



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 272 533**

51 Int. Cl.:
G07F 7/10 (2006.01)
G07F 19/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **01965318 .7**
86 Fecha de presentación : **09.08.2001**
87 Número de publicación de la solicitud: **1323140**
87 Fecha de publicación de la solicitud: **02.07.2003**

54 Título: **Procedimiento para proporcionar datos de identificación de una tarjeta de pago a un usuario.**

30 Prioridad: **28.08.2000 FR 00 11004**

45 Fecha de publicación de la mención BOPI:
01.05.2007

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

73 Titular/es: **Axalto S.A.**
50, avenue Jean Jaurès
92120 Montrouge, FR

72 Inventor/es: **Guion, Christian**

74 Agente: **Elzaburu Márquez, Alberto**

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

Procedimiento para proporcionar datos de identificación de una tarjeta de pago a un usuario.

La presente invención se refiere a un procedimiento para proporcionar datos de identificación de una tarjeta de pago a un usuario.

La presente invención se refiere en especial al suministro de los números de tarjetas temporales, denominadas aún tarjetas de pago de uso limitado asignadas por los bancos a sus clientes para asegurar sus transacciones en Internet.

El término "tarjeta de pago" se utiliza para denominar a todas las tarjetas bancarias de cobro diferido o inmediato, todas las tarjetas de crédito, etc., emitidas por un banco o una entidad especializada.

La seguridad de las transacciones realizadas mediante tarjetas de pago está basada actualmente en dos elementos: el control de la autenticidad de la firma del comprador en la factura, ya sea la firma manuscrita o electrónica, y el control de la autenticidad y validez de la tarjeta preguntando a la entidad emisora de la tarjeta con el fin de obtener la autorización para aceptar la tarjeta.

Este doble control lo realiza normalmente el proveedor, cuando puede disponer físicamente de la tarjeta de pago. La comprobación de la firma manuscrita o electrónica se efectúa fácilmente, al igual que la petición de autorización previa. Existen además terminales de pago lectores de tarjetas que pueden efectuar automáticamente dichos controles.

El comprador introduce en el teclado de estos terminales el código secreto de su tarjeta, denominado aún PIN code (PIN es el acrónimo del término inglés Personal Identification Number). Los circuitos electrónicos comparan entonces el código secreto introducido por el comprador con el código inscrito de manera encriptada en la tarjeta y validan la transacción en curso cuando ambos coinciden. Por otro lado, a partir de las informaciones leídas en la tarjeta, el terminal, a través de una red de telecomunicaciones, es capaz de preguntar a un servidor de gestión de tarjetas de pago para que le confirme que la tarjeta es válida y que no pesa ninguna prohibición sobre ella. Esta comprobación de la validez de la tarjeta se puede efectuar "on line", llamando al servidor durante la transacción, o bien "off line", gracias a la descarga periódica de las listas de tarjetas con prohibición (listas negras o black lists) y/o de las listas de tarjetas auténticas (listas positivas o white lists). Hay que señalar que la utilización de tarjetas con circuitos electrónicos permite controlar directamente la autenticidad de la tarjeta.

La consulta a los servidores de gestión para conocer la situación de una tarjeta de pago y la utilización de un código secreto conocido sólo por el poseedor de la tarjeta, reducen considerablemente las posibilidades de fraude.

Sin embargo, no ocurre lo mismo cuando el comprador y el vendedor están lejos entre sí y no se puede utilizar un terminal de pago lector de tarjetas para comprobar la tarjeta.

Efectivamente, para realizar una transacción cuando el comprador y el vendedor están lejos entre sí, por ejemplo en una compra por correspondencia o una reserva por teléfono o una transacción electrónica por Internet, el vendedor se limita a solicitar el número y la fecha de expiración de la tarjeta de pago del comprador. La comunicación de estas informaciones basta

para validar una factura que el proveedor presentará después para el cobro a su banco.

