(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 307 481**

(51) Int. Cl.:
G06Q 20/00 (2006.01)
G07F 7/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **00200558 .5**
(96) Fecha de presentación : **30.04.1998**
(97) Número de publicación de la solicitud: **1003139**
(97) Fecha de publicación de la solicitud: **24.05.2000**

(54) Título: **Sistema y método de recarga de una tarjeta de valor almacenado.**

(30) Prioridad: **30.04.1997 US 45883 P**
16.10.1997 US 951614

(45) Fecha de publicación de la mención BOPI:
01.12.2008

(45) Fecha de la publicación del folleto de la patente:
01.12.2008

(73) Titular/es:
VISA INTERNATIONAL SERVICE ASSOCIATION
900 Metro Center Boulevard
Foster City, California 94404, US

(72) Inventor/es: **Davis, Virgil M.;**
Cutino, Suzanne C.;
Berg, Michael J.;
Conklin, Fredrick Sidney y
Pringle, Steven John

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Sistema y método de recarga de una tarjeta de valor almacenado.

Campo de la invención

La presente invención se refiere en general a un sistema de carga de valor usando una red de ordenadores. Más específicamente, la presente invención se refiere a un sistema de carga de valor para una tarjeta inteligente usando una red abierta tal como Internet.

Antecedentes de la invención

Con el explosivo crecimiento de las redes abiertas (tal como Internet) en los últimos varios años y el rápido aumento del número de consumidores con acceso a la web mundial, ha habido gran interés por el desarrollo de comercio electrónico en Internet. Las transacciones financieras tradicionales se están transformando.

Varios proveedores de servicios han introducido esquemas de pago para soportar la compra de artículos o servicios en línea en un entorno de comercio virtual. Estos acercamientos han usado varios modelos basados en métodos de pago tradicionales existentes en el mercado directo al por menor, incluyendo tarjetas de crédito/débito, cheques y dinero en efectivo. Sin embargo, por varias razones, varios de estos numerosos esquemas tienen inconvenientes especiales.

Actualmente, un consumidor puede usar su tarjeta de crédito o débito tradicional para hacer una compra por Internet. Un consumidor suministra simplemente el número de cuenta de su tarjeta que posteriormente es transmitido a través de Internet a un comerciante y la transacción de pago se completa de forma tradicional para una tarjeta de crédito. A menudo, estos números de cuenta son transmitidos por Internet con seguridad sumamente limitada o nula. La seguridad se puede mejorar mediante el uso del protocolo "Secure Electronic Transaction" publicado por Visa International y Mastercard en 1996. Estas transacciones todavía requieren alguna forma de validación de la tarjeta y comprobación del saldo. Estas comprobaciones son realizadas en línea entre el comerciante, un comprador y un banco emisor, un proceso que puede ser lento e ineficiente cuando el valor de la transacción es bajo, o cuando tienen lugar varias transacciones de poco valor en un corto período de tiempo.

El cheque electrónico imita al cheque de papel, pero es iniciado electrónicamente usando firma digital y criptografía pública. Los bancos recogen depósitos mediante correo electrónico y los compensan a través de canales existentes tales como la cámara de compensación automatizada (ACH). Sin embargo, la utilización de dicho cheque electrónico por parte del consumidor tiene varios inconvenientes. Uno es que las firmas digitales y el encriptado público hacen necesario el uso de una autoridad de certificación que aumenta las entidades adicionales y pasos "netos" a la transacción. Además, se necesita un registro de tenedores de tarjetas.

Otras alternativas de pago por Internet están modeladas sobre las transacciones de dinero en efectivo e incluyen varios esquemas. Con CyberCash, el consumidor añade el número de su tarjeta de crédito a una factura electrónica recibida del comerciante, devuelve el número de tarjeta de crédito al comerciante que entonces es procesado y enviado a CyberCash donde es tratado posteriormente como una transacción normal con tarjeta de crédito. Sin embargo, esta técnica tiene algunas de las desventajas explicadas anteriormente con respecto a la transacción tradicional con tarjeta de crédito en Internet y requiere un trabajo adicional por parte del comerciante al procesar el número de tarjeta de crédito. También se pueden realizar transacciones de débito, pero es preciso que el consumidor abra una cuenta CyberCash con anterioridad.

Un sistema digital basado en fichas para transacciones por Internet ha sido implementado por DigiCash. Con DigiCash, se compran a DigiCash las denominadas "monedas digitales" de una cuenta de depósito preconsolidada y almacenan en el disco duro del consumidor. Estas monedas digitales son utilizadas posteriormente para una transacción por Internet con un comerciante. Este esquema tiene desventajas porque el consumidor debe establecer primero una relación con DigiCash y usar una tarjeta de crédito o instrumento similar para comprar estas monedas digitales, que entonces deben ser descargadas al ordenador del consumidor. Esta transacción puede ser lenta para el consumidor y está sujeta a fraude. Además, un comerciante debe estar preparado no solamente para aceptar estas monedas digitales, sino también para verificar su autenticidad, confirmar la transacción, y posteriormente enviar finalmente estos números a su banco con el fin de recibir finalmente el pago. Un inconveniente desde el punto de vista del comerciante es que el comerciante debe realizar mucho trabajo relacionado con la transacción.

Otro esquema para completar una transacción por Internet lo ofrece First Virtual Holding, Inc. First Virtual ofrece una solución de software basada en un único número de identificación y confirmación por correo electrónico. Para usar este esquema, un consumidor abre una cuenta especial con First Virtual y posteriormente recibe un número de identificación confidencial. Cuando el consumidor desea comprar un producto o servicio por Internet, envía un mensaje de correo electrónico conteniendo el número de identificación confidencial al comerciante. El comerciante envía posteriormente el número a First Virtual por correo electrónico para verificación e identificación del cliente. First Virtual confirma posteriormente con el consumidor por correo electrónico que el consumidor inició de hecho la transacción y desea hacer la compra. Este esquema tiene los inconvenientes de que el consumidor debe abrir primero una cuenta especial con First Virtual. Además, el comerciante debe comunicar con First Virtual para identificar al

cliente y para identificar el número de cuenta de la tarjeta de crédito del consumidor que es identificada por el número de identificación confidencial.

Aparte de los esquemas de pago por Internet, una técnica en uso para realizar una transacción financiera en un terminal autónomo usa una tarjeta inteligente. Una tarjeta inteligente es típicamente una tarjeta de plástico del tamaño de una tarjeta de crédito que incluye un chip semiconductor para contener el equivalente digital de dinero en efectivo directamente, en lugar de anotar en una cuenta o proporcionar créditos. Cuando se usa una tarjeta de este tipo para hacer una compra, el equivalente digital de dinero en efectivo es transferido al "registro de caja" del comerciante y posteriormente a una institución financiera. Las tarjetas de valor almacenado son recargables (el valor se puede recargar en la tarjeta usando un terminal) o no recargables (el valor de la tarjeta disminuye con cada transacción y se tira cuando se ha agotado su valor).

Físicamente, una tarjeta inteligente se asemeja a menudo a una tarjeta de "crédito" tradicional que tiene uno o más dispositivos semiconductores unidos a un módulo incrustado en la tarjeta, que proporciona contactos al mundo exterior. La tarjeta puede conectar con un terminal de punto de venta, un CA, o un lector de tarjetas integrado en un teléfono, un ordenador, una máquina vendedora, o cualquier otro aparato. Un dispositivo microcontrolador de semiconductores incrustado en una tarjeta inteligente de "procesador" permite a la tarjeta llevar a cabo un rango de operaciones computacionales, almacenamiento protegido, encriptado y toma de decisiones. Tal microcontrolador incluye típicamente un microprocesador, memoria, y otros elementos de hardware funcionales. Varios tipos de tarjetas se describen en "The Advanced Card Report: Smart Card Primer", Kenneth R. Ayer y Joseph F. Schuler, The Schuler Consultancy, 1993.

Un ejemplo de una tarjeta inteligente implementada como una tarjeta de procesador se ilustra en la figura 1. Naturalmente, una tarjeta inteligente se puede implementar de muchas formas, y no tiene que incluir necesariamente un microprocesador u otras características. La tarjeta inteligente puede ser programada con varios tipos de funcionalidad, tal como una aplicación de valor almacenado; crédito/débito; programas de lealtad, etc. A los efectos de esta descripción, la tarjeta 5 está programada al menos con una aplicación de valor almacenado, y se denominará tarjeta de "valor almacenado" 5.

Una tarjeta de valor almacenado 5 tiene un microcontrolador incrustado 10 que incluye un microprocesador 12, memoria de acceso aleatorio (RAM) 14, memoria de lectura solamente (ROM) 16, memoria no volátil 18, un módulo de encriptado 22, y una interface de lector de tarjetas 24. Otras características del microcontrolador pueden estar presentes, pero no se muestran, tal como un reloj, un generador de números aleatorios, control de interrupciones, control lógico, una bomba de carga, conexiones de potencia, y contactos de interface que permiten que la tarjeta comunique con el mundo exterior.

El microprocesador 12 es cualquier unidad central de proceso adecuada para ejecutar órdenes y controlar el dispositivo. La RAM 14 sirve como almacenamiento de los resultados calculados y como memoria de pila. La ROM 16 guarda el sistema operativo, datos fijos, rutinas estándar, y tablas de consulta. Una memoria no volátil 18 (tal como EPROM o EEPROM) sirve para almacenar información que no se debe perder cuando la tarjeta se desconecte de una fuente de potencia, pero que también debe ser alterable para acomodar datos específicos de tarjetas individuales o posibles cambios sobre la duración de la tarjeta. Esta información podría incluir un número de identificación de tarjeta, un número de identificación personal, niveles de autorización, saldos de dinero en efectivo, límites de crédito, etc. El módulo de encriptado 22 es un módulo de hardware opcional usado para realizar una variedad de algoritmos de encriptado. La interface de lector de tarjetas 24 incluye el software y hardware necesarios para comunicación con el mundo exterior. Una amplia variedad de interfaces son posibles. A modo de ejemplo, la interface 24 puede proporcionar una interface de contacto, una interface de acoplamiento próximo, una interface de acoplamiento remoto, u otras varias interfaces. Con una interface de contacto, las señales del microcontrolador son dirigidas a varios contactos metálicos en el exterior de la tarjeta que entran en contacto físico con contactos similares de un dispositivo lector de tarjetas.

Un uso posible de una tarjeta de valor almacenado por un consumidor se ilustra en la figura 2. La figura 2 ilustra un diagrama de bloques de un terminal de pago de servicio operado por el cliente 50. Un cliente usa típicamente tal terminal de pago de servicio en un entorno de cara a cara con el fin de comprar artículos en una tienda o directamente del terminal propiamente dicho. El terminal de pago de servicio 50 puede ser un dispositivo atendido o puede estar integrado en un dispositivo de autoservicio tal como una máquina vendedora o teléfono público. Por ejemplo, el terminal de pago de servicio puede estar incorporado en una máquina de bebidas con el fin de dispensar bebidas a un cliente, en la que el cliente paga introduciendo la tarjeta de valor almacenado. O el terminal de pago de servicio puede ser un terminal de punto de venta tal como el hallado en un mostrador de caja donde un cliente introduce su tarjeta de valor almacenado con el fin de comprar artículos.

