(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 823 592**

(51) Int. CI.:

G06F 12/14 (2006.01)
G06Q 10/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.11.2004 PCT/AU2004/001663**

(87) Fecha y número de publicación internacional: **09.06.2005 WO05052801**

(96) Fecha de presentación y número de la solicitud europea: **26.11.2004 E 04797105 (6)**

(97) Fecha y número de publicación de la concesión europea: **30.09.2020 EP 1687725**

(54) Título: **Sistema de pago seguro**

(30) Prioridad:

26.11.2003 AU 2003906527

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.05.2021

(73) Titular/es:

VEROGUARD SYSTEMS PTY LIMITED (100.0%)
17 McNaughton Road
Clayton, Victoria 3168, AU

(72) Inventor/es:

ELBAUM, HECTOR DANIEL;
JAMIESON, ANDREW y
MCGREGOR, DAVID

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Sistema de pago seguro

Campo de la invención

La invención se refiere a la autenticación de usuarios con el fin de realizar, por ejemplo, transacciones financieras, y más específicamente a un sistema, método y aparato mediante el cual se pueden asegurar las transacciones entre dos partes físicamente separadas conectadas a través de una red pública de datos tal como internet.

Antecedentes de la invención

Los sistemas para asegurar los pagos a través de internet se han mejorado desde sus inicios a mediados de la década de 1990 hasta el punto en que el fraude directamente relacionado con tarjetas de crédito ha alcanzado la paridad con el de otras transacciones de titular de tarjeta no presente (CNP). Sin embargo, la falta de comprensión de estos métodos combinada con un enfoque de los medios dispar en los pocos casos de fraude que ocurren ha dado como resultado un nivel constantemente bajo de confianza del consumidor.

Los intentos de aumentar la percepción de seguridad del cliente, garantizando el reembolso de las transacciones CNP impugnadas, simplemente han exacerbado el problema desde la otra dirección. Muchos de los comerciantes en línea más pequeños han retirado la aceptación de transacciones con tarjeta de crédito porque no pueden respaldar el impago repetido de bienes que se asocia con los clientes que impugnan las transacciones, ya sea de manera genuina o fraudulenta.

Los problemas que existen son sistemáticos de los métodos y convenciones mediante los cuales se procesan los pagos a través de internet. El cliente debe proporcionar al comerciante todos los detalles relevantes de su tarjeta de pago, tales como el número de cuenta principal (PAN), la fecha de vencimiento, etc., lo que permite al comerciante cargar la tarifa a esta tarjeta. La mecánica de este pago implica que el comerciante envíe una solicitud de pago que incluye los detalles de pago del cliente a la institución financiera que tiene su cuenta bancaria, o a un proveedor de servicios financieros que facilita la conexión entre los comerciantes y sus instituciones financieras. La institución financiera del comerciante, conocida como el banco adquirente, envía un mensaje de autorización a la institución financiera que emitió la tarjeta de pago, cuyos detalles fueron proporcionados por el cliente. Este mensaje se envía a través de una red interbancaria, generalmente mantenida por un tercero, tal como una gran autoridad de tarjetas de pago, tal como MasterCard, VISA u otro proveedor. La institución financiera que emitió la tarjeta de pago se identifica mediante los primeros 6 dígitos del número de la tarjeta de pago, conocido como número de emisor del banco (BIN).

Sin embargo, no hay forma de garantizar que los datos proporcionados al comerciante por el cliente pertenezcan realmente a ese cliente y no se hayan obtenido de forma fraudulenta. Es esta incapacidad para confirmar la presencia del propietario real de la tarjeta lo que conduce a un porcentaje tan alto de 'rechazos de cargo', o transacciones en las que el cliente niega participar en la transacción. Tradicionalmente, si el cliente cuestiona una transacción y el comerciante no puede presentar prueba de su autorización, tal como una firma, el dinero se reembolsa al cliente y el comerciante debe cubrir la pérdida.

Los clientes también están privados del derecho a utilizar las opciones de pago por internet debido al temor al robo de los detalles de su tarjeta. Este robo puede ocurrir durante la transacción en sí, o puede ocurrir después del hecho debido a una inseguridad de la tienda web del comerciante. Muchos comerciantes mantienen una base de datos de detalles de tarjetas de clientes, aparentemente para agilizar las compras repetidas para el consumidor, y estas bases de datos se convierten en objetivos atractivos para la fraternidad criminal. De hecho, es esta persistencia de la información confidencial del cliente lo que más asusta a muchos consumidores. Aunque las transacciones que resultan de tal 'tarjeta robada' pueden ser 'rechazadas por cargo' al comerciante, el inconveniente de hacerlo, junto con la carga de obtener una nueva tarjeta, es suficiente para desanimar a muchos consumidores.

