3” del diagrama (este “3”, se corresponde con el primer “3” de “32zap3hxf hs”) y después en la columna buscamos el carácter clave “[un espacio]” (este “[espacio]”, se corresponde con el primer carácter de “espacio” del texto cifrado recibido, que es la orden de pago: “ x 60wiltbh3”), determinada así a qué altura de la columna nos encontramos, vemos qué letra de fila le corresponde, que en este caso es la “j”;
2. Continuamos con el proceso y nos situamos en la columna “2” (este “2”, se corresponde con el “2” de “32zap3hxf hs”) y después en la columna buscamos el carácter clave “x” (esta “x”, se corresponde con “x” de “ x 60wiltbh3”), determinada así a qué altura de la columna nos encontramos, vemos qué letra de fila le corresponde, que en este caso es el “3”;
3. Y así sucesivamente. El resultado es: “j3xjdqx4mdkd”.

Columna	3	2	z	a	p	3	h	x	f		h	s	Texto clave (segundo grupo)
Clave-Columna		*x*		*6*	*0*	*w*	*i*	*l*	*t*	*b*	*h*	*3*	Mensaje cifrado recibido por Entidad de Pago
Resultado	j	3	x	j	d	q	x	4	m	d	k	d	Letra de fila (que pasa a ser clave-columna en la siguiente fase)

A continuación, se hace la misma operación con este resultado de “j3xjdqx4mdkd” y con el primer grupo de texto clave “casaxy32xbf5”, teniendo en cuenta que el primer grupo de texto clave “casaxy32xbf5”, corresponde a las columnas y el resultado “j3xjdqx4mdkd”, pasa a ser el carácter clave de la columna. Se realizan las siguientes operaciones:

1. Primero nos situamos en la columna “c” del diagrama (esta “c”, se corresponde con la “c” de “casaxy32xbf5”) y después en la columna buscamos el carácter clave “j” (esta “j”, se corresponde con la primera “J” de “j3xjdqx4mdkd”), determinada así a qué altura de la columna nos encontramos, vemos qué letra de fila le corresponde, que en este caso es la “l”;
2. Continuamos con el proceso y nos situamos en la columna “a” (este “a”, se corresponde con la primera “a” de “casaxy32xbf5”) y después en la columna buscamos el carácter clave “3” (este “3”, se corresponde con el “3” de “j3xjdqx4mdkd”), determinada así a qué altura de la columna nos encontramos, vemos qué letra de fila le corresponde, que en este caso es la “i”;
3. Y así sucesivamente. El resultado es: “Librería ABC”.

Columna	c	a	s	a	x	y	3	2	x	b	f	5	Texto clave (primer grupo)
Clave-Columna	j	3	x	j	d	6	x	4	m	d	k	d	Resultado de la primera fase de descifra
Resultado	**L**	**i**	**b**	**r**	**e**	**r**	**i**	**a**		**A**	**B**	**C**	Que es el texto cifrado

MODO DE REALIZACIÓN DE LA INVENCIÓN:

La mejor forma de explicar el modo de realización de la invención, es mediante un caso práctico completo de acuerdo a una de las realizaciones de la invención:

NOTAS PREVIAS.

A.- El Comprador, para poder utilizar este sistema de pago, previamente ha tenido que contactar con lo que denomino su "Entidad de Pago" (es decir: banco, caja, entidad de tarjetas, etc.) y solicitar esta forma de pago. Ello conlleva:

a) Que el Comprador tiene que tener en su Entidad de Pago un importe económico (cuenta, tarjeta de pago, o cualquier otro tipo de depósito económico disponible) y del cual se hacen los pagos.
b) Que la Entidad de Pago le dé al Comprador todos los datos necesarios para poder operar con el Ste.

B.- El Vendedor, para poder utilizar este sistema de pago, previamente ha tenido que contactar con lo que denomino su "Entidad de Cobro" (es decir: banco, caja, entidad de tarjetas, etc.) y solicitar esta forma de cobro. Ello conlleva:

a) Que el Vendedor tiene que tener en su Entidad de Cobro una cuenta en la cual se pueda ingresar el importe económico de la venta.
b) Que la Entidad de Cobro le dé al Vendedor todos los datos necesarios para contactar entre ambos de forma segura.