El terminal de pago de servicio 50 incluye un router 51, una interface de usuario 52, un manipulador/lector de tarjetas 54, un manipulador de tarjetas de seguridad 56, una tarjeta de seguridad 58, una aplicación de terminal 60, un dispositivo de almacenamiento de datos 64 y un manipulador de punto de concentración 66. El router 51 es hardware y software para dirigir información entre bloques funcionales. La interface de usuario 52 controla el estado de la pantalla en el terminal y suministra instrucciones al usuario. Por ejemplo, la interface de usuario proporciona instrucciones relativas a la introducción de la tarjeta de valor almacenado 5 o tarjeta de seguridad 58. Además, la interface de usuario proporciona instrucciones y/o botones para que el cliente interactúe con la aplicación de terminal 60 con el fin

de comprar artículos y/o servicios. El manipulador de tarjetas 54 proporciona un lector físico de tarjetas y software asociado para aceptar y comunicar con tarjetas de valor almacenado 5. Igualmente, el manipulador de tarjetas de seguridad 56 proporciona un lector de tarjetas y software asociado para comunicar con tarjetas de seguridad 58. En unión con el manipulador de tarjetas de seguridad 56, la tarjeta de seguridad 58 controla la secuencia de órdenes del terminal y realiza transacción y una seguridad por lotes.

La aplicación de terminal 60 recibe órdenes e información acerca de la transacción e inicia la compra real. Además, la aplicación de terminal 60 es responsable de toda la funcionalidad específica de aplicación tal como guiar al cliente en el uso del terminal mediante una pantalla, y proporcionar todo el hardware y software necesarios para dar al usuario un artículo y/o servicio una vez que ha sido informado por la tarjeta de seguridad de que un valor apropiado ha sido deducido de la tarjeta de valor almacenado.

El dispositivo de almacenamiento de datos 64 controla el almacenamiento de transacciones de compra y totales. El manipulador de punto de concentración 66 controla el envío y la recepción de información a y de un punto de concentración. El punto de concentración 68 es un ordenador de etapa que comunica con cualquier número de terminales de pago de servicio para recoger lotes de transacciones. El punto de concentración envía entonces estos lotes de transacciones a un sistema de compensación y administración para procesado (tal como en la figura 3). Una vez procesados, los reconocimientos de lotes, junto con otras actualizaciones del sistema, son enviados a los terminales mediante el punto de concentración. El punto de concentración asegura una transferencia satisfactoria de datos entre los terminales de pago de servicio y el sistema de compensación y administración, y evita la sobrecarga del sistema de compensación y administración. El proveedor de servicios contrata con un punto de concentración para la recogida de los pagos de servicios. El punto de concentración también puede ser una instalación central existente tal como una compañía telefónica que recoge sus propios pagos de teléfonos de tarjeta.

Tal terminal de pago de servicio 50 permite al cliente usar una tarjeta de valor almacenado para el pago de artículos y/o servicios, genera un resultado de pago de una transacción, y agrupa resultados de pago individuales en una colección para transferencia a un sistema de compensación y administración, que entonces transfiere fondos que habían sido adeudados en una tarjeta de valor almacenado del cliente al comerciante cuyos artículos y/o servicios han sido comprados en el terminal.

La figura 3 ilustra un entorno 100 útil para emitir tarjetas de valor almacenado y reconciliar transacciones realizadas con tal tarjeta. Un proveedor de terminales 102 crea el equipo usado por un proveedor de servicios 104 para suministrar artículos y/o servicios a clientes que tienen una tarjeta de valor almacenado en un terminal de pago de servicio 50. El proveedor de tarjetas 106 contrata con un fabricante de circuitos integrados y un fabricante de tarjetas para circuitos integrados y cuerpos de tarjetas de plástico, entonces embebe los circuitos integrados en las tarjetas y los inicializa con un número de serie. Entonces suministra las tarjetas al emisor de tarjetas 108. En unión con el sistema de compensación y administración 110 (tal como un sistema proporcionado por Visa International de Foster City, CA), el emisor de tarjetas 108 personaliza nuevas tarjetas y posteriormente transfiere estas tarjetas a individuos (tenedores de tarjetas 112). El tenedor de tarjeta puede cargar entonces en la tarjeta un valor antes de usarla. Alternativamente, la tarjeta puede venir con valor ya cargado. El tenedor de tarjeta 112 puede usar entonces la tarjeta en un terminal de pago de servicio 50 para comprar artículos y/o servicios del proveedor de servicios 104. El terminal 50 adeuda entonces el valor de la tarjeta, creando así un pago de servicio.

Periódicamente, todas las transacciones son enviadas en un archivo de datos desde el terminal 50 mediante el punto de concentración 68 y un comprador 114 al sistema de compensación y administración por lotes 110 junto con lotes acumulados de pago de servicio de otros terminales. En base a estos datos de recogida, el sistema de compensación y administración 110 recibe entonces dinero del emisor de tarjetas 108 que originalmente procedía del tenedor de tarjeta 112. El sistema de compensación y administración 110 transfiere entonces una suma global al comprador 114 usando un servicio de liquidación adecuado (tal como el proporcionado por Visa International) para pagar a los varios proveedores de servicios que tienen relación con el comprador 114. En base a los datos previamente recogidos, el comprador 114 transfiere entonces a cada proveedor de servicios 104 una cantidad apropiada de dinero que refleja el valor de los artículos y/o servicios que el proveedor de servicios realizó ese día a tenedores de tarjetas en base a las deducciones de sus tarjetas de valor almacenado.

Aunque tal terminal de pago de servicio descrito anteriormente es útil para la compra *in situ* de artículos por un consumidor con una tarjeta inteligente, no permite la compra de artículos y/o servicios por un cliente por una red. Tampoco permite dicho terminal la transferencia inmediata de información electrónica a un ordenador del consumidor. Los terminales de pago de servicio son típicamente unidades de hardware y software de diseño especial situadas en un comercio. Además, el terminal de pago de servicio está diseñado para integrar en una posición de hardware las funciones de la aplicación de terminal (proporcionar artículos y/o servicios), un manipulador de tarjetas para la tarjeta de valor almacenado, y la gestión de transacciones realizada en la tarjeta de seguridad. Tal diseño no es adecuado para transacciones donde un cliente puede desear realizar una transacción desde casi cualquier posición (incluyendo la casa u oficina) rápida y fácilmente con un mínimo de preparación y gasto. Además, aunque se han sugerido varios esquemas de pago por Internet, no están orientados a transacciones de poco valor, y no permiten el uso de una tarjeta inteligente para transacciones por Internet.

Así, sería deseable tener una arquitectura y sistema que permitiesen a un consumidor realizar rápida y fácilmente transacciones por una red abierta tal como Internet usando una tarjeta inteligente. También es deseable tener una

arquitectura y sistema donde un usuario puede usar una tarjeta inteligente para compras por Internet así como compras en terminales de pago de servicio existentes.

Sin embargo, para comprar, primero hay que cargar un valor en la tarjeta. El valor puede ser cargado de varias formas en una tarjeta de valor almacenado. Actualmente, es inconveniente que un usuario cargue valor en su tarjeta de valor almacenado. Un usuario debe ir físicamente a un banco u otra institución que tenga un cajero automático (CA) u otro dispositivo similar con el fin de cargar valor en su tarjeta de valor almacenado. El usuario puede introducir dinero en la máquina y pasar el valor correspondiente a la tarjeta de valor almacenado, el usuario puede usar una tarjeta de débito pare deducir el valor de la cuenta de usuario en el banco para transferirlo a la tarjeta, o se puede usar una tarjeta de crédito como la fuente de fondos a transferir a la tarjeta de valor almacenado. En cualquier caso, el usuario debe ir al banco a cargar valor. También crea dificultades el hecho de que no todos los bancos u otras instituciones financieras tengan tal máquina para cargar valor en una tarjeta de valor almacenado del usuario.

Consiguientemente, también sería deseable tener una técnica que permitiese a un usuario cargar conveniente y fácilmente valor en una tarjeta de valor almacenado.

La solicitud de patente internacional WO 94/28498 describe un sistema y método para revalorización de tarjetas inteligentes usando una red telefónica pública.

Resumen de la invención

Para lograr lo anterior, se describe una arquitectura y sistema que permite cargar valor en una tarjeta inteligente en línea por una red abierta tal como Internet.

En un primer aspecto de la presente invención, una técnica de carga permite al consumidor cargar convenientemente un valor en su tarjeta de valor almacenado desde cualquier dispositivo adecuado mediante una red abierta tal como Internet. Un consumidor puede utilizar cualquier ordenador adecuado en la casa, oficina o en otro lugar con el fin de conectar a su banco u otra institución financiera. Usando integridad de mensaje apropiada, se transfiere valor desde el banco a la tarjeta de valor almacenado del consumidor. Al mismo tiempo, el valor correspondiente es transferido desde el banco al emisor de tarjetas de valor almacenado a través de redes existentes para posterior liquidación con un comerciante a quien el consumidor compra artículos o servicios. Ventajosamente, esta realización utiliza un sistema existente de compensación y administración para liquidación eventual de la transacción entre el comerciante y el emisor de tarjetas. Además, la transacción es completamente auditable y en la tarjeta se guarda un registro de transacciones previas para posterior visualización. Así, un consumidor puede cargar convenientemente valor en su tarjeta mientras se mantiene un nivel alto de seguridad y el emisor de tarjetas puede sacar provecho d los fondos no gastados de la tarjeta.

Desde la perspectiva del consumidor, la presente invención opera de forma similar a cargar una tarjeta de valor almacenado en un CA, a excepción de que el consumidor no tiene que introducir dinero en efectivo o una tarjeta de débito o crédito adicional, no tiene que ir a un banco. La funcionalidad de carga se distribuye a través de Internet entre el dispositivo de lectura de tarjetas situado donde está el cliente, un servidor de banco que lleva la cuenta del consumidor, y un servidor de carga con un módulo de seguridad central que proporciona seguridad. Todas estas entidades pueden estar físicamente remotas una de otra, proporcionando Internet la funcionalidad de enrutamiento.

Además, un banco solamente tiene que hacer una inversión mínima en tiempo y dinero para aprovechar la presente invención con el fin de permitir a sus clientes cargar valor desde sus cuentas existentes por Internet. El banco no tiene que participar en el desarrollo de software complejo personalizado o procedimientos de contabilidad. Incorporando librerías de software, un banco está preparado para comenzar a cargar valor en las tarjetas de sus clientes desde su sitio web. Preferiblemente, se facilitan librerías que conectan con un servidor existente en un banco para facilitar la creación de una página HTML. Dado que se usa una tarjeta inteligente con una aplicación de valor almacenado, el servidor de banco, el servidor de carga y el terminal de cliente realizan los detalles de la transacción y el banco propiamente dicho queda liberado de tener que controlar y hacer el seguimiento de una transacción. Además, el servidor de carga y tarjeta de valor almacenado gestionan y proporcionan seguridad a la transacción. Es decir, el banco no tiene que preocuparse por seguridad ni ser responsable de autenticar una tarjeta de valor almacenado ni de determinar un saldo en la tarjeta.

El servidor de carga y su módulo de seguridad los proporciona una institución financiera separada o un procesador de terceros.