Los sistemas y métodos tales como los divulgados en los documentos US6,098,053, US2002/0123972A1, US2003/0140004A1, US2002/0077978A1 y US2003/0154139A1 US6327578B1 han intentado proporcionar una solución a este problema integrando la funcionalidad EFTPOS tradicional en el ámbito de los pagos por internet. En estos documentos se enseñan métodos que implican el uso de un dispositivo EFTPOS que el cliente sostiene y mantiene con el fin de realizar un pago seguro al comerciante sin temor a fraude. Como los detalles de pago del cliente no se transmiten al comerciante, o se pasan al comerciante solo en forma cifrada, no hay riesgo de que se vean comprometidos, en cualquier etapa. Sin embargo, estos sistemas requieren cambios fundamentales en la interacción entre el cliente, el comerciante y las instituciones bancarias. Se requiere que el comerciante cambie sus sistemas de compra de 'tienda web', y la relación entre el comerciante y su adquiriente se elimina de la transacción. Sin embargo, sin el apoyo de los comerciantes, no hay ningún incentivo para que el cliente participe en el sistema; de hecho, sin el apoyo del comerciante, no hay un sistema en el que el cliente pueda participar. Por el contrario, no hay ningún incentivo para que el comerciante modifique sus sistemas de pago sin una gran base de clientes capaces de utilizar estos cambios. Por lo tanto, cualquier sistema revolucionario de este tipo enfrenta un desafío fundamental para ganar impulso en un mercado dominado por un paradigma alternativo, y este problema ha impedido la adopción de estos sistemas.

Alternativamente, otros sistemas brindan al cliente un PAN de un solo uso, que solo se puede usar para una transacción. Esto elimina el riesgo asociado con el robo de los datos del cliente, ya que no son útiles fuera del contexto de una sola transacción que el cliente ya ha realizado. Este sistema tiene méritos, pero se puede considerar que protege solo al cliente en la transacción, sin brindar ningún beneficio para el comerciante. Como se indicó anteriormente, el alto nivel de 'rechazos de cargo' generado a través del comercio por internet es un problema clave para aumentar los ingresos en este campo, y cualquier sistema que no brinde beneficios al comerciante enfrenta una alta barrera de entrada al mercado. Estos sistemas también adolecen del requisito de que el emisor de la tarjeta debe alterar sus sistemas de servidor para identificar e interpretar correctamente el PAN sustituido como perteneciente al cliente que inició la transacción. Las alteraciones de estos sistemas bancarios son costosas y requieren mucho tiempo debido a los requisitos de alta calidad y certificación que deben cumplirse. Además, estos sistemas son incompatibles con algunos software de compra de comerciantes (tales como los sistemas de "un clic") donde se espera que el cliente utilice un solo número de tarjeta para muchas transacciones. Finalmente, el cliente está limitado a usar solo tarjetas que brinden esta facilidad PAN de reemplazo para cualquier transacción que realice en internet. Esto limita las opciones de compra y pago del consumidor, reduciendo así el atractivo del comercio por internet para él.

Un sistema similar se divulga en la solicitud de patente de E.U. no. 2003/0195842A1, sin embargo, el sistema descrito en el mismo está además limitado en su aplicación al requerir el uso de tarjetas de pago de valor almacenado por parte del cliente.

Otro método para asegurar las transacciones de internet se enseña en la solicitud de patente de E.U. no. US2003/0097343A1. Este sistema requiere que una parte intermediaria, conocida como centro de procesamiento, actúe como un conducto a través del cual se realiza la transacción. La seguridad del cliente se proporciona al reducir la exposición de los detalles de pago de los clientes a una única parte de confianza, en lugar de a una pluralidad de comerciantes. Sin embargo, este sistema también adolece del requisito de un cambio de paradigma en todo el sistema en el método mediante el cual se realizan los pagos por internet.

La patente de E.U. no. 5,809,143 enseña el uso de un teclado seguro para transacciones comerciales por internet. Este sistema proporciona una entrada segura de la información del titular de la tarjeta, tal como el número de cuenta y el PIN. Sin embargo, los mecanismos de interacción con el comerciante se alteran una vez más. Además, el requisito de un medio de comunicaciones secundario limita la aplicación de este sistema en el entorno actual.

En consecuencia, existe la necesidad de un sistema que pueda proporcionar beneficios a todas las partes involucradas (clientes, comerciantes e instituciones financieras) y que se pueda implementar y aplicar de inmediato sin afectar a ninguna otra parte que no sea el cliente que usa el sistema.

Por lo tanto, es un objeto de la presente invención proporcionar un método y sistema para autenticar información de identificación, tal como número de cuenta y PIN, proporcionado por un usuario de una red pública de datos, tal como internet, que mitiga los problemas de la técnica anterior ya mencionados.

Se incluye cualquier discusión de documentos, dispositivos, actos o conocimiento en esta especificación para explicar el contexto de la invención. No debe tomarse como una admisión de que cualquier material formaba parte de la base de la técnica anterior o del conocimiento general común en la técnica relevante en o antes de la fecha de prioridad de las reivindicaciones en este documento.

Resumen de la invención

En un aspecto, la presente invención proporciona un sistema para la autenticación por parte de una institución financiera emisora de tarjetas de información de identificación de un usuario titular de tarjeta de una red pública de datos, que incluye:

un dispositivo de entrada de datos segura conectado a la red pública de datos; y
un dispositivo de puerta de enlace conectado a la red pública de datos y a una red privada de datos utilizada para transmitir mensajes entre instituciones financieras;
en donde el dispositivo de entrada de datos segura incluye medios para que el usuario introduzca información de identificación de una tarjeta emitida por la institución financiera emisora de la tarjeta, y medios para transmitir la información de identificación de forma segura a través de la red pública de datos al dispositivo de puerta de enlace; y
en donde el dispositivo de puerta de enlace incluye medios para transmitir la información de identificación a la institución financiera emisora de la tarjeta y para recibir una respuesta de aprobación de la institución financiera emisora de la tarjeta a través de la red de datos privados;
por lo que la respuesta de aprobación proporciona autenticación de la información de identificación por parte de la institución financiera emisora de la tarjeta.