C.- Para que el Ste sea operativo, es necesario que tanto la "Entidad de Pago", como la "Entidad de Cobro", admitan esta forma de pago/cobro.

D.- Partimos de la base de que, la persona que decide pagar con el Ste, para hacer el pago se conecta a través de internet (mediante ordenador, teléfono móvil, tableta, o cualquier otro dispositivo con funciones similares).

E.- El caso práctico expuesto a continuación comprende dos supuestos de compra: a) La compra de un libro realizada desde casa, a través del ordenador; y b) El pago del llenado de un depósito de gasolina, a través del teléfono móvil.

CASO PRÁCTICO.

1.- Primer paso:

- Un supuesto: Si queremos comprar un libro, antes de comprar el libro, lo primero es entrar en la página web correspondiente y seleccionar el libro a comprar; después, para pagar, seleccionamos la forma de pago "Ste" y pulsamos "comprar" (recuérdese, que este sistema de pago tiene que ser admitido por ambas partes, Comprador y Vendedor).
- Otro supuesto: Si lo que queremos es pagar el importe del llenado del depósito de gasolina del coche en una estación de servicio, a la hora de pagar, tenemos que decir en caja que pagamos con "Ste" (lo mismo que avisamos cuando pagamos con tarjeta de pago), para que nos den o nos envíen los datos del vendedor, del módulo de cobro y de la compra/venta.

2.- Segundo paso:

- El vendedor, al recibir el comunicado de compra (en el caso del libro, el mensaje de compra lo recibe de forma telemática; y en el caso de la gasolinera, lo recibe de palabra), ejecuta dos operaciones: 1) proporciona al comprador, al menos, sus datos de identidad, bancarios y de la compra (de la compra/venta); y 2), envía un mensaje a su módulo de cobro, que comprende, al menos, la información de identificación de la compra/venta.
- En el apartado anterior, se indica que el vendedor "*proporciona al comprador, al menos, sus datos de identidad, bancarios y de la compra (de la compra/venta)*", pero no se indica cómo; y aquí, se debe tener en cuenta si se trata de una compra telemática o de una compra presencial. En este caso práctico, la compra del libro es telemática y el pago del gasóleo es presencial:
    - Compra telemática. En este supuesto, el mensaje de compra lo recibe el vendedor de forma telemática, lo que permite al vendedor enviar un mensaje al comprador comunicando sus datos de identidad, los datos del módulo de cobro y de la compra/venta (para que el comprador, pueda hacer la orden de pago).
    - Compra presencial. En este supuesto, el mensaje de compra, no lo recibe el vendedor de forma telemática, sino presencial; por lo tanto, el vendedor, en principio, no puede enviar al comprador el mensaje conteniendo los datos

necesarios para que pueda hacer la orden de pago. Aquí, las soluciones pueden ser varias (lógicamente, partimos de la base que el comprador dispone de un teléfono móvil), por ejemplo:

- El vendedor, da al comprador la referencia de contacto por bluetooth o por la pantalla de ordenador (es este supuesto, para que el teléfono pueda "leer" estos datos de la pantalla, los datos tendrán que estar en un lenguaje que permita su lectura, por ejemplo: código de barras, QR-Code, etc.). El comprador, teniendo en su móvil la referencia de contacto, abre la interfaz "Ste" y pulsa el icono "comprar"; es decir, envía un mensaje al vendedor, indicándole que quiere pagar. El vendedor, al tener abierta la vía de contacto, ya le puede enviar todos los datos.
- El vendedor proporciona al comprador todos los datos para que pueda hacer la orden de pago, por bluetooth o por la pantalla de ordenador (y al mismo tiempo, comunica a su módulo de cobro la referencia de la compra/venta). Lo que tiene que hacer el comprador, es únicamente verificar que los datos recibidos son correctos (como cualquier tique o factura, en una tienda física).