La presente invención proporciona beneficios a emisores y compradores. La expansión de la funcionalidad para una tarjeta de valor almacenado incrementa las oportunidades de negocio de tenedores de tarjetas y comerciantes. Además, puede haber nuevas oportunidades comerciales para los compradores. La presente invención también ofrece una solución de micropago para comercio electrónico sin la necesidad de introducir un producto separado o marca o de establecer nuevas relaciones con proveedores de servicios. Además, en una realización específica de la invención, los fondos que se cargan en una tarjeta son transferidos desde el banco de carga al emisor de tarjetas de modo que el emisor pueda sacar ventaja de los fondos de la tarjeta hasta que se gasten.

Otra ventaja de la presente invención es su capacidad de minimizar el tráfico de transacciones en Internet y de minimizar la cantidad de tiempo que una tarjeta de seguridad (o un módulo de seguridad) pasa en una transacción.

En el aspecto de pago, emulando las órdenes de las tarjetas de seguridad dadas a una tarjeta de valor almacenado, un terminal de cliente es capaz de recibir y agrupar respuestas relativas a transmisión a un servidor de pago todas a la vez, en vez de una a una por Internet. El servidor de pago es entonces capaz de emular una tarjeta de valor almacenado puesto que interactúa con la tarjeta de seguridad al suministrar las respuestas a la tarjeta de seguridad. El resultado es menos tráfico de mensajes por Internet, ahorro de tiempo e interrupciones.

Además, suministrando una firma esperada de la tarjeta de valor almacenado al servidor de pago, la tarjeta de seguridad se libera de tener que comparar las firmas propiamente dichas, y se puede liberar antes y pasar a una nueva transacción. El servidor de pago también puede suministrar la firma esperada de tarjeta de valor almacenado al terminal de cliente o servidor de comerciante para comparación, reduciendo así la ida y vuelta del tráfico de mensajes entre el servidor de pago y el terminal de cliente.

La presente invención es adecuada para uso con cualquier tipo de tarjeta de valor almacenado que sea capaz de almacenar una cantidad y de decrementar un valor a una orden. En una realización de la invención, una tarjeta de valor almacenado implementada como una tarjeta de procesador funciona bien. El uso de una tarjeta de procesador tiene ventajas donde el procesado de información se realiza en la tarjeta más bien que en el terminal u ordenador central. Las tarjetas de procesador permiten que el encriptado lo realice la tarjeta, permiten la generación de firmas, y pueden acomodar múltiples contraseñas o identificación personal (tal como biometría que identifican de forma única al tenedor de la tarjeta). Las tarjetas de procesador también proporcionan mayor seguridad de los datos, una capacidad anti-fraude, flexibilidad en las aplicaciones, una capacidad multiuso, y validación fuera de línea. Dado que los altos costos de las telecomunicaciones y/o la baja fiabilidad de una red pueden hacer inviable la autorización en línea, una tarjeta de valor almacenado con la capacidad de realizar procesado y autenticación fuera de línea por sí misma es sumamente valiosa.

Breve descripción de los dibujos

Ejemplos de la presente invención se describirán ahora con detalle con referencia a los dibujos acompañantes, en los que:

La figura 1 es un diagrama de bloques de un ejemplo de una tarjeta de valor almacenado útil en realizaciones de la presente invención.

La figura 2 es un diagrama de bloques de un terminal de pago de servicio en el que se puede introducir una tarjeta de valor almacenado para comprar mercancías.

La figura 3 es un diagrama de bloques de un ejemplo de un sistema de compensación y administración útil para reconciliar transacciones financieras recibidas de un terminal de pago de servicio.

La figura 4 ilustra un sistema para cargar valor en una tarjeta de valor almacenado según una realización de la presente invención.

Las figuras 5A-5D son un diagrama de flujo que describe la carga de una tarjeta de valor almacenado del consumidor usando una realización de la presente invención.

Y la figura 6 es un diagrama de bloques de un sistema informático típico adecuado para uso en realizaciones de la presente invención.

Descripción detallada

La presente invención separa la funcionalidad implicada en una transacción usando una tarjeta de valor almacenado para aprovechar las capacidades de enrutamiento de Internet.

La figura 4 ilustra un sistema 850 para cargar valor en una tarjeta de valor almacenado según una realización de la presente invención. El sistema 850 incluye un terminal de cliente 204, servidor de banco 860 y servidor de carga 862. El terminal de cliente 204 comunica con la tarjeta 5 mediante el lector de tarjetas 210, y con el servidor de banco 860 y el servidor de carga 862 por cualquier red abierta adecuada tal como Internet 202.

Preferiblemente, cada terminal de cliente 204, servidor de banco 860 y servidor de carga 862 implementan un módulo de código (de operación similar al módulo de códigos descrito anteriormente) en el lenguaje de programación Java que realiza la funcionalidad descrita más adelante. Para simplicidad de la explicación, a continuación se hará referencia a “terminal de cliente”, “servidor de banco” y “servidor de carga” incluso aunque el código residente realice las funciones. El emisor de tarjetas 108 se ha descrito previamente en la figura 3. El emisor de tarjetas 108 puede ser una institución financiera separada del banco que incluye el servidor de banco 860, o el emisor de tarjetas 108 puede ser el mismo banco que incluya el servidor de banco 860.

El servidor de banco 860 es cualquier ordenador adecuado dentro de un banco u otra institución financiera. A modo de ejemplo, el servidor de banco 860 es cualquier ordenador personal adecuado, una estación de trabajo o un ordenador mainframe. En una realización, el servidor de banco 860 ejecuta un programa "servlet" (un applet de Java que funciona en el servidor) para comunicación con el cliente 204.

El servidor de carga 862 también es cualquier ordenador adecuado y puede estar situado en una posición de terceras partes (tal como en un procesador). El servidor de carga 862 también ejecuta un programa servlet para comunicación con el terminal de cliente 204 y el módulo de seguridad central 864.

El módulo de seguridad central (HSM) 864 es un dispositivo conocido en la técnica que puede ser realizado en una "caja negra" de hardware o en cualquier ordenador adecuado. El módulo de seguridad central puede ser implementado en un módulo de hardware fuera del servidor de carga 862, puede ser implementado dentro del servidor de carga 862, puede ser implementado en software, o puede ser implementado como una tarjeta de seguridad descrita anteriormente. El módulo de seguridad central 864 contiene las claves de encriptado en hardware usado para generar firmas (por ejemplo S1, S2 y S3) que proporcionan seguridad para la transacción. Estas firmas son utilizadas por la tarjeta de valor almacenado 5 y el módulo de seguridad central 864 para asegurar que la tarjeta no esté caducada o sea falsa (es decir, que sea una tarjeta válida), para asegurar que el módulo 864 sea auténtico, para asegurar que el sistema 850 sea auténtico y, en general, para realizar una transacción válida y para evitar el fraude. La tarjeta 5 también incluye claves de encriptado para la generación de una firma de tarjeta de valor almacenado. En una realización alternativa, el módulo 864 podría ser sustituido por un terminal estándar que incluya una tarjeta de seguridad tal como se representa en las realizaciones anteriores. En esta situación, las claves de encriptado se almacenarían en la tarjeta de seguridad.

Brevemente, el sistema 850 opera de la siguiente manera. Un consumidor accede al servidor de banco 860 mediante el terminal de cliente 204. Suponiendo que la tarjeta 5 no esté sobrecargada y que la cuenta del usuario con el banco tenga fondos suficientes, el usuario es capaz de descargar valor mediante el servidor de banco 860 a su tarjeta de valor almacenado 5. El terminal de cliente 204 comunica con el servidor de carga 862 para recibir autorización para la carga y para mayor seguridad. La tarjeta 5 puede ser usada entonces para hacer compras por Internet como se ha descrito anteriormente en la aplicación o puede ser usada para compras en otro lugar. Una vez que el banco ha descargado valor en la tarjeta 5, se transfiere una cantidad correspondiente de fondos del banco al emisor de tarjetas 108.

El emisor de tarjetas 108 pone estos fondos en un depósito de retención. Una vez que la tarjeta de valor almacenado 5 se usa para hacer una compra a un comerciante, la transacción es capturada y liquidada a través de un servicio de liquidación, tal como VisaNet. El banco emisor decrementa el depósito de fondos en la cantidad de la compra, que es pagada al banco del comerciante. El banco del comerciante paga la transacción al comerciante. La liquidación puede tener lugar de cualquier forma adecuada, como es conocido en la técnica y, en particular, puede ser implementada como se ha descrito previamente en la figura 3.

Una realización de una técnica por la que se carga una tarjeta de valor almacenado por Internet, se describirá ahora usando el diagrama de flujo de las figuras 5A a 5D con referencia a la figura 4. Varios de los pasos siguientes pueden tener lugar en un orden diferente; la descripción siguiente tiene fines ilustrativos.

Algunos detalles de implementación mencionados anteriormente con respecto al pago son igualmente aplicables a la carga de una tarjeta de valor almacenado. Además, el flujo ejemplar representado en las figuras ilustra una transacción satisfactoria (aunque un resultado negativo también se explica a continuación en el texto). Por esta razón, se hace referencia a un mensaje de "confirmación", que se puede denominar más ampliamente un mensaje de "resultado" (para reflejar ambas posibilidades de éxito y fallo de una carga). Además, se hace referencia a un mensaje de "carga exitosa", que también se puede denominar un mensaje de "confirmación", para reflejar su estado como confirmar un resultado positivo de la carga o un resultado negativo de la carga.

Inicialmente, el usuario usa un navegador web adecuado del terminal de cliente 204 para acceder a un sitio de Internet del servidor de banco. En el paso 871 el usuario selecciona una opción de cargar valor en la tarjeta 5. En el paso 872 el servidor de banco envía una petición de información de la tarjeta (incluyendo saldo actual de la tarjeta y saldo máximo de la tarjeta); el terminal de cliente 204 lee el saldo corriente de la tarjeta, divisa, y otra información de la tarjeta mediante el lector de tarjetas 210 y devuelve el saldo al servidor de banco 860. En el paso 873 el servidor de banco determina el valor de carga máxima y verifica que haya fondos suficientes en la cuenta del usuario para aceptar una petición de carga.

En el paso 874 el servidor de banco crea una página HTML que incluye los siguientes parámetros applet del cliente: el valor de carga; el tipo de divisa usado; el puerto y la dirección IP del servidor de carga; un identificador de transacción único usado por el servidor de carga y el servidor de banco para el seguimiento de una transacción; un identificador de banco único asignado al banco y conocido por el servidor de carga; y una clave de sesión. También se puede incluir otra información tal como el exponente de divisa, una dirección URL de estado del servidor de banco usada para comunicación del terminal de cliente, y otra información de seguridad para asegurar la identidad del servidor de banco y la integridad del mensaje. También se puede comunicar otra información relacionada con proceso tal como nivel de versión del software, metodología de encriptado y claves. Una vez creada esta página, la página es enviada al navegador del cliente solicitante y dispara la activación del módulo de código de cliente (en este ejemplo un applet de Java) en el terminal de cliente.