En consecuencia, el sistema permite que la información de identificación de un titular de tarjeta ubicado en un punto de compra remoto de cualquier punto de venta sea verificada por la institución financiera emisora de la tarjeta de manera segura a través de una red pública de datos.

Preferiblemente, la red pública de datos es internet. El dispositivo de entrada de datos segura puede conectarse a la red pública de datos a través del ordenador personal del usuario.

La red de datos privados puede ser una red interbancaria utilizada para la transferencia de datos de transacciones electrónicas. La red de datos privados se puede proporcionar a través de una red dedicada operada con el único propósito de realizar tales transacciones electrónicas. Alternativamente, la red de datos privada puede ser una red privada virtual proporcionada a través de una red de datos pública de servidor. La red de datos pública de servidor puede ser internet.

El dispositivo de entrada de datos segura incluye preferiblemente un lector de tarjetas para leer información relevante almacenada en la tarjeta del usuario. El lector de tarjetas puede leer tarjetas de tipo "tarjeta inteligente" ISO 7816 o tarjetas de tipo "banda magnética" ISO 7811, y preferiblemente puede leer ambos tipos de tarjetas.

Preferiblemente, el dispositivo de entrada de datos segura también incluye un teclado para permitir que el usuario introduzca datos en el sistema. Los datos ingresados por el usuario pueden incluir un número de identificación personal asociado con la tarjeta.

La información de identificación incluye preferiblemente uno o más de: el número de cuenta principal asociado con la tarjeta; la fecha de caducidad de la tarjeta; y el número de identificación personal del usuario asociado con la tarjeta. Ventajosamente, al permitir que el usuario proporcione esta información para la autenticación de manera segura en un punto de compra que puede estar alejado de cualquier punto de venta, el sistema puede confirmar la presencia del propietario real de la tarjeta en el punto de compra.

La información de identificación se puede transmitir usando un formato de mensaje de transacción estándar que cumpla con ISO 8583. Preferiblemente, el mensaje ISO 8583 usado es uno de: un mensaje de presentación financiera '0200'; y un mensaje de autorización '0104'.

El dispositivo de puerta de enlace incluye preferiblemente también medios para transmitir la respuesta de aprobación al dispositivo de entrada segura de datos. En una realización preferida, el dispositivo de entrada segura de datos incluye además medios para derivar de la respuesta de aprobación una prueba verificable de que la información de identificación del cliente ha sido autenticada por la institución financiera emisora de la tarjeta. La prueba puede ser un bloque de datos de autenticación, que consta de datos calculados de manera segura a partir de la aprobación enviada por el banco emisor de la tarjeta. El bloque de datos puede ser un cifrado completo o truncado del mensaje de aprobación derivado utilizando una clave de cifrado almacenada de forma segura dentro del dispositivo de entrada de datos segura.

Ventajosamente, el sistema permite así que el dispositivo de entrada segura de datos obtenga una prueba verificable de la presencia del propietario real de la tarjeta en el punto de compra que se puede utilizar en transacciones posteriores con otros dispositivos que tienen la capacidad de verificar la prueba.

En una realización particularmente preferida, el dispositivo de puerta de enlace también incluye medios para generar un número de tarjeta de reemplazo al recibir la respuesta de aprobación de la institución emisora de la tarjeta. El número de tarjeta de reemplazo puede transmitirse al dispositivo de entrada de datos segura a través de la red pública de datos. El número de tarjeta de reemplazo se puede utilizar en una transacción de pago posterior realizada a través de la red pública de datos. Ventajosamente, de acuerdo con la invención, los detalles reales de la tarjeta nunca se transmiten a través de la red de manera insegura, ni se proporcionan a un comerciante u otro operador en línea, proporcionando así una mayor seguridad de los detalles de la tarjeta y una mayor confianza del consumidor en el sistema.

El número de tarjeta de reemplazo se puede generar dinámicamente para su uso en una sola transacción. Alternativamente, el número de tarjeta de reemplazo puede mantenerse y usarse para múltiples transacciones.

Los detalles suplementarios de una transacción, que incluyen uno o más del monto de la transacción y una identificación del comerciante, también pueden transmitirse al dispositivo de puerta de enlace mediante el dispositivo de entrada de datos segura. Preferiblemente, dichos detalles suplementarios se transmiten al dispositivo de puerta de enlace en el mensaje de transacción que lleva la información de identificación.

En una realización particularmente preferida, el número de identificación bancaria del número de tarjeta de reemplazo puede seleccionarse de manera que la transacción de pago se enrute a través del dispositivo de puerta de enlace en la red de datos privados antes de enviarse a la institución financiera emisora de la tarjeta. alternativamente, el número de identificación bancaria del número de tarjeta de reemplazo puede seleccionarse de manera que la transacción de pago se dirija a través de la red de datos privados al dispositivo de puerta de enlace identificando el dispositivo de puerta de enlace como una institución emisora de la tarjeta del número de tarjeta de reemplazo.