La sencillez del actual mecanismo de cobro mediante tarjeta de pago de las transacciones realizadas a distancia, origina gran número de fraudes, ya que cualquier persona que conozca un número de una tarjeta de pago y la fecha de expiración de esta última puede utilizar esas informaciones de manera ilegal para comprar bienes y servicios, mientras que el verdadero poseedor de la tarjeta, al no enterarse de la sustracción de la que es víctima, no realiza ninguna oposición a la entidad emisora de la tarjeta. Por otro lado, este sistema permite negaciones abusivas por parte de compradores poco honestos que se niegan a que se les cobre en cuenta con el falso pretexto de que las transacciones se han realizado sin su conocimiento. Esto ocurre sobre todo en las transacciones electrónicas realizadas por Internet, ya que, en esta red de comunicación abierta, es particularmente fácil interceptar las informaciones que se intercambian. Esta inseguridad constituye actualmente un freno importante para el comercio por Internet.

Se han lanzado numerosas tentativas para paliar este inconveniente y hacer que las transacciones a distancia sean más seguras, sobre todo las transacciones electrónicas.

Entre estas tentativas, podemos citar los sistemas de tipo SET, que consisten en encriptar las informaciones que se intercambian en Internet. Con estos sistemas, ya no se comunican abiertamente los números de las tarjetas bancarias y por lo tanto ya no son interceptables. La aplicación de estos sistemas choca sin embargo con la disponibilidad de un mayor número de medios específicamente previstos para asegurar las transacciones como los lectores de tarjetas por ordenador, medios de criptografía en los ordenadores o en los lectores y la estandarización de los protocolos elegidos por los distintos operadores. Por otro lado, aunque los números ya no sean interceptables directamente durante la comunicación entre el comprador y la página web, sí lo pueden ser en la página web donde los números de las tarjetas están almacenados de una manera descriptada y lo pueden ser en el ordenador del titular a partir de programas espías residentes capaces de grabar las informaciones introducidas por el titular en las teclas de su ordenador.

Otro enfoque consiste en utilizar una tarjeta de pago temporal o de uso limitado. Generalmente, estas tarjetas las crea la entidad financiera del comprador a petición de este último. Estas tarjetas, cuya duración está por lo general limitada a una transacción o a una cantidad dada de dinero, se presenta sobre todo en forma de un número y una fecha de expiración con los mismos formatos ISO que la tarjeta de pago principal del comprador (de tipo Visa, Mastercard, etc.).

En consecuencia, esta solución requiere poder transmitir de manera segura los números de las tarjetas temporales a los compradores. La solución que eligen sobre todo los bancos consiste en utilizar enlaces encriptados de tipo SSL entre los ordenadores de los compradores y los servidores bancarios. Este método conlleva sin embargo riesgos de fraude, ya que los métodos desarrollados por los defraudadores en Internet son cada vez más eficaces.

En el documento US-A-6000832, los datos de identificación de la tarjeta se generan con medios adecuados del usuario.

En consecuencia, el objeto de la presente inven-

ción es proponer una alternativa para transmitir de manera confidencial a los usuarios los datos de identificación de las tarjetas temporales, como pueden ser los números y fechas de expiración; dicha alternativa deberá ser segura y al mismo tiempo sencilla de aplicar.

El procedimiento, según la invención tiene por tanto el objeto de proporcionar a un usuario de manera segura los datos de identificación de una tarjeta de pago.

Según la invención, el procedimiento se caracteriza por que dichos datos de identificación de la tarjeta de pago los crea directamente el usuario a partir de medios de creación apropiados y que dichos datos de la tarjeta, creados de ese modo, son comunicados a continuación mediante medios de telecomunicación a un servidor informático de una entidad financiera gestora de la tarjeta de pago.

Según otra característica del procedimiento objeto de la presente invención, los datos de identificación de la tarjeta consisten en el número y la fecha de expiración de dicha tarjeta de pago.

Según otra característica del procedimiento objeto de la presente invención, los datos de identificación de la tarjeta de pago se crean directamente por medio de un teléfono especialmente adaptado para ello.

Según otra característica del procedimiento objeto de la presente invención, los datos de identificación de la tarjeta de pago se elaboran con un software adecuado que facilita la tarjeta con microprocesador SIM que lleva un radio-teléfono celular de tipo GSM.