Para determinar el valor de carga, el servidor de banco pide al usuario que introduzca la cantidad a cargar en la tarjeta. Suponiendo que la cuenta de usuario sea adecuada, el servidor de banco pide que se adeude el valor de carga en la cuenta de usuario en el paso 875. Ventajosamente, la petición de débito del servidor de banco puede usar el CA y sistemas contabilidad existentes del banco para adeudar la cuenta de usuario. Desde el punto de vista del banco, el valor es transferido de la cuenta del usuario en gran parte de la misma forma que se transferiría el valor a un usuario en forma de dinero en efectivo en un CA. Pero en esta situación el valor no se da como dinero en efectivo en un CA, sino que es enviado por Internet a una tarjeta de valor almacenado.

En el paso 876 el terminal de cliente interactúa con la tarjeta de valor almacenado 5 para obtener información acerca de la tarjeta con el fin de crear un mensaje de petición de carga para transmisión posterior al servidor de carga 862. Una vez recibidas las respuestas de la tarjeta, el terminal del cliente combina estas respuestas en una corriente de bytes adecuada para transmisión por una red a un servidor de carga.

El terminal de cliente emula unas varias órdenes del módulo de seguridad central 864 para recibir respuestas de dichas órdenes de la tarjeta de valor almacenado. La tarjeta de valor almacenado y el módulo de seguridad están físicamente separados uno de otro; la comunicación tiene lugar por Internet. En el interés de la velocidad y fiabilidad, es ventajoso intercambiar solamente los mensajes tradicionales de autenticación, respuesta y confirmación.

Para operar de forma segura y fiable en este entorno, en una realización de la presente invención el terminal de cliente emula un módulo de seguridad y recoge todas las respuestas para transmisión en un mensaje de petición de carga. El mensaje de petición de carga puede incluir una variedad de información e incluye preferiblemente una primera firma de tarjeta (denominada S1), un número de tarjeta, una fecha de caducidad, y una cantidad de carga. También se facilita preferiblemente otra información tal como el algoritmo de seguridad, contador de transacciones, saldo corriente de la tarjeta, y sello de fecha del servidor de banco.

Cuando se preempaqueta toda esta información en un solo mensaje de petición de carga, se minimiza el número de mensajes intercambiados entre la tarjeta de valor almacenado y el módulo de seguridad por Internet.

A continuación, en el paso 877, el terminal de cliente accede al servidor de carga usando la dirección IP recibida del servidor de banco. En el paso 878 el terminal de cliente envía el mensaje de petición de carga al servidor de carga. En el paso 879 el servidor de carga procesa la petición de carga en unión con un módulo de seguridad central asociado 864, como se explicará con más detalle más adelante con referencia a la figura 5D. Después del paso 879, el servidor de carga ha recibido una firma del módulo de seguridad del emisor (denominada S2) como parte de una orden de carga del módulo de seguridad 864. La firma de módulo de seguridad es un valor que identifica de forma única y valida el módulo de seguridad para demostrar a la tarjeta de valor almacenado 5 que la orden de carga entrante es una orden válida de un módulo de seguridad real. Así, al usuario de la tarjeta de valor almacenado, y a otras partes interesadas se les garantiza que se ha producido una carga válida de la tarjeta. En una realización preferida de la invención, la firma de módulo de seguridad es un valor encriptado asegurando que ninguna otra entidad puede falsificar una identidad de un módulo de seguridad.

En el paso 880 el servidor de carga envía la orden de carga con incluyendo la firma de módulo de seguridad al terminal de cliente para que la tarjeta de valor almacenado se cargue. En el paso 881, al recibir la orden de carga del servidor de carga, el terminal de cliente pasa la orden de carga a la tarjeta de valor almacenado 5 que verifica la firma, se carga con el valor de carga, y también genera un mensaje de realización satisfactoria de la carga, una segunda firma de tarjeta de valor almacenado (denominado S3), y un código de resultado que indica el éxito o fallo de la carga. En una realización preferida de la invención, esta firma está en forma encriptada para evitar la falsificación.

En el paso 882, la tarjeta 5 envía de nuevo un mensaje de realización satisfactoria de la carga conteniendo la firma de la tarjeta (S3) y el código de resultado al terminal de cliente 204. A continuación, en el paso 883 el terminal de cliente 204 empaqueta el mensaje de realización satisfactoria de la carga junto con la firma de la tarjeta y los envía de nuevo al servidor de carga 862. En el paso 884 el servidor de carga recibe el mensaje entrante. El servidor de carga procesa entonces el mensaje en sus componentes y dirige los componentes al módulo de seguridad. A continuación, en el paso 885 el módulo de seguridad puede procesar esta respuesta del terminal del cliente y verificar la firma de tarjeta de valor almacenado recibida (S3).

Dado que el módulo de seguridad contiene las claves y algoritmos necesarios para calcular firmas de tarjetas de valor almacenado, el módulo de seguridad es capaz de validar que una firma de tarjeta de valor almacenado recibida es de hecho válida comparando la firma de tarjeta de valor almacenado recibida con un valor esperado generado. Una comparación exitosa indica que un mensaje de realización satisfactoria de la carga recibida de la tarjeta de valor almacenado es de hecho un mensaje exitoso válido y que la tarjeta de valor almacenado ha sido cargada. Suponiendo que la transacción sea válida, en el paso 886 el módulo de seguridad envía de nuevo un mensaje de “confirmación” al servidor de carga.

Es posible que la tarjeta de valor almacenado no haya sido cargada en la cantidad apropiada, que la tarjeta no sea válida, que un usuario sea fraudulento u otra discrepancia. Por ejemplo, es posible que un usuario haya falsificado la tarjeta para que parezca que no se ha producido carga cuando, de hecho, se ha producido una carga. En esta situación, el procesado en el paso 882 y siguientes es ligeramente diferente. Por ejemplo, en lugar de generar un mensaje de

"carga exitosa", la tarjeta puede generar un código de "resultado negativo", indicando potencialmente que la tarjeta no se ha cargado. El procesado de esta situación se produciría entonces como sigue.

En el paso 882, la tarjeta 5 envía un mensaje de carga conteniendo el código de resultado y la firma de tarjeta de valor almacenado S3 de nuevo al terminal de cliente 204. El terminal de cliente 204 reconoce un código de resultado negativo, e invoca manipulación de resultado negativo. El terminal de cliente 204 interactúa con la tarjeta 5 y genera una nueva petición de carga de valor cero usando elementos de la petición original, junto con una nueva firma de tarjeta S1.

El código de resultado negativo, junto con las firmas S3 y nueva S1, y la petición de carga de valor cero se pasan al servidor de carga para análisis. El servidor de carga determina si el contador de transacciones en la carga de valor cero es igual al contador de transacciones en la petición anterior, verificando al mismo tiempo otra información pertinente tal como fecha y hora, número de tarjeta, y código de divisa y exponente. Si los contadores de transacciones son los mismos, entonces es posible que se haya recibido un resultado negativo válido, pero deberá ser verificado porque el cliente no es de confianza. Si los contadores son iguales, el servidor de carga mantendrá la original S3 y generará una nueva petición de carga al módulo de seguridad usando valores de elementos de datos que cabría esperar si la transacción original hubiese fallado. La nueva petición de carga junto con la nueva S1 es enviada al módulo de seguridad. El módulo de seguridad compara entonces la S1 original (de la petición de carga original) con la nueva S1. Si S1 es válida, entonces el resultado negativo original es verdadero y el módulo de seguridad genera una firma para confirmar al servidor de carga que no hubo carga. El resultado negativo original de la tarjeta es enviado entonces al módulo de seguridad para completar la transacción original. El procesado continuaría, pero no se adeudaría una cuenta de usuario, y no habría que hacer liquidación porque la tarjeta no se cargó, de hecho. Si S1 no es válido, la respuesta negativa no es verdadera y entonces el código de resultado en la petición original se cambia para reflejar una carga exitosa y se pasa al módulo de seguridad. El procesado continúa entonces reflejando que se ha producido una carga.

Por otra parte, si los contadores de transacciones no son los mismos, entonces todavía es posible que se haya recibido un resultado negativo válido, pero se deberá verificar porque el cliente no es de confianza. En primer lugar, el servidor de carga disminuye el contador de transacciones en la nueva petición de carga para que concuerde con la original. La petición junto con la nueva S1 es pasada al módulo de seguridad. El módulo de seguridad calcula su propia nueva S1 en base a la nueva petición de carga modificada. Si no hay concordancia, significa que el resultado negativo era erróneo y que la tarjeta se había cargado. El procesado continúa para reflejar una tarjeta cargada. Si hay concordancia, significa que el resultado negativo era correcto y que el contador de transacciones se había incrementado por accidente. La cuenta de usuario no es adeudada, y no tiene lugar liquidación.

Volviendo ahora al procesado adicional, en el paso 887 el servidor de carga registra la respuesta recibida del módulo de seguridad y actualiza su base de datos con el identificador de transacción, el identificador de banco, el valor de carga, etc. En general, toda la información que pasa a través del servidor de carga puede ser añadida a su base de datos. A continuación, en el paso 890 el servidor de carga crea un mensaje de confirmación incluyendo el identificador de transacción y envía este mensaje al terminal de cliente en forma encriptada. Enviando este mensaje de confirmación en forma encriptada, el mensaje de confirmación puede ser enviado al servidor de banco por medio del terminal de cliente sin temor a manipulación. Dado que el mensaje de confirmación está encriptado, sería difícil que el terminal de cliente u otra entidad falsificase un mensaje de confirmación e indujese al servidor de banco a pensar que tubo lugar una carga válida.

En el paso 891 el terminal de cliente envía el mensaje de confirmación al servidor de banco en la dirección URL previamente recibida del servidor de banco. El terminal de cliente también puede enviar un mensaje al usuario informando de que la carga ha finalizado: el terminal de cliente también registra confirmación de la carga. En el paso 892 el servidor de banco registra el mensaje de confirmación. El servidor de banco reclama una rutina para desencriptar el mensaje de confirmación. Si el mensaje de confirmación desencriptado es aceptable, el servidor de banco determina que se ha producido una carga exitosa. El mensaje de confirmación proporciona certeza al banco de que en la tarjeta del usuario se cargó, de hecho, un valor particular y evita el fraude. Por ejemplo, un usuario fraudulento que intente reclamar que su cuenta bancaria fue adeudada y que su tarjeta no se cargó (y así deberá recibir dinero fraudulento del banco) quedaría con un palmo de narices porque el mensaje de confirmación demuestra que la tarjeta del usuario se cargó de hecho. Alternativamente, el mensaje de "confirmación" puede indicar que no se produjo carga, en cuyo caso la cuenta no sería debitada, y no se produciría liquidación.

En este punto se ha producido una carga exitosa de la tarjeta del usuario (suponiendo que todo vaya bien). Por ejemplo, si el usuario había pedido $100, dicha cantidad ha sido adeudada en la cuenta de usuario en el banco, y se han cargado $100 en la tarjeta del usuario de valor almacenado. Preferiblemente, en este punto la cantidad cargada (en este ejemplo $100) es transferida desde el banco al emisor de tarjetas de valor almacenado preferiblemente a través de una red existente. Los $100 son transferidos de modo que el emisor de tarjetas pueda gestionar el dinero en tránsito en estos fondos no gastados hasta que el usuario gaste los $100. Una vez gastados los $100 (o una porción más pequeña) en un comercio, el emisor de tarjetas es capaz entonces de liquidar la transacción con el comerciante usando cualquier sistema de compensación y administración adecuado. En realización alternativa, el banco puede retener los $100 y liquidar directamente con el comerciante. En otra realización, el banco y el emisor de tarjetas son la misma institución financiera, y los $100 se pueden traspasar entre partes de la organización o permanecen en su lugar.