Preferiblemente, el dispositivo de puerta de enlace incluye además medios para recibir mensajes de transacciones de pago desde la red de datos privada, medios para modificar mensajes de transacciones de pago recibidos y medios para transmitir dichos mensajes de transacciones de pago modificados a la institución financiera emisora de

la tarjeta, por lo que el dispositivo de puerta de enlace puede sustituir números de tarjeta reales por números de tarjetas de reemplazo antes de transmitir los mensajes de transacciones de pago recibidos a la institución financiera emisora de la tarjeta.

En una realización particularmente preferida, el dispositivo de puerta de enlace incluye además una base de datos de números de tarjetas de reemplazo que incluyen los correspondientes números de tarjetas reales y detalles de transacciones adicionales.

En otro aspecto, la invención proporciona un método para la autenticación por parte de una institución financiera emisora de tarjetas de información de identificación de un usuario titular de la tarjeta de una red pública de datos, que incluye los pasos de:

proporcionar un dispositivo de entrada de datos segura conectado a la red pública de datos;
proporcionar un dispositivo de puerta de enlace conectado a la red pública de datos y a una red de datos privada utilizada para transmitir mensajes entre instituciones financieras;
el usuario ingresa información de identificación de una tarjeta emitida por la institución financiera emisora de la tarjeta en el dispositivo de entrada segura de datos;
transmitir la información de identificación de una manera segura a través de la red pública de datos al dispositivo de puerta de enlace;
transmitir la información de identificación a la institución financiera emisora de la tarjeta; y
recibir una respuesta de aprobación de la institución financiera emisora de la tarjeta a través de la red de datos privados;
por lo que la respuesta de aprobación proporciona autenticación de la información de identificación por parte de la institución financiera emisora de la tarjeta.

En otro aspecto más, la invención proporciona un aparato de entrada de datos segura para su uso en un sistema para la autenticación por parte de una institución financiera emisora de tarjetas de información de identificación de un usuario con tarjeta de una red pública de datos que incluye:

una interfaz para la conexión a una red pública de datos;
medios para que el usuario ingrese información de identificación de una tarjeta emitida por la institución financiera;
medios para transmitir la información de identificación de manera segura a través de la red pública de datos a un dispositivo de puerta de enlace que incluye medios para transmitir la información de identificación a la institución financiera emisora de la tarjeta y para recibir una respuesta de aprobación de la institución financiera emisora de la tarjeta a través de la red de datos privados;
por lo que la respuesta de aprobación proporciona autenticación de la información de identificación por parte de la institución financiera emisora de la tarjeta.

La invención proporciona además un proceso para la autenticación, por parte de una institución financiera emisora de tarjetas, de la información de identificación de un usuario titular de la tarjeta de una red pública de datos, el proceso incluye los siguientes pasos:

proporcionar un dispositivo de entrada segura de segura conectado a la red pública de datos; y
proporcionar un dispositivo de puerta de enlace conectado a la red pública de datos y a una red de datos privada utilizada para transmitir mensajes entre instituciones financieras;
transmitir la información de identificación de una manera segura a través de la red pública de datos al dispositivo de puerta de enlace;
transmitir la información de identificación a la institución financiera emisora de la tarjeta; y
recibir una respuesta de aprobación de la institución financiera emisora de la tarjeta a través de la red de datos privada;
por lo que la respuesta de aprobación proporciona autenticación de la información de identificación por parte de la institución financiera emisora de la tarjeta.

Breve descripción de los dibujos

Los beneficios y ventajas adicionales de la presente invención resultarán evidentes en la siguiente descripción de las realizaciones preferidas de la invención, que, sin embargo, no deben considerarse que limitan el alcance de la invención o cualquiera de las declaraciones anteriores. Las realizaciones preferidas se describen con referencia a los dibujos adjuntos en los que:

La figura 1 ilustra una realización de un dispositivo de entrada segura de datos del cliente de acuerdo con la presente invención;

La figura 2 muestra el dispositivo de entrada segura de datos de la figura 1 en forma de diagrama de bloques funcional;

La figura 3 es un diagrama de bloques de una realización de un dispositivo de puerta de enlace de acuerdo con la presente invención;

La figura 4 ilustra un sistema para realizar una transacción segura entre un cliente y un comerciante de acuerdo con una realización preferida de la presente invención; y

La figura 5 es un diagrama de flujo que ilustra los pasos que se pueden llevar a cabo en el curso de una transacción dentro del sistema de la figura 4.

Descripción de la realización preferida

La figura 1 proporciona una ilustración de una realización de un dispositivo de entrada segura de datos, también denominado en este documento como dispositivo de punto de pago o PoP. La figura 2 representa este dispositivo como un diagrama de bloques lógico de sus partes compuestas.

El dispositivo 1 PoP es un producto seguro de bajo coste que incluye una unidad 3 de procesamiento, un lector 5 de tarjetas, un teclado 6, un visualizador 4 y una interfaz 7 que proporciona la transmisión de datos y potencia entre el dispositivo y un ordenador 8 personal. La interfaz 7 puede ser, por ejemplo, una interfaz periférica estándar tal como una conexión USB.