Según otra característica del procedimiento objeto de la presente invención, el teléfono comunica automáticamente dichos datos de identificación de la tarjeta al servidor gestor.

Según otra característica del procedimiento objeto de la presente invención, los datos de la tarjeta se comunican al servidor gestor mediante la red de radiotelefonía celular en forma de un mensaje SMS.

Según otra característica del procedimiento objeto de la presente invención, los datos de identificación de la tarjeta de pago se crean directamente por medio de un microordenador personal.

Según otra característica del procedimiento objeto de la presente invención, el microordenador comunica automáticamente los datos de identificación de la tarjeta al servidor gestor utilizando la red Internet.

Según otra característica del procedimiento objeto de la presente invención, la tarjeta de pago sólo es válida para un número limitado de transacciones y por un tiempo limitado.

Según otra característica del procedimiento objeto de la presente invención, la tarjeta de pago sólo es válida para una transacción.

Se comprenderán mejor los objetivos, aspectos y ventajas de la presente invención, con la descripción que se da a continuación de varios modos de realización de la invención, presentados a título de ejemplos no limitativos, referidos al esquema que se anexa, en el que:

la figura 1 es una vista esquemática del sistema necesario para aplicar el procedimiento según la presente invención.

En la figura 1, sólo se han representado los elementos útiles para la comprensión de la invención.

El ejemplo que se ha elegido para ilustrar el procedimiento y su dispositivo de aplicación según la invención, se refiere a la utilización de una tarjeta de

pago temporal para realizar una transacción electrónica en la red Internet. Por supuesto, la invención no se limita a ese único ejemplo y se refiere más ampliamente a la comunicación segura de los datos de identificación de una tarjeta de pago, como pueden ser su número, su fecha de validez o bien un código PIN, realizándose dicha comunicación entre dos emplazamientos distantes, fundamentalmente entre el domicilio de un usuario y su entidad financiera.

Según la representación de la figura 1, el sistema necesario para la aplicación de la invención es el siguiente. Un comprador se encuentra ante un ordenador que puede ser por ejemplo su microordenador personal señalado con la referencia 1, el cual está equipado con un módem que le permite conectarse a la red Internet 2. El ordenador 1 se puede conectar a través de la red Internet 2 con el servidor 7 de una página comercial que propone un servicio de venta de bienes o de servicios, como por ejemplo un servicio de venta de libros. El ordenador 1 también se puede conectar a través de la red Internet 2 con el servidor de gestión 4 de su entidad financiera. La conexión entre el servidor de gestión 4 y el microordenador del comprador es preferentemente segura, por ejemplo de tipo SSL.

Por otro lado, el comprador tiene un teléfono móvil 6 provisto de una tarjeta SIM (Subscriber Identity Module). Dicho teléfono 6 es apto para recibir o emitir, a través de una red 5 de radio-telecomunicación de tipo GSM u otra, datos procedentes o destinados a un servidor 4 en forma de mensajes radioeléctricos emitidos según un protocolo denominado de servicio de mensajes cortos, conocido también con el nombre de SMS (Short Message Service). Este protocolo permite mensajes con una longitud de 160 caracteres. Se pueden encadenar hasta quince mensajes consecutivos, es decir 2.400 caracteres en un mensaje. Además, este protocolo está incluido en todos los teléfonos móviles del mercado. Lo utilizan en general los operadores por ejemplo para prevenir a sus abonados de que han recibido nuevos mensajes en sus buzones de voz.

El comprador que se ha conectado a la página comercial 3 a través de la red Internet 2 y ha elegido comprar un libro recibe de la página 3 un formulario para registrar su pedido en el que se deben introducir un cierto número de informaciones, como el número y la fecha de expiración de una tarjeta de pago. En la medida en que el comprador no desee comunicar abiertamente las informaciones relativas a su tarjeta de pago, va a utilizar en su lugar una tarjeta temporal que él mismo va a crear.

Estas tarjetas de pago temporales son totalmente similares a la tarjeta permanente del comprador en lo que se refiere a las prestaciones que ofrecen.