Volviendo ahora a una explicación más detallada del paso 879, la figura 5D describe una técnica para procesar un mensaje de petición de carga en unión con un módulo de seguridad. Una vez que el mensaje de petición de carga es recibido por el servidor de carga, el servidor de carga analiza los elementos apropiados y pasa una petición al módulo de seguridad como se explicará más adelante. Alternativamente, el servidor de carga puede crear un mensaje de red y pasar la petición a un servidor de autenticación remoto. O un terminal inteligente podría analizar el mensaje y pasar respuestas al módulo de seguridad.

En el paso 895 el servidor de carga edita la petición de carga para comprobar la corrección sintáctica y registra la petición recibida. En el paso 896 el servidor de carga crea un mensaje de petición de carga. En el paso 897 el servidor de carga pasa la petición de carga al módulo de seguridad para emular una tarjeta de valor almacenado que interactúa con el módulo de seguridad. El servidor de carga se comporta como si una tarjeta de valor almacenado interactuase realmente en un CA (por ejemplo) a través de una red con un ordenador central con un módulo de seguridad. De esta forma, la petición de carga que se origina en el terminal de cliente ha sido enviada en forma preempaquetada por Internet emulando una interacción tradicional entre la tarjeta de valor almacenado en un CA.

En el paso 898, el módulo de seguridad verifica la firma de tarjeta de valor almacenado recibida (S1) para evitar el fraude. El módulo de seguridad genera su firma de módulo de seguridad (denominada S2) y la orden de carga. La firma S2 confirmará al terminal de cliente y la tarjeta de valor almacenado que el módulo de seguridad central es auténtico y pertenece al emisor de la tarjeta de valor almacenado. Adicionalmente, S2 protege contra un usuario que intente realizar una carga falsificada, claves fuera de sincronismo, una tarjeta falsa, una tarjeta caducada, etc. El módulo de seguridad envía entonces la firma y orden de carga al servidor de carga como se ha indicado en el paso 899. En este punto, el paso 879 termina y el control vuelve al paso 880.

En otra realización de la técnica de carga, un consumidor puede desear acceder a alguno de varios servidores Web para cargar kilómetros gratuitos, puntos de premio, etc, que ha acumulado. Una técnica para autenticación y redención de tales "puntos" se describe anteriormente. En la realización de carga, un consumidor ha acumulado puntos a través de alguno de varios programas con líneas aéreas, restaurantes, compañías de alquiler de coches, hoteles, bancos, emisores de tarjetas de crédito o débito, compañías de teléfono u otros medios de comunicación, etc. Estos puntos son almacenados por la compañía aérea concreta, etc, que los ha concedido. El consumidor desea cargar estos puntos en su tarjeta de valor almacenado para redimirlos en otro lugar, recibiendo así billetes de compañías aéreas, vales de comidas, coche de alquiler, estancias en hoteles, premios, recompensas, descuentos u otros beneficios. Accediendo a un servidor de Internet asociado con el programa particular, el consumidor es capaz de cargar su tarjeta de valor almacenado en cualquiera de las realizaciones aquí descritas para recibir los beneficios del programa, en gran parte de la misma forma que se carga dinero.

La figura 6 ilustra un sistema informático 900 adecuado para implementar una realización de la presente invención. El sistema informático 900 incluye cualquier número de procesadores 902 (también denominados unidades centrales de proceso o CPUs) que están acoplados a dispositivos de almacenamiento incluyendo almacenamiento primario 906 (tal como una memoria de acceso aleatorio, o RAM) y almacenamiento primario 904 (tal como una memoria de lectura solamente o ROM). Como es bien conocido en la técnica, el almacenamiento primario 904 actúa para transferir datos e instrucciones unidireccionalmente a la CPU y el almacenamiento primario 906 se usa típicamente para transferir datos e instrucciones de manera bidireccional. Estos dos dispositivos de almacenamiento primario pueden incluir cualquier medio adecuado de los medios legibles por ordenador descritos más adelante. Un dispositivo de almacenamiento masivo 908 también está acoplado bidireccionalmente a la CPU 902 y proporciona capacidad adicional de almacenamiento de datos y también puede incluir alguno de los medios legibles por ordenador descritos más adelante. El dispositivo de almacenamiento masivo 908 puede ser usado para almacenar programas, datos y análogos y es típicamente un medio de almacenamiento secundario (tal como un disco duro) más pequeño que el almacenamiento primario. Se apreciará que la información retenida dentro del dispositivo de almacenamiento masivo 908 se puede incorporar, en casos apropiados, de forma estándar como parte del almacenamiento primario 906 como memoria virtual. Un dispositivo de almacenamiento masivo específico, tal como un CD-ROM 914, pasa datos unidireccionalmente a la CPU.

La CPU 902 también está acoplada a una interface 910 que incluye uno o más dispositivos de entrada/salida tales como monitores vídeo, trackballs, ratones, teclados, micrófonos, pantallas táctiles, lectores de tarjetas de transductor, lectores de cinta magnética o de papel, tabletas, plumas, dispositivos de reconocimiento de voz y escritura, lectores biométricos, u otros ordenadores. La CPU 902 puede estar acoplada opcionalmente a otro ordenador o red de telecomunicaciones usando una conexión de red como se representa generalmente en 912. Con dicha conexión de red, se contempla que la CPU pueda recibir información de la red, o pueda enviar información a la red en el transcurso de la realización de los pasos del método antes descritos. Además, las realizaciones del método de la presente invención se pueden ejecutar únicamente en CPU 902 o se pueden ejecutar por una conexión de red tal como Internet en unión con una CPU remota que comparta una porción del procesado.

Además, las realizaciones de la presente invención también se refieren a productos de almacenamiento en ordenador con un medio legible por ordenador que tienen un código de programa para realizar varias operaciones implementadas en ordenador. Los medios y el código de programa pueden ser los diseñados y construidos especialmente a los efectos de la presente invención, o pueden ser del tipo conocido y disponible para las personas con conocimiento en la técnica de software de ordenador. Los ejemplos de medios legibles por ordenador incluyen, aunque sin limitación: medios magnéticos como discos duros, discos flexibles, y cinta magnética; medios ópticos tales como discos CD-ROM; medios magneto-ópticos tales como discos flópticos; y dispositivos de hardware que están especialmente

configurados para almacenar y ejecutar códigos de programa, tales como circuitos integrados específicos de aplicación (ASICs), dispositivos lógicos programables (PLDs) y dispositivos ROM y RAM. Los ejemplos de códigos de programa incluyen código máquina, tal como el producido por un compilador, y archivos conteniendo código de nivel más alto que son ejecutados por un ordenador usando un intérprete.

Aunque la invención anterior se ha descrito con cierto detalle para claridad de la comprensión, será evidente que se puede poner en práctica algunos cambios y modificaciones. Por ejemplo, cualquier tarjeta de valor almacenado adecuada capaz de cargar, almacenar y decrementar valor a la orden puede ser usada en la presente invención. Además, se puede usar cualquier red capaz de realizar funcionalidad de enrutamiento entre un terminal de cliente y un servidor de carga y banco. Además, el módulo de seguridad puede ser un módulo físicamente separado, una tarjeta situada en un terminal unido a un servidor de carga, o su funcionalidad puede estar incorporada directamente en un servidor de carga en hardware o software. Y aunque el terminal de cliente puede ser usado para enrutar mensajes entre el servidor de banco y el servidor de carga, estos dos servidores también pueden comunicar directamente entre sí, e incluso pueden ser el mismo ordenador. Los mensajes específicos representados pasando entre los ordenadores son ejemplares, y se puede utilizar otros tipos de mensajes. Se muestra una petición de carga especificada, pero también se puede cargar otra información en una tarjeta de valor almacenado usando emulación de un módulo de seguridad y entonces enviar empaquetada como un mensaje al módulo de seguridad por una red. Además de valor monetario, se puede cargar otros tipos de valor tal como dinero electrónico en efectivo, cheques, premiso, puntos de fidelidad, beneficios, etc, en una tarjeta, y se ha previsto que el término "valor" cubra ampliamente todos estos varios tipos. Se puede usar cualquier tipo de encriptado adecuado para encriptar mensajes que pasan entre los ordenadores.

REIVINDICACIONES

1. Un sistema de carga para cargar valor por una red sobre una tarjeta de valor almacenado (5), incluyendo dicho sistema de carga:

un servidor de banco (860) bajo el control por una primera entidad y en comunicación con dicha red, estando dispuesto dicho servidor de banco (860) para debitar en una cuenta de usuario un valor indicado; y

un terminal de cliente (204) bajo el control por un consumidor y en comunicación con dicha red, incluyendo dicho terminal de cliente (204) un lector de tarjetas para comunicar con una tarjeta de valor almacenado (5) y un dispositivo de entrada para indicar un valor a debitar en dicha cuenta de usuario; donde, en la práctica, el terminal de cliente es efectivo para:

comunicar con la tarjeta de valor almacenado usando el lector de tarjetas;

recibir una indicación de un valor a debitar en la cuenta de usuario desde el dispositivo de entrada;

transmitir al servidor de banco (860) una petición de carga de la tarjeta de valor almacenado (5);

recibir de dicho servidor de banco (860) un valor de carga verificado;

caracterizado porque dicho sistema incluye un servidor de carga (862), distinto de dicho servidor de banco (860), bajo el control por una segunda entidad y en comunicación con dicha red (202), incluyendo dicho servidor de carga una interface para comunicar con un módulo de seguridad (864);

caracterizado además porque, en la práctica, el terminal de cliente es efectivo para:

enviar una petición de carga al servidor de carga (862), incluyendo la petición de carga una firma de tarjeta de valor almacenado;

recibir una orden de carga de dicho servidor de carga (862), incluyendo la orden de cargar una firma de módulo de seguridad;

pasar la orden de carga a la tarjeta de valor almacenado para verificación de la firma de módulo de seguridad y para cargar dicha tarjeta de valor almacenado (5) con dicho valor de carga;

recibir un mensaje de realización satisfactoria de la carga de dicha tarjeta de valor almacenado, incluyendo el mensaje de realización satisfactoria de la carga una segunda firma de tarjeta de valor almacenado;

enviar el mensaje de realización satisfactoria de la carga al servidor de carga;

recibir un mensaje de confirmación encriptado del servidor de carga; y,

enviar dicho mensaje de confirmación a dicho servidor de banco (860), por lo que dicho servidor de banco (860) tiene seguridad de que dicha carga se ha realizado satisfactoriamente.

2. Un sistema de carga según la reivindicación 1, donde dicha red (202) es Internet y dicho servidor de banco (860) incluye un sitio web de banco para aceptar una petición de carga.

3. Un sistema de carga según la reivindicación 1 o 2, donde dicho terminal de cliente (204) y dicho servidor de banco (860) están en posiciones separadas y comunican por dicha Internet.

4. Un sistema de carga según cualquier reivindicación precedente, incluyendo además:

un sistema de compensación y administración para reconciliar dicho débito de dicha cuenta de usuario con una compra usando dicha tarjeta de valor almacenado (5).