El dispositivo 1 PoP es capaz de obtener de forma segura información de pago de un cliente, tal como los detalles de la tarjeta de pago y el número de identificación personal (PIN), y cifrar estos detalles para su transporte seguro a un dispositivo remoto. En la realización preferida, los formatos de cifrado y mensajes usados por el dispositivo PoP cumplen con ISO 8583.

La unidad 3 de procesamiento es un ensamblaje de componentes electrónicos que proporciona los requisitos de control y almacenamiento electrónico del dispositivo, tales como controlar el teclado, el visualizador y el lector de tarjetas, y proporcionar el almacenamiento seguro de claves de cifrado. En la realización preferida, la unidad 3 de procesamiento es un solo circuito integrado, pero puede consistir en un ensamblaje de circuitos integrados físicamente separados u otras partes electrónicas tales como transistores y puertas lógicas.

El lector 5 de tarjetas se usa para obtener la información de identificación relevante de la tarjeta de pago de un cliente, y se puede construir para admitir tarjetas con electrónica integrada, tales como las que cumplen con el estándar ISO 7816 'tarjeta inteligente' o tarjetas que solo poseen una banda magnética en una o ambas caras para contener información tales como tarjetas de 'banda magnética' que cumplen con la norma ISO 7811. En la realización preferida, el lector 5 de tarjetas soporta tanto dichos tipos de tarjeta 'tarjeta inteligente' como dichos tipos de tarjeta de 'banda magnética'.

El teclado 6 se utiliza para la interacción del usuario con el sistema. Consiste en un número de claves que permiten al usuario realizar acciones, incluida la entrada de dígitos numéricos y la aceptación o cancelación de entradas. El teclado 6 también puede admitir entradas basadas en caracteres y está construido y escaneado de una manera que garantiza la seguridad e integridad de la entrada del usuario. El teclado 6 también puede admitir el uso de claves de 'función' adicionales cuya función está dictada por el estado y el funcionamiento de la aplicación de software que está siendo ejecutada por el dispositivo 3 de procesamiento.

El visualizador 4 proporciona información al usuario sobre el estado del dispositivo y su función. En la realización preferida, el visualizador consta de un visualizador de cristal líquido, que es capaz de visualizar al menos 2 filas de 8 caracteres.

Todos los componentes del dispositivo 1 PoP están encerrados dentro de una carcasa 2, preferiblemente hecha de una aleación de plástico económica. Las medidas de seguridad tales como evidencia de manipulación, detección de manipulación y respuesta a manipulación están integradas en el dispositivo y la carcasa para evitar el acceso no autorizado a los componentes, tales como el teclado o el dispositivo de procesamiento. Dichas medidas de seguridad son requisitos de las instituciones financieras a las que debe conectarse el dispositivo PoP y son esenciales para que el dispositivo acepte los PIN asociados con las tarjetas de los clientes. Dichos PIN se utilizan en la autenticación del titular de la tarjeta durante la transacción.

La Figura 3 muestra un diagrama de bloques lógico de un dispositivo 12 de puerta de enlace, también denominado en este documento una puerta de enlace PoP, que está conectado tanto a internet 10 como a una red 15 de datos privada utilizada para transmitir mensajes, tales como mensajes de transacción, entre instituciones financieras. La red 15 también se denomina en este documento red interbancaria. La puerta de enlace incluye un medio 20 de procesamiento, tal como un microprocesador y una memoria asociada y otro hardware periférico, que ejecuta una aplicación 17 PoP que controla el funcionamiento de la puerta de enlace 12 PoP e interactúa con un conmutador 18 de servidor financiero y una base 19 de datos de números de tarjeta.

El medio 20 de procesamiento podría ser cualquier sistema que permita la ejecución de comandos programados, tal como un ordenador personal, industrial o de ordenador central. Alternativamente, los medios 20 de procesamiento podrían ser un solo circuito integrado, o una combinación de muchos circuitos integrados físicamente separados o puertas lógicas.

El conmutador 18 de servidor financiero es una aplicación que está diseñada para proporcionar la transmisión y recepción de mensajes con una institución financiera, incluidos, entre otros, los mensajes definidos por la norma internacional de intercambio financiero ISO 8583.

La base 19 de datos de números de tarjetas es una base de datos de números de tarjetas 'virtuales' que se han asignado a los titulares de tarjetas para su uso en una o más transacciones.

La figura 4 es un diagrama de bloques de un sistema de transacciones completo, de acuerdo con una realización actualmente preferida de la invención, que ilustra las diferentes partes que están potencialmente involucradas en una transacción y las conexiones entre ellas. En resumen, el sistema incluye un cliente 9 que tiene un dispositivo de entrada segura de datos (dispositivo PoP) conectado a internet 10. Como se describió anteriormente, esta conexión se puede proporcionar a través del ordenador personal (PC) del cliente. El sistema también incluye un comerciante 11, que tiene una tienda virtual a la que se puede acceder a través de internet 11, y una institución 16 financiera adquirente que mantiene la cuenta bancaria del comerciante (comerciante adquirente). El sistema incluye además una institución 13 financiera emisora de tarjetas (emisor de tarjetas) que tiene una cuenta bancaria del cliente; y un dispositivo 12 de puerta de enlace (PoP puerta de enlace).

