



(19)



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 272 517**

(51) Int. Cl.:
G07F 19/00 (2006.01)
G07F 7/02 (2006.01)

(12)

TRADUCCIÓN DE PATENTE EUROPEA

T3

(86) Número de solicitud europea: **01957958 .0**
(86) Fecha de presentación : **12.07.2001**
(87) Número de publicación de la solicitud: **1410352**
(87) Fecha de publicación de la solicitud: **21.04.2004**

(54) Título: **Método para la compra en línea con una elevada seguridad operativa.**

(30) Prioridad: **19.07.2000 IT MI00A1642**

(73) Titular/es: **DTS S.R.L.**
Rampe S. Antonio a Posillipo 13
80100 Napoli, IT

(45) Fecha de publicación de la mención BOPI:
01.05.2007

(72) Inventor/es: **Tarabbo, Francesco**

(45) Fecha de la publicación del folleto de la patente:
01.05.2007

(74) Agente: **No consta**

ES 2 272 517 T3

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

DESCRIPCIÓN

Método para la compra en línea con una elevada seguridad operativa.

Campo técnico

La presente invención hace referencia a un método para la compra en línea con una elevada seguridad operativa. Más particularmente, la invención hace referencia a un método para la compra en línea con una elevada seguridad operativa tal como por ejemplo la compra en Internet.

Estado de la técnica

Es conocido que el comercio con pagos y compras en línea realizado utilizando una tarjeta de crédito se está desarrollando cada vez más, especialmente gracias a la difusión de redes de comunicación de datos tales como Internet, que alberga un muy gran número de empresas que pueden ofrecer sus productos a precios competitivos y promover compras realizadas directamente en línea utilizando una tarjeta de crédito.

Sin embargo, una limitación al crecimiento de tal comercio electrónico es el hecho en sí de que el usuario, con el fin de poder realizar la compra, debe introducir su número de tarjeta de crédito en línea con el fin de completar la compra.

El hecho de tener que transmitir el número de tarjeta de crédito a través de redes de comunicación de datos produce considerables dudas entre los usuarios, que temen, algunas veces de forma justificada, que su número de tarjeta de crédito pueda ser interceptado fraudulentamente y utilizado por gente malintencionada para realizar compras no autorizadas, cargándolas a la cuenta corriente del usuario legítimo a quien pertenece la tarjeta.

Por lo tanto, cuando el usuario se encuentra con la necesidad de introducir su número de tarjeta de crédito en un formulario electrónico preparado por el operador de servicios o el distribuidor de bienes a través de una red de comunicación de datos, no está motivado por una confianza absoluta en el sistema de codificación que pueda ofrecer el operador, y por lo tanto, incluso aunque realice la compra, no se siente suficientemente protegido en cuanto al secreto de sus datos.

Sin embargo, la herramienta básica para poder realizar compras en línea es desde luego la tarjeta de crédito, debido a su método de uso, y por lo tanto el crecimiento del comercio electrónico y el comercio en línea en general está cada vez más unido a esta herramienta.

Además, incluso si el operador del servicio propone un sistema de codificación de los datos, de forma que los datos no puedan ser leídos por terceros, es conocido que la codificación mediante cualquier clave pública o privada está sujeta a descodificación, incluso si esto requiere una cantidad de tiempo significativa.

Todos los sistemas utilizados en la actualidad para proteger las transacciones realizadas en línea utilizando el código de una tarjeta de crédito conllevan, en el mejor de los casos, una codificación que sin embargo no asegura la inviolabilidad absoluta de los datos.

US 5,883,810 muestra un sistema de comercio en línea en el que una tarjeta es emitida electrónicamente a un cliente para asignar un número de cuenta de cliente permanente. El cliente obtiene un número de transacción que se asemeja a un número de tarjeta de

crédito para el uso en una única transacción mediante un programa wizard instalado en su ordenador.

WO00/02150 muestra un sistema para realizar una transacción financiera remota entre un cliente y un proveedor en el que un código de transacción relacionado a una transacción en particular es creado basado en una contraseña, un número existente de tarjeta de crédito/débito o de cuenta, un código de proveedor identificando al proveedor y una cantidad límite para la transacción.

Explicación de la invención

El objetivo de la presente invención es proveer un método para la compra en línea con una elevada seguridad operativa que permita asegurar la inviolabilidad sustancial de los datos de la transacción realizada por el usuario.

Dentro de este objetivo, un objeto de la presente invención es proveer un método para la compra en línea con una elevada seguridad operativa que permita inutilizar, después de un periodo de tiempo preestablecido, cualquier dato de la transacción que pudiera ser interceptado fraudulentamente por terceros.