3.- <u>Tercer paso</u> (ver figura 1):

El comprador (ref. 1) , cumplimenta la "orden de pago" y envía esta orden de pago (ref. 5) a su "Entidad de Pago" (ref. 2).

- Se denomina "orden de pago", al comunicado que envía el comprador a su Entidad de Pago, para que la Entidad de Pago, page al Vendedor el importe de la compra. La "orden de pago", contiene la siguiente información:
  - Datos de identificación del Comprador,
  - Datos de identificación y bancarios del Vendedor y
  - Datos de la compra (tipo tique o tipo factura).
- En la orden de pago:
  - Los únicos datos que constan del comprador, son los de identificación, pues todos los demás datos, ya los tiene su Entidad de Pago.
  - Sin embargo, tienen que constar todos los datos de identificación y bancarios del Vendedor, a fin de poder hacer el ingreso económico en su cuenta.
  - También tienen que constar en la orden de pago, los datos de la compra; es decir, aquellos datos que identifican la compra y su importe.
- Al margen de lo dicho, la orden de pago, puede ser de dos tipos: "tique" o "factura".

- La modalidad “tique”, contendría los datos de compra esenciales (al igual que el tique que nos dan en una tienda física).
- La modalidad “factura”, contendría los datos de compra que requiere cualquier factura.

- Los datos de la orden de pago se cumplimentan automáticamente.
  - Con relación al Comprador, los datos ya constan en el ordenador o teléfono móvil (téngase en cuenta, que la orden de pago la hace el Comprador en su ordenador o teléfono móvil).
- Con relación a los datos del Vendedor y datos de la compra/venta, los datos los proporciona el Vendedor. Cumplimentada la orden de pago y verificado que es correcta, hacemos clic en el icono “continuar”:
  - En la pantalla sale un mensaje diciendo: “introduzca Tarjeta/USB”. Introducimos la Tarjeta/USB.
  - Al introducir la Tarjeta/USB, en pantalla sale un mensaje diciendo: “escriba código PIN”. Ponemos el código PIN y pulsamos “continuar”.
  - Al pulsar “continuar”, el ordenador cifra la información y cuando termina, aparece un aviso en pantalla: “Retire Tarjeta/USB”. Retiramos la Tarjeta/USB.
  - Al retirar la Tarjeta/USB, aparece un nuevo icono: “enviar” y pulsamos “enviar” [Nota.- Mientras no se retire la Tarjeta/USB, no aparece el icono “enviar”].
  - El mensaje enviado, que es la orden de pago (ver figura 1, ref. 5), lo recibe nuestra Entidad de Pago.

4.- <u>Cuarto paso</u> (ver figura 1):

La Entidad de Pago (ref. 2), verifica la orden de pago y emite el pago (ref. 6) a la “Entidad de Cobro” (ref. 3).

- La Entidad de Pago descifra de forma automática la orden de pago (ref. 5).
- Si la orden de pago es correcta, la Entidad de Pago realiza el pago (ref. 6) a la Entidad de Cobro del vendedor, para su ingreso en la cuenta del vendedor.
  - Este pago, viene siendo una transferencia bancaria. Es de señalar aquí lo siguiente:
    - La Entidad de Cobro, no admitirá cobro alguno, si los datos de identificación y bancarios del Vendedor que constan en el pago, no concuerdan con los que tiene la propia Entidad de Cobro.

- El pago, además, tiene que tener los datos de identificación de la compra/venta [Nota.- En las transferencias bancarias, este dato de identificación encajaría perfectamente en el apartado “concepto”].

- A los efectos de esta interfaz Ste, lo único que interesa aquí, es la existencia de la comunicación entre la Entidad de Pago y la Entidad de Cobro, a los efectos del pago/cobro (esta comunicación forma parte de la interfaz); pero no forma parte de la interfaz, ni es objeto de este trabajo, la forma en que se relacionan ambas entidades.