En la realización actualmente preferida, el cliente 9 es el iniciador y pagador de una transacción y posee un dispositivo 1 PoP que está conectado a un ordenador 8 personal que está conectada a internet 10. El cliente también posee una tarjeta de pago y PIN asociado.

El comerciante 11 es el destinatario y beneficiario de una transacción. El comerciante posee un sitio de internet que utiliza un sistema de pago estándar para el procesamiento de transacciones por internet y este sistema está conectado a través de internet 10 al banco 16 del comerciante ya sea directamente o a través de un proveedor de servicios de pago que facilita el comercio por internet conectando comerciantes e instituciones financieras.

El banco 16 del comerciante, también conocido como el banco adquirente, es la institución que mantiene la cuenta bancaria de ese comerciante y está conectada al comerciante a través de internet 10, ya sea directa o indirectamente, y una red 15 interbancaria utilizada para la transferencia de datos de transacciones electrónicas. Ejemplos de tales redes son Bank Net, que es mantenida por MasterCard, y VISA Net, que es mantenida por VISA. Estas redes son el método estándar para la transferencia de transacciones entre instituciones financieras separadas físicamente, y tal como las utilizan los actuales sistemas de comercio por internet para emitir solicitudes de autorización y transferencia de fondos.

El banco 13 emisor de la tarjeta es la institución financiera que emitió la tarjeta de pago al cliente y también está conectada a la red 15. interbancaria

La puerta de enlace 12 PoP está conectada tanto a internet 10 como a la red 15 interbancaria y está involucrada tanto en la transacción EFTPOS inicial que se utiliza para confirmar la identidad y los fondos del cliente 9, y los mensajes estándar de autorización/transferencia de fondos que se envían desde el comerciante 11 a través del banco 16 adquirente del comerciante. Pueden existir múltiples puertas de enlace de pago al mismo tiempo para evitar la congestión o posibles ataques, tal como un ataque de 'denegación de servicio', que inutilice el sistema. También es posible que se requiera que cualquier dispositivo PoP arbitrario se conecte a una puerta de enlace PoP específica debido a la ubicación geográfica o acuerdos contractuales de dicho dispositivo PoP. Además, la puerta de enlace PoP no necesita ser una entidad físicamente separada, sino que de hecho puede estar integrada en la red interbancaria o desplegada y mantenida por el banco 13 emisor de la tarjeta como parte de su sistema de servidor financiero.

La figura 5 proporciona un diagrama 500 de flujo del funcionamiento de la realización preferida de la invención. El diagrama 500 ilustra que el sistema se puede utilizar para obtener autenticación de los detalles financieros relacionados con el cliente con el fin de:

transferir prueba de autenticación a otra parte;
obtener un número de tarjeta de reemplazo que pueda usarse junto con la invención para compras remotas posteriores; o
obtener un número de tarjeta de reemplazo que se pueda usar junto con la invención para una compra actualmente en curso.

Para realizar una de las tres operaciones descritas anteriormente, primero se selecciona 502 el modo de funcionamiento apropiado. El modo de funcionamiento es uno de los siguientes: prueba de autenticación; reemplazo dinámico del número de tarjeta; o reemplazo de número de tarjeta estático. El modo de operación deseado puede ser seleccionado a través de la interacción del cliente, o automáticamente por el ordenador personal del cliente, o los medios de procesamiento del dispositivo PoP.

En el siguiente paso 504 en todos los modos de operación, el cliente ingresa la información de identificación de su tarjeta ingresando su tarjeta de pago y PIN en el dispositivo PoP.

Para obtener la autenticación de la información de identificación del cliente, en el siguiente paso 506 el dispositivo PoP comunica la información a la puerta de enlace PoP. En particular, el dispositivo 1 PoP proporciona la transmisión segura de los detalles de pago de los clientes a la puerta de enlace 12 PoP a través de internet 10.

Esta seguridad se proporciona mediante el cifrado de la información, utilizando un esquema de cifrado y una clave de cifrado mantenida dentro de la carcasa segura de dicho dispositivo 1 PoP de manera que los detalles de pago del cliente no estén disponibles para ninguna parte o dispositivo externo al dispositivo PoP en forma no cifrada. En la realización preferida, el formato de cifrado y mensaje utilizado para comunicarse con dicha puerta de enlace PoP se ajusta a ISO 8583, y específicamente los detalles de pago se formatean como una compra '0200' o una transacción de autorización '0104'. El dispositivo PoP proporciona una indicación en este mensaje para informar a la puerta de enlace PoP del modo de operación seleccionado para la transacción actual.

En el paso posterior 508, la puerta de enlace 12 PoP descifra y reenvía esta transacción al banco 13 emisor de la tarjeta. Esto puede implicar que la puerta de enlace PoP vuelva a cifrar y/o formatear el mensaje para su transmisión al banco 13 emisor de la tarjeta. Si el banco emisor de la tarjeta no indica la aprobación de los detalles de pago (por ejemplo, debido a un PIN incorrecto proporcionado por el cliente), entonces se devuelve una indicación de que la transacción ha sido rechazada al dispositivo PoP, que informa 510 al cliente del fracaso.

Sin embargo, si los detalles del pago son aprobados por el banco emisor de la tarjeta, entonces se llevan a cabo más pasos, seleccionándose 512 las operaciones precisas sobre la base del modo de operación elegido.