Están asociadas a la misma cuenta bancaria y pueden ser aceptadas por los mismos comerciantes que la tarjeta permanente (redes Visa, Mastercard, etc.). Sus principales diferencias se encuentran en que sólo son válidas para un número limitado de transacciones, preferentemente para una única transacción. Preferentemente, estas tarjetas tienen además una vida relativamente breve, desde unas decenas de segundos hasta unos días.

Aunque se pueden utilizar para cualquier transacción temporal, estas tarjetas temporales de pago son particularmente aptas para las transacciones a distancia. Las tarjetas temporales de pago pueden en particular no tener un soporte físico (visualización temporal en una pantalla o bien comunicación de voz).

Exceptuando estas diferencias, las tarjetas temporales de pago son perfectamente similares a las demás tarjetas sobre todo en lo que respecta al formato y la codificación de sus números o a su fecha de expiración (formato de cuatro cifras: mes/año (07/01)). De este modo, en la medida en que, según la norma ISO actualmente vigente, las tarjetas de pago tradicionales tienen números de dieciséis cifras, cada número de tarjeta temporal contará también con dieciséis cifras: las seis primeras cifras forman el código BIN de la entidad financiera emisora y la última cifra el código de autenticación Luhn (CHECKSUM). Por supuesto, el formato de dieciséis cifras no es limitativo de la invención, pudiendo adoptar los números de las tarjetas temporales cualquier otra forma: serie de diecinueve cifras, serie alfanumérica de una longitud dada, etc.

Por otro lado, se puede proporcionar a cada tarjeta temporal un código secreto, que se llamará también código PIN (Personal Identification Number). La tarjeta temporal puede también incluir de manera más precisa su fecha y su hora de final de validez (por ejemplo, en formato día/mes/año hora (27/07/01 14:31)), estando destinada esta información únicamente al titular de la tarjeta.

Es por tanto el mismo comprador quien genera su propia tarjeta temporal a partir de un algoritmo adecuado instalado en su ordenador o con la tarjeta electrónica SIM de su teléfono móvil 6.

Vamos a considerar en primer lugar el uso del teléfono 6 para crear una tarjeta temporal. El comprador que desea realizar una compra, coge su teléfono 6 y lanza el programa correspondiente de creación de tarjeta temporal. La aplicación de este programa requiere que se marquen en el teclado del teléfono 6 las características de la tarjeta temporal y, en particular, el importe autorizado y el tiempo de validez.

El programa le comunica en respuesta todos los datos característicos de la tarjeta que ha creado, los cuales se verán en la pantalla de su teléfono 6 o bien le son simplemente indicados verbalmente en el auricular del aparato. Estos datos de identificación son el número de dieciséis cifras, una fecha de expiración y, si es el caso, un código secreto asociado.

Como la tarjeta se ha creado en primer lugar, el citado programa transfiere en un segundo paso todas las características de la tarjeta al servidor 4 de la entidad financiera en la que se encuentra la cuenta bancaria a la que está vinculada la tarjeta temporal y que será el gestor de esa tarjeta temporal. La transferencia se efectúa automáticamente a través de la red telefónica a la que está conectado el teléfono 6 del usuario, en forma de un mensaje SMS (Short Message Service).

El servidor 4 que es apto para recibir esos mensajes SMS, gestiona la nueva tarjeta temporal del mismo modo que si la hubiera creado él mismo.

De manera similar, la presente invención se puede aplicar con el microordenador 1 del comprador alojando el programa de creación de tarjeta correspon-

diente. Las características de la tarjeta temporal creada de este modo y sobre todo sus datos de identificación temporal se transmiten automáticamente al servidor 4 a través de la red Internet 2 y de la conexión SSL. Como variante, el comprador puede transferir directamente estos datos al servidor 4 utilizando su teléfono 6, por ejemplo, enviando un SMS.

El comprador, como ha obtenido directamente las informaciones de identificación de su tarjeta temporal creada de este modo con su teléfono 6 o su ordenador 1, se encuentra en situación de poder utilizarla.

El comprador sólo tiene que introducir el número y la fecha de expiración en el formulario de pedido de la página comercial 3.