5.- <u>Quinto paso</u> (ver figura 1):

La Entidad de Cobro (ref. 3), al recibir el pago (ref. 6), verifica la concordancia entre la referencia de pago de la compra/venta y la referencia de cobro de la compraventa que el Vendedor (ref. 4) previamente le envió (ref. 02). Si concuerdan ambas referencias, ingresa el importe del pago en la cuenta que tiene el Vendedor y acusa recibo del pago (ref. 7) a la Entidad de Pago (ref. 2).

- Lógicamente, aunque por motivos de simplicidad didáctica no se diga en el párrafo anterior, para que la Entidad de Cobro haga el ingreso, además de concordancia de las referencias de la compra/venta, también tienen que coincidir los demás datos (titular de la cuenta, número de cuenta, importe, etc.).
- En cuanto a la forma de comunicación entre la Entidad de Cobro y el Vendedor, nada hay que decir, pues cualquier forma de comunicación segura, es válida. Lo único que interesa aquí, por formar parte de la interfaz, es la existencia de esta comunicación (y no la forma en que se comunican, que no forma parte de la interfaz).

6.- Sexto <u>paso</u> (ver figura 1):

La Entidad de Pago (ref. 2), al recibir el acuse del pago (ref. 7), comunica el pago (ref. 8) al Comprador (ref. 1).

7.- Séptimo <u>paso</u> (ver figura 1):

El Comprador (ref. 1), recibe el acuse de pago (ref. 8) –lo que le confirma la compra-. Fin.

- Y si imprimimos nuestra orden de pago con el acuse de pago, nos sirve de tique o factura.
    - Con este sistema, el Vendedor no tiene que expedir ni tique ni factura.

REIVINDICACIONES

1.- Método de telepago electrónico para realizar un pago entre un usuario comprador y un usuario vendedor que comprende los pasos de:

a) recibir, en un dispositivo electrónico del usuario comprador, información que comprende al menos información de identificación del usuario comprador, información de identificación del usuario vendedor, información bancaria del usuario vendedor e información de identificación de una compra/venta asociada al pago;

b) conectar un módulo de memoria externo al dispositivo electrónico, donde el módulo de memoria externo contiene unos parámetros de cifrado asignados previamente al usuario comprador;

c) recibir, en el dispositivo electrónico, un código PIN de identificación único del usuario comprador;

d) cifrar, en el dispositivo electrónico, la información recibida en el paso a) junto con el código PIN de identificación recibido en el paso c) de acuerdo a los parámetros de cifrado del módulo de memoria externo conectado en el paso b);

e) enviar un mensaje que contiene la información cifrada en el paso d), desde el dispositivo electrónico del usuario comprador, a un módulo de pago, a través de una red de telecomunicaciones;

f) descifrar el mensaje recibido en el módulo de pago;

g) realizar el pago, de acuerdo a la información contenida en el mensaje descifrado, desde el módulo de pago a un módulo de cobro asociado con el usuario vendedor;

donde el método está caracterizado por que comprende los siguientes pasos previos al paso a):

- enviar, desde el dispositivo electrónico del usuario comprador, un primer mensaje de compra al dispositivo electrónico del vendedor, donde dicho primer mensaje de compra comprende información de identificación de un objeto de compra; y
- una vez recibido en el dispositivo electrónico del vendedor el primer mensaje de compra:
    - enviar un segundo mensaje desde el dispositivo electrónico del vendedor al dispositivo electrónico del usuario comprador con información al menos de identificación del usuario vendedor, información bancaria del usuario vendedor e información de identificación de la compra/venta;
    - enviar un tercer mensaje desde el dispositivo electrónico del vendedor al módulo de cobro con información al menos de identificación de la compra/venta.

2.- Método de acuerdo a la reivindicación 1 donde, una vez realizado el pago desde el módulo de pago al módulo de cobro, además comprende los pasos de:

- verificar, por parte del módulo de cobro, la coincidencia entre una referencia de cobro contenida en la información de identificación de la compra/venta enviada desde el dispositivo electrónico del vendedor al módulo de cobro, con una referencia asociada al pago de la compra/venta;

- enviar, si las referencias de pago y cobro coinciden un mensaje de confirmación del pago, desde el módulo de cobro al módulo de pago, en cambio, si las referencias no coinciden, el módulo de cobro rechaza el pago;

- una vez recibido en el módulo de pago el mensaje de confirmación del pago, enviar un mensaje adicional que confirma el pago desde el módulo de pago al dispositivo electrónico del usuario comprador.