En el modo de funcionamiento de prueba de autenticación, la puerta de enlace PoP transfiere 514 la aprobación del banco emisor de la tarjeta al dispositivo PoP. El dispositivo PoP luego usa esta aprobación para obtener 516 pruebas verificables de que la información de identificación del cliente ha sido autenticada. La prueba generalmente tomará la forma de un bloque de datos de autenticación, que consiste en datos que pueden derivarse de manera segura de la aprobación enviada por el banco emisor de la tarjeta. Un bloque de datos de autenticación puede generarse, por ejemplo, en forma de un resumen seguro del mensaje de aprobación, tal como un cifrado completo o truncado del mensaje de aprobación. Dicho cifrado puede realizarse utilizando una clave secreta almacenada de forma segura dentro del dispositivo PoP.

El mensaje de aprobación en combinación con el bloque de datos de autenticación puede usarse posteriormente como prueba de autorización por parte del banco emisor de la tarjeta. Un dispositivo receptor puede verificar la prueba confirmando que un mensaje de aprobación y un bloque de autenticación que le proporcionó el dispositivo PoP son válidos. Si se utiliza un sistema de cifrado simétrico para generar el bloque de datos de autenticación, entonces el dispositivo receptor requiere la misma clave secreta para la verificación que utilizó el dispositivo PoP para generar el bloque de datos. Dichas claves secretas se pueden distribuir a aquellos dispositivos seguros y confiables que las requieran a través de cualquiera de varios métodos seguros de distribución de claves conocidos en la técnica. Alternativamente, se puede usar un sistema de cifrado asimétrico, en cuyo caso el dispositivo PoP usa una clave privada para generar el bloque de datos de autenticación y el dispositivo receptor puede verificar la prueba usando la clave pública correspondiente, que no necesita ser almacenada o distribuida de forma segura.

En el modo de funcionamiento de sustitución de número de tarjeta estático, el sistema se utiliza para emitir al cliente un número de tarjeta de reemplazo estático que permite que el dispositivo PoP se use con comerciantes que utilizan un sistema de pago que almacena los detalles de pago de los clientes para su uso en transacciones posteriores. El sistema de pago de 'un clic' es un ejemplo de dicho sistema. Preferiblemente, la puerta de enlace PoP almacena este número de tarjeta de reemplazo estático, permitiendo así que se proporcione el mismo número de tarjeta de reemplazo para una tarjeta de pago en particular, independientemente del dispositivo PoP particular utilizado. Alternativamente, el dispositivo PoP puede almacenar el número de tarjeta de reemplazo estático.

En el modo de reemplazo de número de tarjeta estático, una vez que se ha indicado la aprobación en la respuesta del banco emisor de la tarjeta, la puerta de enlace 12 de PoP establece 534 con el dispositivo 1 de PoP un número de tarjeta de reemplazo estático. Preferiblemente, los primeros seis dígitos del número de tarjeta de reemplazo, conocido como número de identificación bancaria, se establecen en un valor específico que indica que el número de tarjeta fue emitido por la puerta de enlace 12 de PoP. Esto permite que una transacción desde el banco 16 de cualquier comerciante sea enrutada a través de dicha puerta de enlace 12 PoP durante su tránsito a través de la red 15 interbancaria hasta el banco 14 emisor de la tarjeta. Preferiblemente, el número de identificación bancaria utilizado en el número de la tarjeta de reemplazo indica que la tarjeta es emitida por los clientes del banco 13 emisor, pero que la transacción debe enrutarse a través de la puerta de enlace 12 PoP antes de llegar al banco 13 emisor. Tal enrutamiento específico se puede indicar en los campos 33 y 100 de un mensaje de transacción ISO 8583, los valores de estos campos se establecen de acuerdo con el BIN de la tarjeta. Los dígitos restantes del número de la tarjeta de reemplazo podrían ser el número de cuenta principal original cifrado por el dispositivo 1 PoP o la puerta de enlace 12, un número de tarjeta generado aleatoriamente por la puerta de enlace o un número de tarjeta elegido de una lista contenida en la base 19 de datos de números de tarjeta. Si se utiliza una versión cifrada del número de tarjeta de pago del cliente original, es posible que sea necesario modificar este valor cifrado para garantizar que el número de tarjeta de reemplazo cumpla con los estándares de tarjetas de pago requeridos.

El número de tarjeta de reemplazo estático se transfiere luego al usuario a través del dispositivo 1 PoP, y puede almacenarse en el dispositivo 1, o en la base 19 de datos de número de tarjeta de la puerta de enlace 12 PoP.

Para completar una compra posterior, el cliente 9 proporciona al comerciante 11 el número de tarjeta de reemplazo estático en lugar de su número de tarjeta real, y la transacción se completa de acuerdo con los pasos 520-532 como se describe con mayor detalle en el después de la discusión sobre el modo de operación de reemplazo dinámico de tarjeta.

En el modo de operación de reemplazo dinámico de tarjeta, el sistema se usa para emitir al cliente un número de tarjeta de pago de reemplazo que se puede usar en una transacción actualmente en curso a través de internet. El cliente 9 selecciona bienes/servicios del sitio web del comerciante 11 y procede a la 'página' de pago de la manera normal, donde se le presenta el formulario de información de pago del comerciante 11.