Otro objeto de la presente invención es proveer un método para la compra en línea con una elevada seguridad operativa que permita asegurar el anonimato de la compra realizada en línea.

Otro objeto de la presente invención es proveer un método para la compra en línea con una elevada seguridad operativa que sea altamente fiable, relativamente simple de proveer y con costes competitivos.

Este objetivo y este y otros objetos que resultarán aparentes de mejor modo a continuación se consiguen mediante el método de la reivindicación 1.

Breve descripción del dibujo

Otras características y ventajas de la invención resultarán aparentes de mejor modo a partir de la descripción de ejemplos de realización preferidos pero no exclusivos del método según la invención, en los que la única figura es un diagrama esquemático de la arquitectura del sistema utilizada para implementar el método según la presente invención.

Formas de realizar la invención

Con referencia a la figura, el método según la presente invención provee los siguientes pasos.

En primer lugar, una primera tarjeta está provista que lleva un código que, junto con la entrada de un PIN (Número de Identificación Personal), permite activar dicha tarjeta.

Sustancialmente, el emisor de dichas tarjetas, que está designado por el número de referencia 1 en la Figura, mediante una conexión a la red bancaria 2, genera una cuenta virtual 3 la cual el usuario tiene disponible para realizar compras en línea mediante dicha tarjeta.

El método utiliza una segunda tarjeta, del tipo desechable, que contiene un código secreto que permite transferir a la cuenta virtual 3 un valor monetario que corresponde a la suma pagada por el usuario para comprar la tarjeta desechable.

El método entonces conlleva un primer paso, en el que el usuario compra una tarjeta, que lleva un código aplicado a ella de forma visible y con un PIN, y una segunda tarjeta, del tipo desechable, que lleva un código secreto y permite recargar la cuenta virtual 3 del usuario.

El segundo paso del método según la invención conlleva activar la tarjeta con un PIN de seguridad y transferir un valor monetario seleccionado por el

usuario a su cuenta virtual mediante la tarjeta desechable que contiene el código secreto.

En este punto, cuando el usuario tiene que realizar una compra en línea, por ejemplo en Internet, y por lo tanto ya sabe la cantidad a ser gastada, contacta con el emisor de tarjetas 1 por ejemplo mediante los siguientes sistemas:

- abriendo una nueva ventana, designada por el número de referencia 5, en el ordenador personal 4;
- por teléfono 6;
- por teléfono móvil 7 (por ejemplo con mensajes de tipo SMS);
- por terminales 8 conectados a la red telefónica (por ejemplo por el circuito POS -punto de venta-).

Una vez que el usuario ha contactado con el emisor de tarjetas 1, introduce el número provisto en la tarjeta de forma visible y el PIN correspondiente. Al recibir estos datos, el sistema los confirma e informa del crédito residual disponible en la cuenta virtual 3 a nombre del usuario que introdujo el número de tarjeta.

En este punto el usuario introduce la cantidad que pretende gastar para comprar los bienes o servicios, que por lo tanto debe deducirse de su cuenta virtual 3.

El sistema compara la cantidad (en la cuenta virtual) con la cantidad que el usuario ha introducido, que corresponde a la cantidad de los bienes o servicios que desea gastar.

Una vez que la operación ha sido confirmada, al usuario se le envía a través de la red bancaria 2 un código de tarjeta de crédito virtual con una fecha de caducidad muy específica que generalmente está muy cercana.

Esta información es provista al usuario, por ejemplo, si se requiriese, de forma codificada. El número de tarjeta de crédito virtual secreto es decodificado en el ordenador personal del usuario antes de poder proceder a la compra utilizando el código secreto enviado por la red bancaria.

En la operación final, el usuario introduce el código de tarjeta de crédito virtual recibido de la red bancaria en la pantalla de compra en línea específica. El sitio entonces realiza la transacción de compra hacia el banco del usuario para verificación y aprobación.

En este punto el usuario puede imprimir una copia de la compra para ser utilizada como recibo de pago.

Poco después de que el usuario haya introducido en la red el código de tarjeta de crédito virtual que se le envió a través del sistema de comunicación de datos en forma codificada, dicho código se cancela automáticamente, de este modo inutilizando cualquier interceptación del código por parte de personas

malintencionadas.

Prácticamente, el usuario en primer lugar no informa de sus datos personales, tales como su nombre y apellidos, en la red, de este modo consiguiendo el anonimato completo de la compra, y en segundo lugar el código que introduce en la red no es el código que está presente en la tarjeta que posee físicamente, que en la actualidad debe estar activada conociendo el PIN, sino que es un código que se envía al usuario a través de la red bancaria 2 y que, además de estar codificado, tiene una duración limitada muy específica.

En cualquier caso, la cancelación del código enviado por la red bancaria inmediatamente después de la compra realizada por el usuario hace que dicho código sea inutilizable.