3.- Método de acuerdo a la reivindicación 2 donde, si al verificar la coincidencia entre referencias de pago y cobro en el módulo de cobro dichas referencias no coinciden, comprende adicionalmente el paso de eliminar, por el módulo de cobro, la información de identificación de la compra/venta.

4.- Método de acuerdo a cualquiera de las reivindicaciones anteriores donde realizar el pago de acuerdo a la información contenida en el mensaje descifrado, desde el módulo de pago a un módulo de cobro asociado con el usuario vendedor, además comprende comprobar que el número PIN de identificación único del mensaje descifrado corresponde con el número PIN de identificación único del usuario comprador, que ha sido almacenado previamente en el módulo de pago.

5.- Método de acuerdo a cualquier de las reivindicaciones anteriores donde, realizar el pago de acuerdo a la información contenida en el mensaje descifrado desde el módulo de pago a un módulo de cobro asociado con el usuario vendedor, además comprende comprobar que la información de identificación del usuario vendedor y la información bancaria del usuario vendedor corresponden con un usuario vendedor registrado previamente en dicho módulo de cobro.

6.- Método de acuerdo a cualquiera de las reivindicaciones anteriores donde los parámetros de cifrado del usuario comprador son únicos y el cifrado de la información de cada pago utiliza unos parámetros de cifrado diferentes.

7.- Método de acuerdo a cualquiera de las reivindicaciones anteriores que además comprende almacenar en el módulo de pago los parámetros de cifrado asignados al usuario comprador.

8.- Método de acuerdo a la reivindicación 7 donde el descifrado del mensaje recibido en el módulo de pago se realiza de acuerdo a los parámetros de cifrado asignados al usuario comprador almacenados en el módulo de pago.

9.- Método de acuerdo a cualquiera de las reivindicaciones anteriores donde la información recibida en el dispositivo electrónico del usuario comprador es introducida por el usuario comprador a través de una interfaz instalada previamente en el dispositivo electrónico.

10.- Método de acuerdo a cualquiera de las reivindicaciones anteriores, donde los parámetros de cifrado comprenden al menos unos parámetros de inicio de cifrado, una clave de cifrado y unos textos clave para el cifrado.

11.- Sistema de telepago electrónico para realizar un pago entre un usuario comprador y un usuario vendedor que comprende:

- un dispositivo electrónico del usuario comprador configurado para enviar un primer mensaje de compra a un segundo dispositivo electrónico del usuario vendedor, donde dicho primer mensaje de compra comprende información de identificación de un objeto de compra; recibir información que comprende al menos, información de identificación del usuario vendedor, información bancaria del usuario vendedor e información de identificación del pago; recibir un código PIN de identificación único del usuario comprador; cifrar la información recibida de acuerdo a unos parámetros de cifrado proporcionados por un módulo de memoria externo conectable al dispositivo electrónico; y enviar un mensaje, que contiene la información cifrada, a un módulo de pago a través de una red de telecomunicaciones;
- un dispositivo electrónico del usuario vendedor configurado para, una vez recibido el primer mensaje de compra:
    - enviar un segundo mensaje al dispositivo electrónico del usuario comprador con información al menos de identificación del usuario vendedor, información bancaria del usuario vendedor e información de identificación de la compra/venta;
    - enviar un tercer mensaje desde el dispositivo electrónico del vendedor al módulo de cobro con información al menos de identificación de la compra/venta;

- un módulo de memoria externo y conectable al dispositivo electrónico del comprador, que contiene los parámetros de cifrado;
- un módulo de pago configurado para recibir un mensaje enviado desde el dispositivo electrónico del comprador, descifrar el mensaje recibido y realizar el pago, de acuerdo a la información contenida en el mensaje descifrado, a un módulo de cobro asociado con el usuario vendedor;
- módulo de cobro configurado para recibir pagos enviados desde el módulo de pago.