5. Un sistema de carga según cualquier reivindicación precedente, donde dicho terminal de cliente (204) incluye además un emulador de orden para emular órdenes del módulo de seguridad que son enviadas a dicha tarjeta de valor almacenado (5) y para agrupar respuestas a dichas órdenes del módulo de seguridad en un mensaje de petición de carga a enviar a dicho servidor de carga (862), y donde dicho servidor de carga (862) incluye un emulador de respuesta para emular respuestas de dicha tarjeta de valor almacenado (5) que son enviadas a dicho módulo de seguridad (864).

6. Un sistema de carga según cualquier reivindicación precedente, donde dicho módulo de seguridad (864) incluye un comparador para comparar una firma de tarjeta de valor almacenado recibida de dicha tarjeta de valor almacenado (5) con una firma esperada para confirmar una transacción.

7. Un sistema de carga según cualquier reivindicación precedente, donde dicho módulo de seguridad (864) está adaptado para verificar dicha firma de tarjeta de valor almacenado, generando por ello una firma de módulo de seguridad, y para enviar dicha firma de módulo de seguridad a dicho servidor de carga (862).

8. Un método implementado por ordenador de cargar una tarjeta de valor almacenado por una red, siendo realizado el método por un terminal de cliente, estando dicho terminal de cliente bajo el control por un consumidor, e incluyendo los pasos de:

comunicar con la tarjeta de valor almacenado usando un lector de tarjetas;

recibir una indicación de un valor a debitar en la cuenta de usuario de un dispositivo de entrada;

transmitir por una red (202) a un servidor de banco (860) una petición de carga de la tarjeta de valor almacenado (5), estando dicho servidor de banco bajo el control por una primera entidad;

recibir de dicho servidor de banco (860) un valor de carga verificado;

caracterizado porque el método incluye los pasos de

enviar una petición de carga a un servidor de carga (862) conectado a dicha red (202), incluyendo la petición de carga una firma de tarjeta de valor almacenado y siendo el servidor de carga distinto del servidor de banco e incluyendo una interface para comunicar con un módulo de seguridad (864), estando dicho servidor de carga bajo el control por una segunda entidad;

recibir una orden de carga de dicho servidor de carga (862), incluyendo la orden de cargar una firma de módulo de seguridad;

pasar la orden de carga a la tarjeta de valor almacenado para verificación de la firma de módulo de seguridad y para cargar dicha tarjeta de valor almacenado (5) con dicho valor de carga;

recibir un mensaje de realización satisfactoria de la carga de dicha tarjeta de valor almacenado, incluyendo el mensaje de realización satisfactoria de la carga una segunda firma de tarjeta de valor almacenado;

enviar el mensaje de realización satisfactoria de la carga a dicho servidor de carga;

recibir un mensaje de confirmación encriptado de dicho servidor de carga; y,

enviar dicho mensaje de confirmación a dicho servidor de banco (860), por lo que dicho servidor de banco (860) tiene la seguridad de que dicha carga ha sido realizada satisfactoriamente.

9. Un método según la reivindicación 8, donde dicha red (202) es Internet en la que tienen lugar dichos pasos expuestos de dicho método, donde dicho servidor de banco (860) incluye un sitio web de banco para aceptar una petición de carga, y donde dicho terminal de cliente (204) y dicho servidor de banco (860) están en posiciones separadas.

10. Un método según la reivindicación 8 o 9, incluyendo además los pasos de:

emular órdenes del módulo de seguridad que son enviadas a dicha tarjeta de valor almacenado (5) asociada con dicho terminal de cliente (204); y

agrupar respuestas a dichas órdenes del módulo de seguridad a dicha petición de carga de modo que dichas respuestas puedan ser enviadas como un grupo a dicho servidor de carga (862) para reducir el tráfico de red entre dicho servidor de carga (862) y dicho terminal de cliente (204).

11. Un método según cualquiera de las reivindicaciones 8 a 10, donde dicha información de confirmación incluye un mensaje de confirmación encriptado ilegible por dicho terminal de cliente (204), incluyendo dicho método además:

recibir dicho mensaje de confirmación encriptado de dicho servidor de carga (862).

12. Un método según cualquiera de las reivindicaciones 8 a 11, incluyendo además verificar, en el módulo de seguridad (864), dicha firma de tarjeta de valor almacenado, generando por ello una firma de módulo de seguridad, y enviar dicha firma de módulo de seguridad a dicho servidor de carga (862).