El método según la invención permite de esta forma realizar transacciones de pago en línea absolutamente inviolables, puesto que el usuario ya no envía su número de tarjeta de crédito tal y como ocurre en el presente, sino que en su lugar envía un código que permite "generar" un código adicional que entonces se envía en forma codificada al usuario.

Por lo tanto, a diferencia de los sistemas de pago conocidos, en los que el usuario ha de introducir su código de tarjeta de crédito y es este código el que permite el acceso directo a su cuenta personal, el método según la invención conlleva introducir un código que permita generar un código adicional, de tipo temporal, que permita acceder a la cuenta virtual. En cada caso, es decir, para cada transacción individual, el código que da acceso a la cuenta virtual del usuario es cambiado y enviado en forma codificada al usuario.

De forma acorde, a partir de lo que se ha descrito anteriormente resulta evidente que el método según la invención asegura la inviolabilidad absoluta de los datos de la transacción, haciendo particularmente inútil el conocimiento fraudulento del código emitido por la red bancaria siguiendo la introducción del código de tarjeta por el usuario.

Es posible proveer una tarjeta diferente, con un código y un PIN que son nuevos cada vez, y deben utilizarse para cada compra diferente.

De esta forma la seguridad del usuario está garantizada incluso más.

En la práctica se ha observado que el método según la invención consigue por completo el objetivo y los objetos pretendidos, puesto que permite realizar transacciones con un nivel de seguridad extremadamente alto, directamente en línea, sin tener que enviar un número de tarjeta de crédito y por lo tanto de hecho sin necesidad de poseer una tarjeta de crédito.

El método concebido de este modo es susceptible de numerosas modificaciones y variaciones, todas ellas estando dentro del ámbito de las reivindicaciones anexadas; todos los detalles pueden además ser reemplazados por otros elementos técnicamente equivalentes.

REIVINDICACIONES

1. Un método para la compra en línea con una elevada seguridad operativa, comprendiendo los pasos de:

- proveer una tarjeta que lleve un código y con la que un PIN para habilitar dicha tarjeta está asociado;
- en el extremo del usuario, comunicar dicho código y dicho PIN a un emisor (1) de dicha tarjeta con el fin de activar dicha tarjeta;
- en el extremo del emisor, mediante una conexión a una red bancaria, creando una cuenta virtual (3) que está unívocamente asociada con dicha tarjeta en respuesta a dicha comunicación;
- en el extremo del usuario
 - cuando el usuario desee realizar una compra en línea, contactar al emisor de la tarjeta e introducir el código de dicha tarjeta y dicho PIN mediante un teléfono o un teléfono móvil o una terminal POS, con el fin de acceder a la cuenta virtual;
 - recibir, a continuación de dicha activación, un número de tarjeta de crédito virtual y una fecha de caducidad específica de dicha tarjeta de crédito virtual, que se envían al usuario a través de la red bancaria y que ofrecen el acceso temporal a la cuenta virtual;
 - introducir dicho número de tarjeta de crédito virtual en línea para realizar la compra, dicho número de tarjeta de crédito virtual siendo cancelado inmediatamente después de que el usuario haya realizado la compra.

2. El método según la reivindicación 1, **caracterizado** por el hecho de que el paso de activar dicha tarjeta enviando dicho código y dicho PIN comprende los pasos de, en el extremo del emisor, confirmar dicho código y dicho PIN e informar a dicho usua-

rio del crédito residual que está disponible en dicha cuenta virtual (3).

3. El método según la reivindicación 1, **caracterizado** por el hecho de que dicha cuenta virtual (3) puede ser recargada utilizando una segunda tarjeta con un código secreto.

4. El método según la reivindicación 3, **caracterizado** por el hecho de que dicha tarjeta añadida para dicha cuenta virtual (3) realiza una recarga por un valor igual al valor de compra de dicha tarjeta.

5. El método según una o más de las reivindicaciones anteriores, **caracterizado** por el hecho de que dicho número de tarjeta de crédito virtual, enviado al usuario a través de una red de comunicación de datos por una red bancaria (2), se envía de forma codificada.

6. El método según la reivindicación 5, **caracterizado** por el hecho de que comprende el paso de decodificar dicho código secreto codificado enviado por la red bancaria (2) a la terminal (4) del usuario.

7. El método según una o más de las anteriores reivindicaciones, **caracterizado** por el hecho de que dicha cantidad está comparada con el balance de dicha cuenta virtual (3).

8. El método según una o más de las anteriores reivindicaciones, **caracterizado** por el hecho de que el paso de introducir dicho código y dicho PIN de dicha tarjeta se realiza mediante el teclado de un teléfono (6, 7).