12.- Sistema de acuerdo a la reivindicación 11 donde, una vez descifrado el mensaje recibido, el módulo de pago está además configurado para comprobar que el número PIN de identificación único del usuario comprador, incluido en el mensaje descifrado, corresponde con el número PIN identificación único del usuario comprador, que ha sido almacenado previamente en el módulo de pago.

13.- Sistema de acuerdo a cualquiera de las reivindicaciones 11, 12 donde:

- el módulo de cobro está además configurado para comprobar que la información de identificación del usuario vendedor y la información bancaria del usuario vendedor corresponden con un usuario vendedor registrado previamente en dicho módulo de cobro y también, verificar la coincidencia entre una referencia de pago de la compra/venta y una referencia de cobro de la compra/venta y además, enviar un mensaje de confirmación del pago al módulo de pago;

- el módulo de pago está además configurado para, una vez recibido el mensaje de confirmación del pago, enviar un mensaje adicional que confirma el pago al dispositivo electrónico del usuario comprador.

14.- Sistema de acuerdo a cualquiera de las reivindicaciones 11-13, donde el módulo de memoria externo y conectable al dispositivo electrónico, que contiene los parámetros de cifrado, es una memoria de tipo USB de sólo lectura.

15.- Sistema de acuerdo a cualquier de las reivindicaciones anteriores 11-14, donde el dispositivo electrónico del usuario comprador y/o vendedor es un teléfono móvil, tableta, ordenador o cualquier otro dispositivo electrónico con funciones similares.