Dado que el número y la fecha de expiración introducidas por el comprador son perfectamente similares a los de una tarjeta de pago tradicional, el comerciante no tiene que modificar sus procedimientos de transacción para aceptar el pedido del titular pagado con la tarjeta temporal. El comerciante no tiene ninguna posibilidad de diferenciar los números y por tanto el tipo de tarjeta de pago que se le comunican.

El comercial efectúa por tanto una petición de autorización totalmente clásica. Una vez obtenida en respuesta la autorización solicitada, se valida la transacción y el libro pedido puede ser entregado al comprador. El comerciante sólo tiene que entregar la factura correspondiente a su entidad financiera para que ésta pueda obtener la transferencia de fondos de la entidad emisora.

Por supuesto, la invención no se limita a los modos de realización arriba descritos.

De este modo, el teléfono 6 puede no ser un radioteléfono móvil de tipo GSM u otro sino un teléfono conectado a la red telefónica pública conmutada PSTN (Public Switching Telephone Network) y con capacidad de cálculo adecuada.

De este modo, los datos de identificación de las tarjetas de pago que se transmiten al servidor 4 por vía telefónica se pueden transmitir de distintos modos y no sólo por SMS. De este modo, puede serlo por voz (enunciación verbal en la línea), sin codificar o codificado utilizando una clave de encriptado de tipo Julio César, en el que cada cifra del cero al nueve tiene asociada una letra, habiendo dado la entidad financiera previamente y de manera segura la clave de encriptado al usuario.

De este modo, al acceder al servidor 4 con el teléfono 6 (ya sea a través de la red conmutada PSTN (Public Switching Telephone Network) o de una red de radioteléfono, por ejemplo de tipo GSM) para transmitir los datos de identificación de la tarjeta temporal creada y las condiciones de utilización de esta última, la identificación del usuario se podrá efectuar de distintos modos: mediante un sistema de reconocimiento de voz, utilizando un código secreto marcado en el teclado del teléfono o enunciado verbalmente en la línea, enviando un mensaje predefinido, etc.

REIVINDICACIONES

1. Procedimiento para proporcionar de manera segura datos de identificación de una tarjeta de pago a un usuario, **caracterizado** porque dichos datos de identificación de la tarjeta de pago los crea directamente dicho usuario a partir de medios de creación adecuados (6,1), siendo comunicados a continuación por el usuario, mediante medios de telecomunicación (6,5; 1,2) los datos de la tarjeta así creados a un servidor informático (4) de una entidad financiera gestora de dicha tarjeta.

2. Procedimiento según la reivindicación 1, **caracterizado** porque dichos datos de identificación consisten en el número y la fecha de expiración de dicha tarjeta de pago.

3. Procedimiento según alguna de las reivindicaciones 1 a 2, **caracterizado** porque dichos datos de identificación de la citada tarjeta de pago se crean directamente por medio de un teléfono (6) especialmente adecuado para ello.

4. Procedimiento según la reivindicación 3, **caracterizado** porque dichos datos son elaborados con un software adecuado que facilita la tarjeta con microprocesador SIM que lleva un radioteléfono celular de tipo GSM (6).

5. Procedimiento según alguna de las reivindicaciones 3 a 4, **caracterizado** porque dicho teléfono (6) comunica automáticamente dichos datos de identificación al citado servidor (4).

6. Procedimiento según las reivindicaciones 4 y 5, **caracterizado** porque dichos datos se comunican al servidor (4) a través de la red de telefonía celular (5) en forma de un mensaje SMS.

7. Procedimiento según alguna de las reivindicaciones 1 a 2, **caracterizado** porque dichos datos de identificación de la citada tarjeta de pago se crean directamente por medio de un microordenador personal (1).

8. Procedimiento según alguna de las reivindicaciones precedentes, **caracterizado** porque dicho microordenador (1) comunica automáticamente los citados datos de identificación al citado servidor (4) utilizando la red Internet (2).

9. Procedimiento según alguna de las reivindicaciones precedentes, **caracterizado** porque dicha tarjeta de pago sólo es válida para un número limitado de transacciones y por un tiempo limitado.