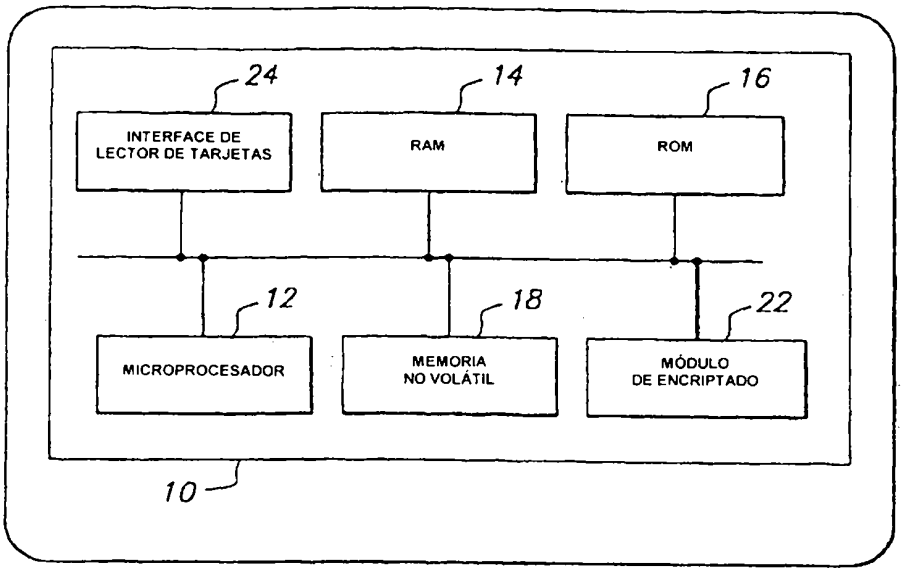


FIG. 1 TÉCNICA ANTERIOR

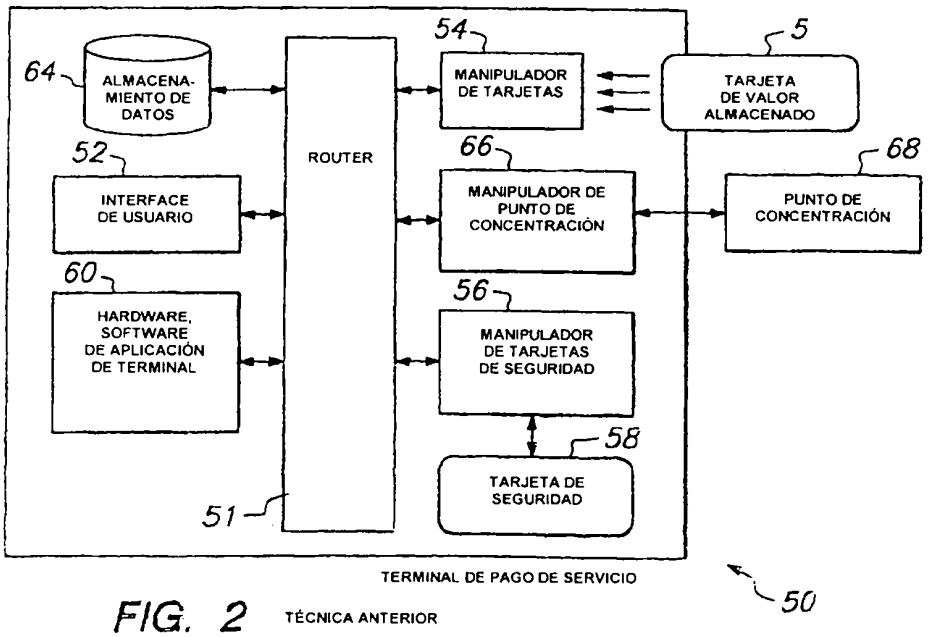


FIG. 2 TÉCNICA ANTERIOR

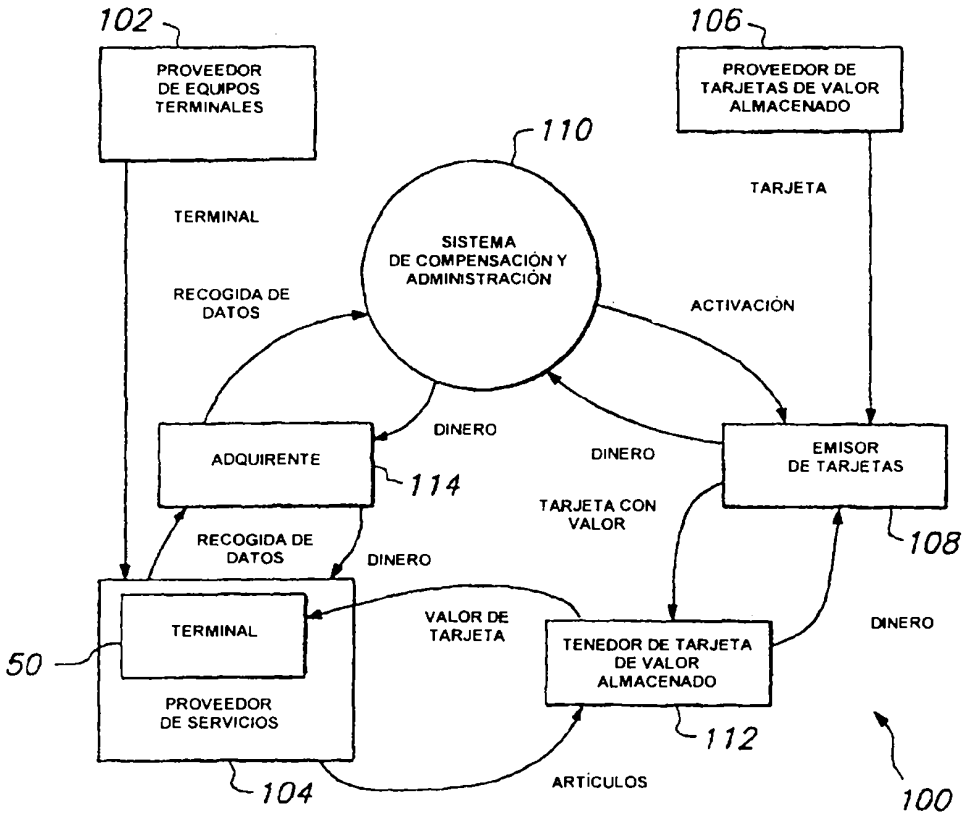


FIG. 3 TÉCNICA ANTERIOR

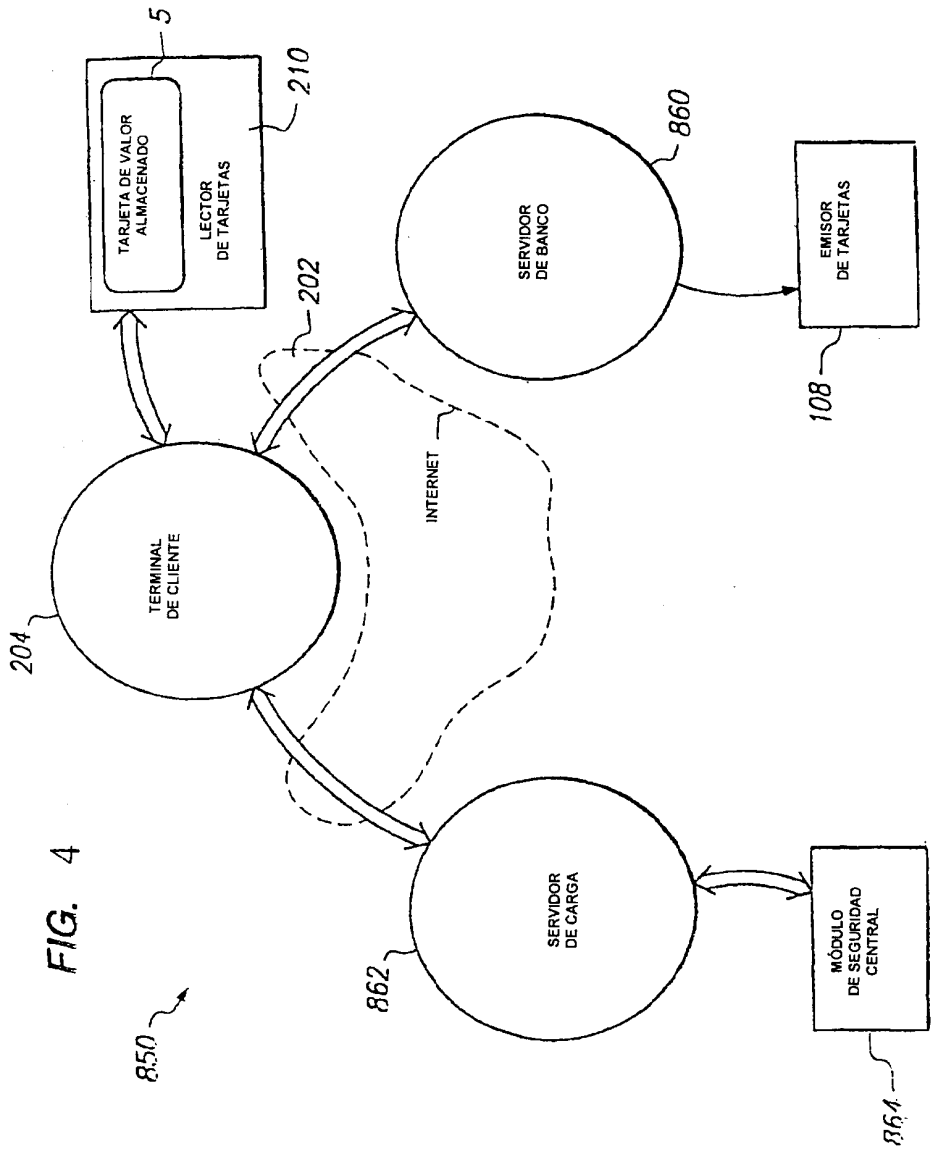

5
TARJETA DE VALOR ALMACENADO
LECTOR DE TARJETAS
210
202
SERVIDOR DE BANCO
860
EMISOR DE TARJETAS
108
INTERNET
TERMINAL DE CLIENTE
204
SERVIDOR DE CARGA
862
MÓDULO DE SEGURIDAD CENTRAL
864
850

FIG. 4

FIG. 5A

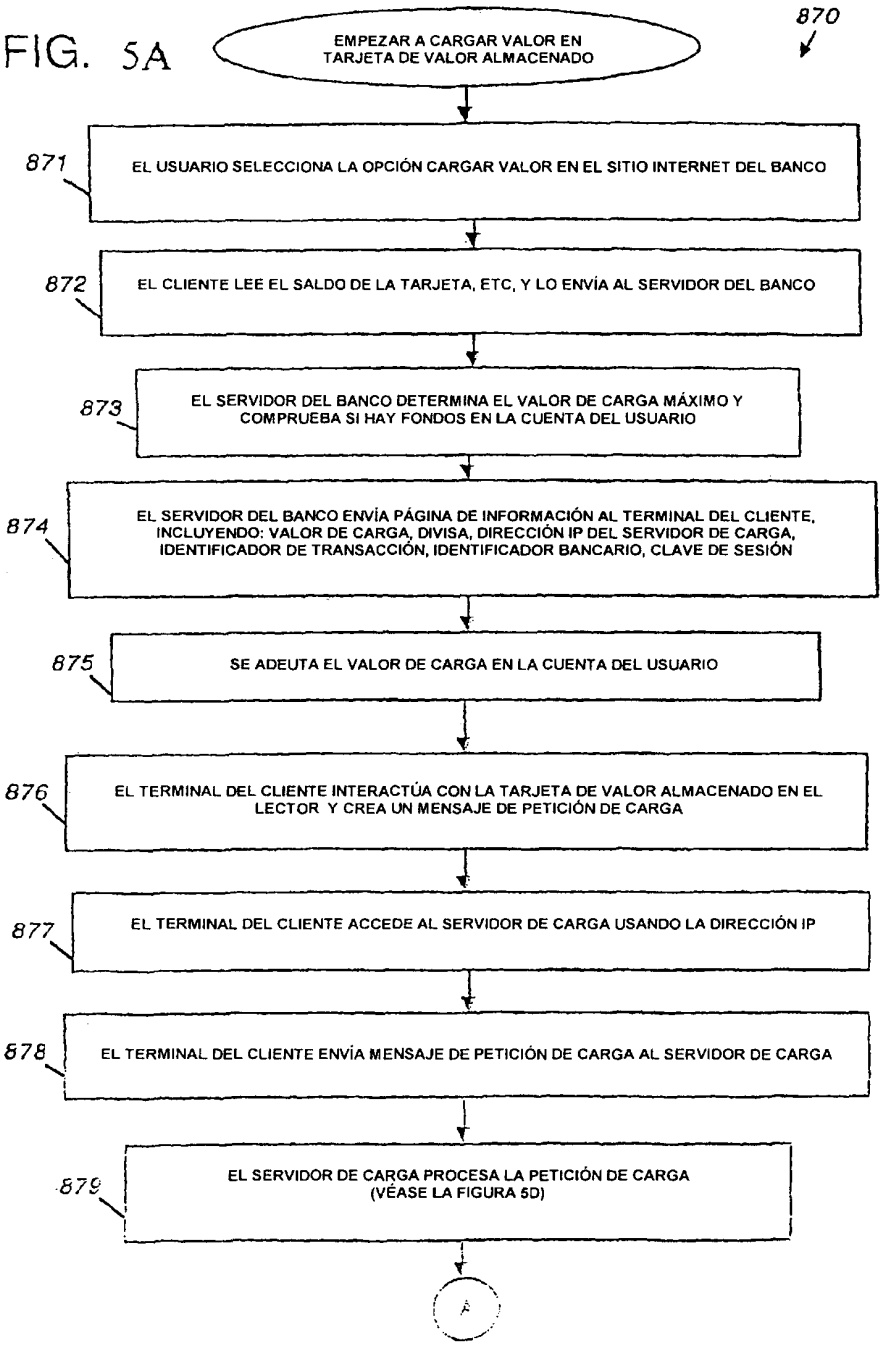

870
EMPEZAR A CARGAR VALOR EN TARJETA DE VALOR ALMACENADO
871
EL USUARIO SELECCIONA LA OPCIÓN CARGAR VALOR EN EL SITIO INTERNET DEL BANCO
872
EL CLIENTE LEE EL SALDO DE LA TARJETA, ETC, Y LO ENVÍA AL SERVIDOR DEL BANCO
873
EL SERVIDOR DEL BANCO DETERMINA EL VALOR DE CARGA MÁXIMO Y COMPRUEBA SI HAY FONDOS EN LA CUENTA DEL USUARIO
874
EL SERVIDOR DEL BANCO ENVÍA PÁGINA DE INFORMACIÓN AL TERMINAL DEL CLIENTE, INCLUYENDO: VALOR DE CARGA, DIVISA, DIRECCIÓN IP DEL SERVIDOR DE CARGA, IDENTIFICADOR DE TRANSACCIÓN, IDENTIFICADOR BANCARIO, CLAVE DE SESIÓN
875
SE ADEUTA EL VALOR DE CARGA EN LA CUENTA DEL USUARIO
876
EL TERMINAL DEL CLIENTE INTERACTÚA CON LA TARJETA DE VALOR ALMACENADO EN EL LECTOR Y CREA UN MENSAJE DE PETICIÓN DE CARGA
877
EL TERMINAL DEL CLIENTE ACCEDE AL SERVIDOR DE CARGA USANDO LA DIRECCIÓN IP
878
EL TERMINAL DEL CLIENTE ENVÍA MENSAJE DE PETICIÓN DE CARGA AL SERVIDOR DE CARGA
879
EL SERVIDOR DE CARGA PROCESA LA PETICIÓN DE CARGA (VÉASE LA FIGURA 5D)
A