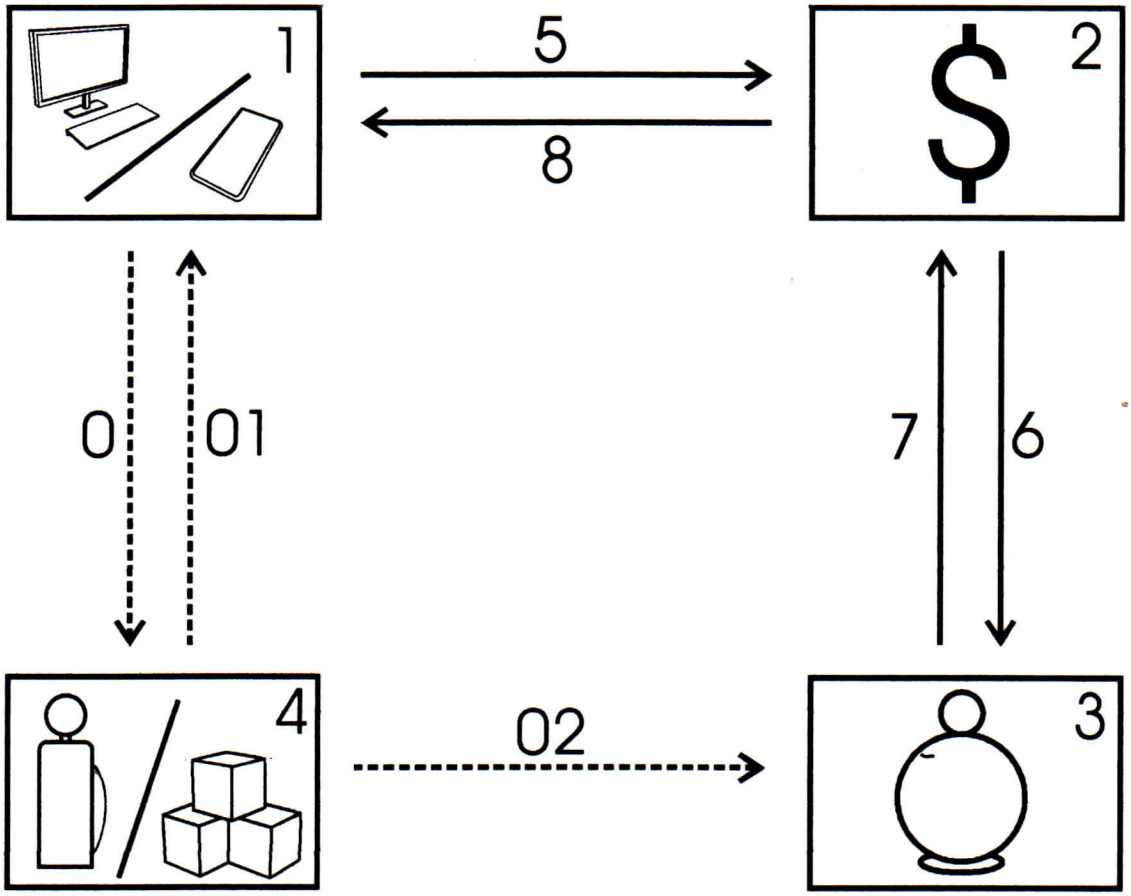

Figura 1

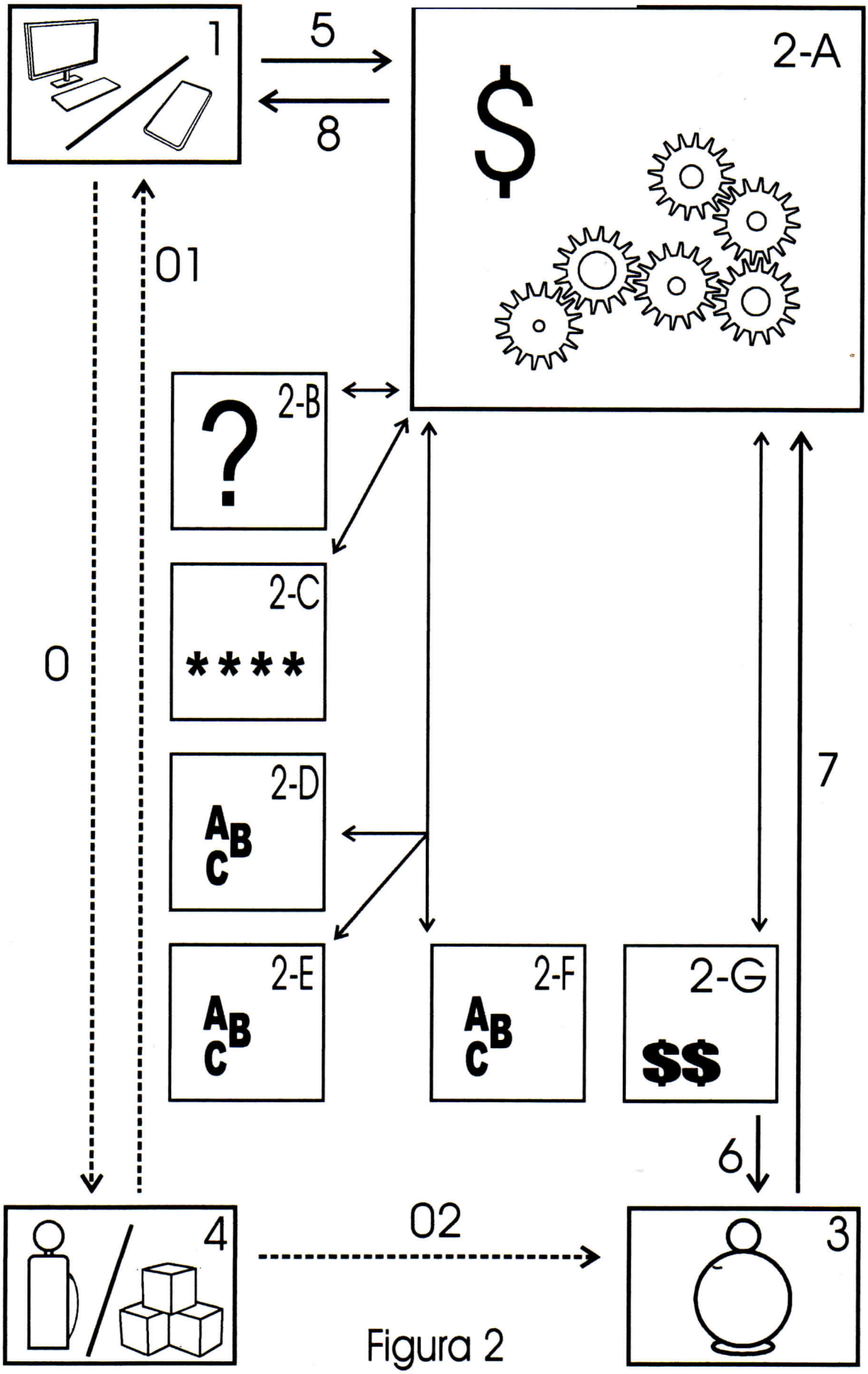

Figura 2

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201531386

(22) Fecha de presentación de la solicitud: 29.09.2015

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** Ver Hoja Adicional

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
A	EP 1326192 A1 (S W I F T SC) 09.07.2003, párrafos [0014-0046]; figuras.	1-15
A	US 2011208594 A1 (DORO JOSHUA A) 25.08.2011, párrafos [0020-0049]; figuras.	1-15
A	US 2007203847 A1 (SCHOOL HOLGER) 30.08.2007, párrafos [0044-0060]; figuras.	1-15
A	US 2013060701 A1 (MOON YONG SEOK et al.) 07.03.2013, párrafos [0042-0244]; figuras.	1-15

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
16.04.2016	P. Pérez Fernández	1/4

CLASIFICACIÓN OBJETO DE LA SOLICITUD

G06Q20/04 (2012.01)
G06Q20/12 (2012.01)
G06Q20/38 (2012.01)
G06Q20/32 (2012.01)
G06Q20/40 (2012.01)

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

G06Q

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

INVENES, EPODOC

Fecha de Realización de la Opinión Escrita: 16.04.2016

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-15	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones	1-15	**SI**
	Reivindicaciones		**NO**

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

Base de la Opinión.-

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

1. Documentos considerados.-

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

Documento	Número Publicación o Identificación	Fecha Publicación
D01	EP 1326192 A1 (S W I F T SC)	09.07.2003