9. El método según una o más de las anteriores reivindicaciones, **caracterizado** por el hecho de que el paso de introducir dicho código y dicho PIN de dicha tarjeta se realiza mediante el reconocimiento de voz.

10. El método según una o más de las anteriores reivindicaciones, **caracterizado** por el hecho de que el paso de introducir dicho código y dicho PIN de dicha tarjeta se realiza mediante una terminal POS (8).

11. El método según una o más de las anteriores reivindicaciones, **caracterizado** por el hecho de que después del paso de introducir dicho número de tarjeta de crédito virtual en línea, los siguientes pasos se realizan:

- realizar la transacción de compra respecto del banco sirviendo a dicho usuario para verificación y aprobación; y
- imprimir una copia de la compra realizada en línea, como recibo de pago.

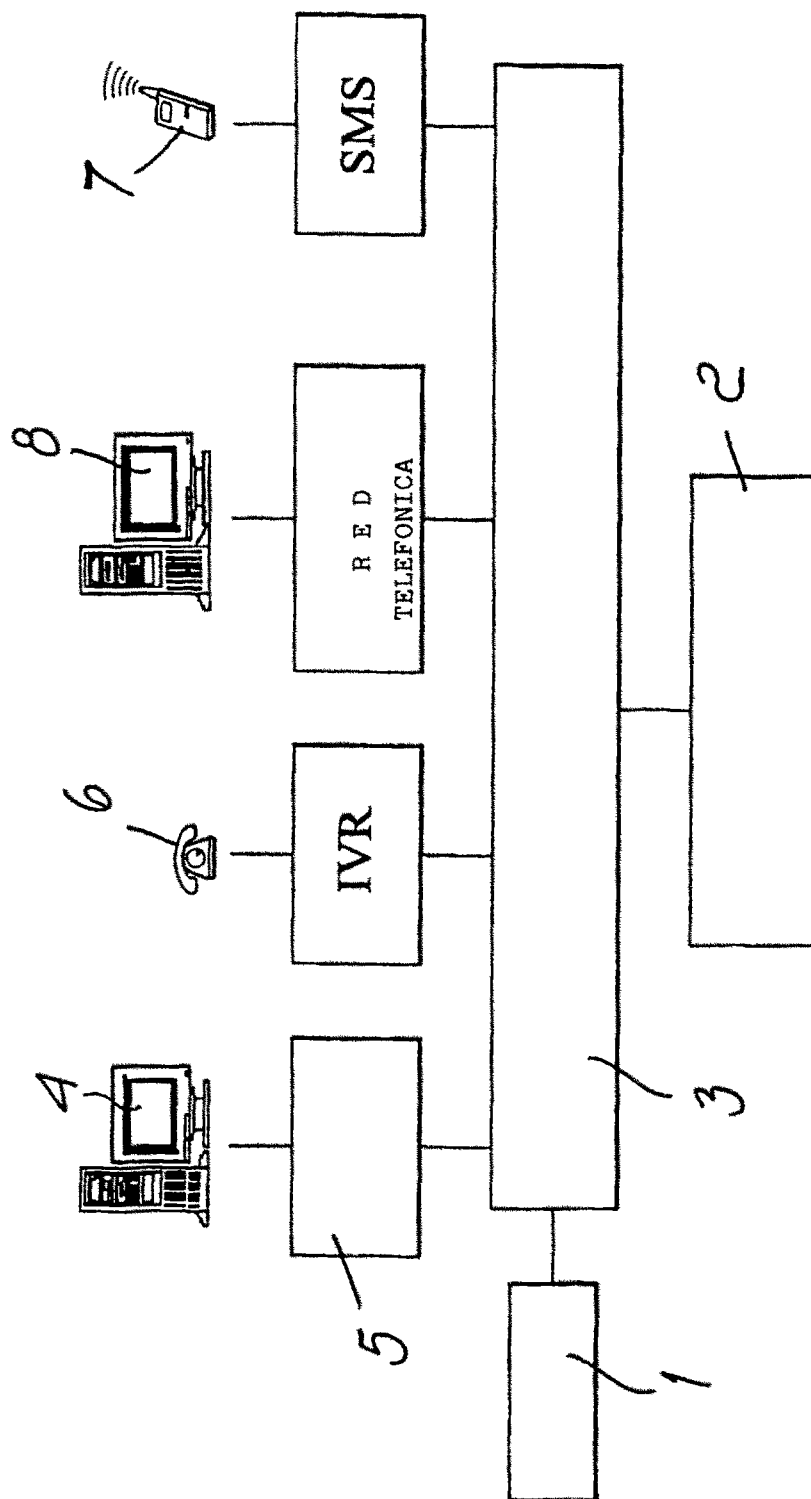


Fig. 1