FIG. 5B

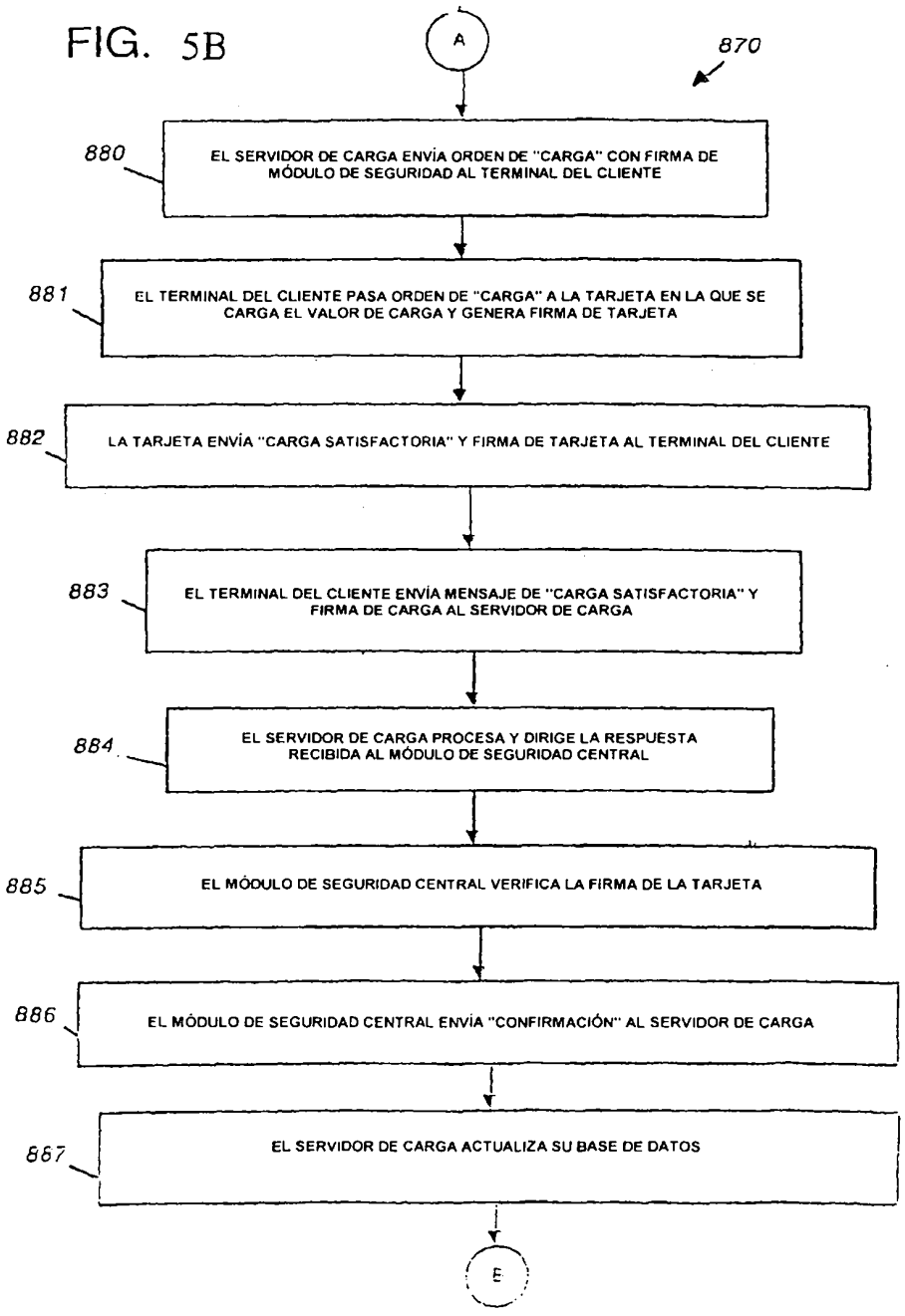
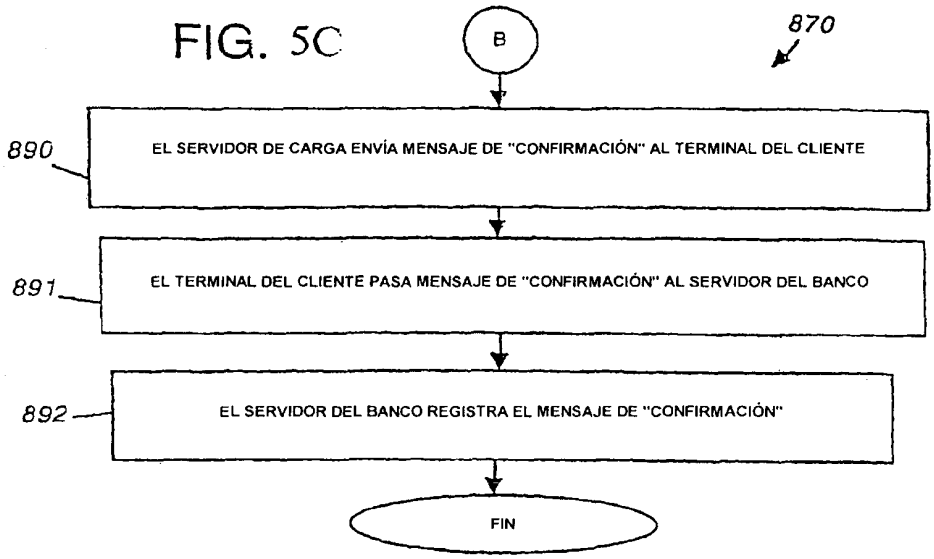

A
870
880
EL SERVIDOR DE CARGA ENVÍA ORDEN DE "CARGA" CON FIRMA DE MÓDULO DE SEGURIDAD AL TERMINAL DEL CLIENTE
881
EL TERMINAL DEL CLIENTE PASA ORDEN DE "CARGA" A LA TARJETA EN LA QUE SE CARGA EL VALOR DE CARGA Y GENERA FIRMA DE TARJETA
882
LA TARJETA ENVÍA "CARGA SATISFACTORIA" Y FIRMA DE TARJETA AL TERMINAL DEL CLIENTE
883
EL TERMINAL DEL CLIENTE ENVÍA MENSAJE DE "CARGA SATISFACTORIA" Y FIRMA DE CARGA AL SERVIDOR DE CARGA
884
EL SERVIDOR DE CARGA PROCESA Y DIRIGE LA RESPUESTA RECIBIDA AL MÓDULO DE SEGURIDAD CENTRAL
885
EL MÓDULO DE SEGURIDAD CENTRAL VERIFICA LA FIRMA DE LA TARJETA
886
EL MÓDULO DE SEGURIDAD CENTRAL ENVÍA "CONFIRMACIÓN" AL SERVIDOR DE CARGA
887
EL SERVIDOR DE CARGA ACTUALIZA SU BASE DE DATOS
E

FIG. 5C


B
870
890
EL SERVIDOR DE CARGA ENVÍA MENSAJE DE "CONFIRMACIÓN" AL TERMINAL DEL CLIENTE
891
EL TERMINAL DEL CLIENTE PASA MENSAJE DE "CONFIRMACIÓN" AL SERVIDOR DEL BANCO
892
EL SERVIDOR DEL BANCO REGISTRA EL MENSAJE DE "CONFIRMACIÓN"
FIN

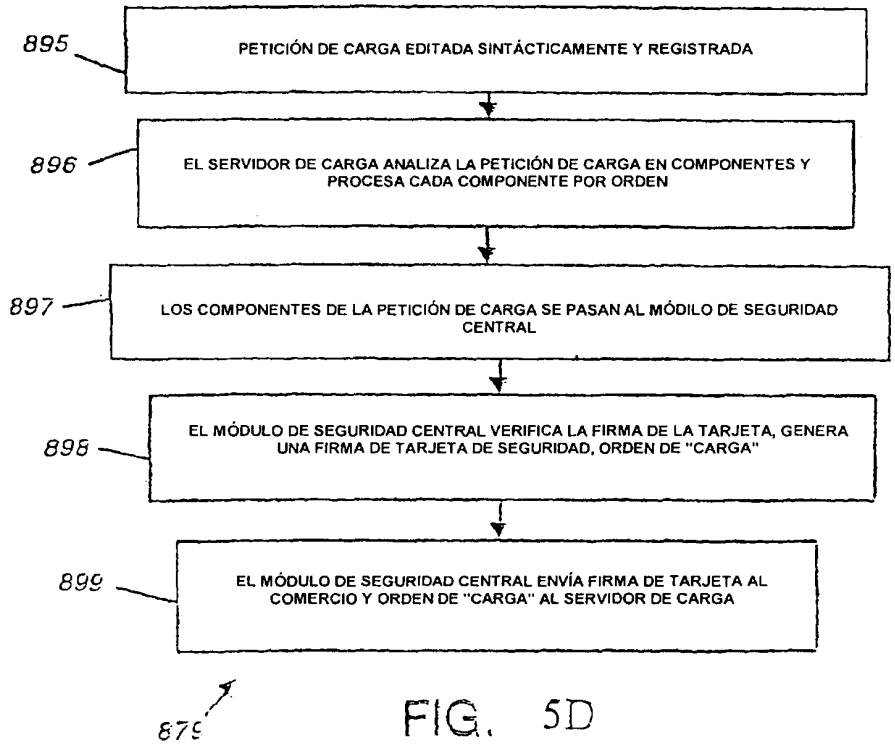

895
PETICIÓN DE CARGA EDITADA SINTÁCTICAMENTE Y REGISTRADA
896
EL SERVIDOR DE CARGA ANALIZA LA PETICIÓN DE CARGA EN COMPONENTES Y PROCESA CADA COMPONENTE POR ORDEN
897
LOS COMPONENTES DE LA PETICIÓN DE CARGA SE PASAN AL MÓDILO DE SEGURIDAD CENTRAL
898
EL MÓDULO DE SEGURIDAD CENTRAL VERIFICA LA FIRMA DE LA TARJETA, GENERA UNA FIRMA DE TARJETA DE SEGURIDAD, ORDEN DE "CARGA"
899
EL MÓDULO DE SEGURIDAD CENTRAL ENVÍA FIRMA DE TARJETA AL COMERCIO Y ORDEN DE "CARGA" AL SERVIDOR DE CARGA
879

FIG. 5D

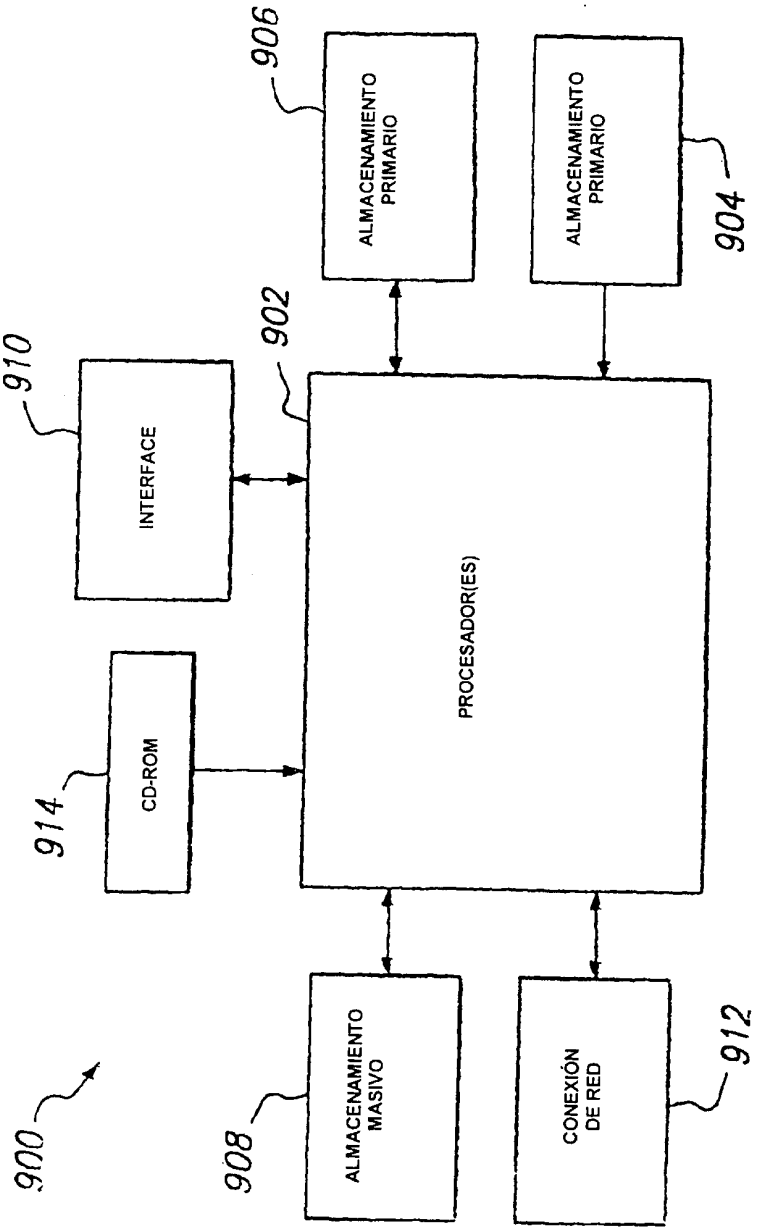

906
ALMACENAMIENTO PRIMARIO
ALMACENAMIENTO PRIMARIO
904
902
910
INTERFACE
PROCESADOR(ES)
914
CD-ROM
900
908
ALMACENAMIENTO MASIVO
CONEXIÓN DE RED
912

FIG. 6