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

Tiene Novedad/Actividad Inventiva

Reivindicación nº 1
Se establece el documento D01 como el más próximo del Estado de la Técnica.
Dicho documento D01 hace referencia a "un método y un sistema de pago para comercio electrónico". Este documento no muestra un método como el reivindicado en la reivindicación nº1. Además, no se considera obvio que un experto en la materia conciba dicho método con las características reivindicadas en la reivindicación nº 1.
Por tanto, la reivindicación nº 1 es Nueva, implica Actividad Inventiva y tiene Aplicación Industrial (Arts 6.1, 8 y 9 LP).

Reivindicaciones nº 2-10
Las reivindicaciones nº 2-10 dependen de una u otra manera de la reivindicación nº 1. Teniendo en cuenta las argumentaciones con respecto a la reivindicación nº 1, la invención de acuerdo con las reivindicaciones nº 2-10 cumple el requisito de Novedad, Actividad Inventiva y Aplicación Industrial (Arts 6.1, 8, 9 LP).

Reivindicación nº 11
De la misma manera que en el caso de la reivindicación nº 1, el documento D01 no expresa las características de la reivindicación nº 11. Por otra parte, no es obvio aplicar las características del documento D01 y llegar a la invención como se reivindica en la reivindicación nº 11. En consecuencia, la reivindicación nº 11 posee Novedad, Actividad Inventiva y Aplicación Industrial (Arts 6.1, 8, 9 LP).

Reivindicaciones nº 12-15
Las reivindicaciones nº 12-15 dependen de la reivindicación nº 11. Por tanto, las reivindicaciones nº 12-15 también poseen Novedad, Actividad Inventiva y Aplicación Industrial (Arts 6.1, 8, 9 LP).