10. Procedimiento según alguna de las reivindicaciones precedentes, **caracterizado** porque dicha tarjeta de pago sólo es válida para una transacción.

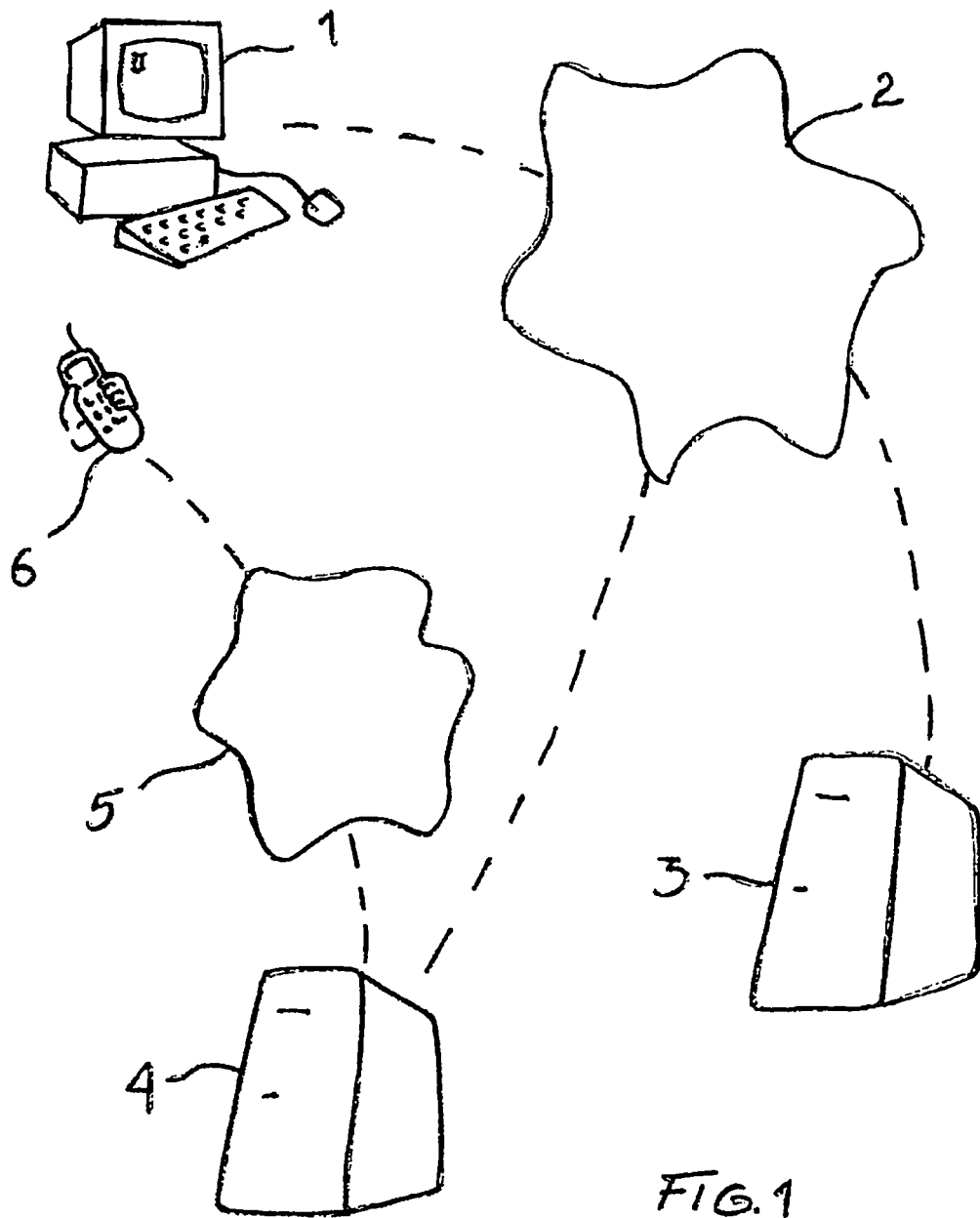


FIG. 1