En el modo de reemplazo dinámico del número de tarjeta, una vez que se ha indicado la aprobación en la respuesta del banco emisor de la tarjeta, la puerta de enlace 12 PoP verifica si la tarjeta de pago tiene un número de tarjeta de reemplazo estático asignado y lo usará si existe. Si no, la puerta de enlace 12 PoP establece 518 con el dispositivo 1 PoP un número de tarjeta de reemplazo que se aplicará durante el resto de la transacción con el comerciante. Es posible que el número de identificación del banco deba establecerse en un valor específico que indique que el número de tarjeta fue emitido por la puerta de enlace 12 PoP para permitir que la transacción desde el banco 16 del comerciante se enrute a través de la puerta de enlace 12 PoP durante su tránsito a través de la red 15 interbancaria hasta el banco 14 emisor de la tarjeta. Preferiblemente, el Número de identificación bancaria utilizado para el número de tarjeta de reemplazo indica que la tarjeta es emitida por el banco 13 emisor del cliente, pero que la transacción debe enrutarse a través de la puerta de enlace 12 PoP antes de llegar al banco 13 emisor. Tal enrutamiento específico se puede indicar en los campos 33 y 100 de un mensaje de transacción ISO 8583, los valores de estos campos se establecen de acuerdo con el BIN de la tarjeta. Los dígitos restantes del número de la tarjeta de reemplazo podrían ser el número de cuenta principal original cifrado por el dispositivo 1 PoP o la puerta de enlace 12, un número de tarjeta generado aleatoriamente por la puerta de enlace 12 o un número de tarjeta elegido de una lista contenida en la base 19 de datos de números de tarjeta. Si se utiliza una versión cifrada del número de tarjeta de pago del cliente original, es posible que sea necesario modificar este valor cifrado para garantizar que el número de tarjeta de reemplazo cumpla con los estándares de tarjetas de pago requeridos.

Preferiblemente, la puerta de enlace 12 PoP también obtiene información relacionada con el coste de la transacción y la identificación del comerciante, con respecto a la compra en curso.

La puerta de enlace 12 PoP almacena entonces el número de tarjeta de reemplazo, y el número de tarjeta original, y cualquier información adicional obtenida en relación con la transacción en proceso, en la base 19 de datos de números de tarjeta para su uso posterior en la transacción. Alternativamente, estos detalles podrían transmitirse a la puerta de enlace 12 PoP en campos especiales del mensaje de transacción, eliminando el requisito de la base de datos de números de tarjeta. Preferiblemente, la puerta de enlace 12 PoP admite ambos métodos.

El dispositivo 1 PoP notifica entonces al software de aplicación PoP residente en el ordenador personal del cliente que se ha obtenido un número de tarjeta de reemplazo. Este número de tarjeta de reemplazo luego se transfiere 520 a la página de pago de internet del comerciante, ya sea a través de la agencia de la aplicación PoP PC que determina automáticamente la ubicación del campo de número de tarjeta, o visualizando el número de tarjeta en el visualizador 4 del dispositivo 1 PoP para el cliente 9 para transcribirlo en la sección apropiada de la página.

El comerciante 11 procede entonces con la transacción usando su sistema de pago estándar, como se usa con cualquier transacción normal. Por ejemplo, el comerciante puede tener su propio sistema de procesamiento de pagos que se utiliza, puede transferir la solicitud de pago a un proveedor de servicios de pago o puede comunicarse directamente con la institución financiera que mantiene la cuenta bancaria del comerciante. Independientemente de la realización de este sistema de pago, en última instancia, se emitirá una solicitud de transferencia de fondos al banco 16 del comerciante.

El banco 16 del comerciante enviará 522 entonces un mensaje de transferencia de fondos a la institución financiera que es indicado por el BIN del número de tarjeta de reemplazo proporcionado por el cliente 9 a través de la red 15 interbancaria. En la realización preferida de la invención, esto es el banco 13 emisor de la tarjeta del cliente, sin embargo, también puede ser la puerta de enlace 12 PoP. Preferiblemente, este mensaje tomará la forma de un mensaje de solicitud de autorización ISO 8583 '0100', un mensaje de solicitud de presentación financiera '0200' o mensaje de aviso de '0220' presentación financiera. El tipo, formato y número de mensajes que se envían a dicho banco emisor de la tarjeta de cliente depende del monto de la transacción y las políticas del banco 16 del comerciante. Se pueden enviar múltiples mensajes, por ejemplo, el banco 16 del comerciante puede enviar un mensaje de solicitud de autorización. para verificar la capacidad del cliente para pagar la compra antes de que finalice la transacción con el cliente, y luego enviar una solicitud de presentación financiera cuando finalice la transacción.

En la realización preferida de la invención, los mensajes de transferencia de fondos se envían al banco 13 emisor de la tarjeta del cliente a través de la puerta de enlace 12 de PoP. Esta ruta está determinada por el BIN del número de

tarjeta de reemplazo proporcionado por el cliente 9. En el siguiente paso 524 de la transacción, en la puerta de enlace PoP, la aplicación 17 PoP identifica el número de tarjeta de reemplazo en su base 19 de datos de números de tarjeta y luego restablece el número de tarjeta original de los clientes. Todos los detalles adicionales proporcionados durante la transacción de autorización inicial, tales como el monto del pago y los detalles del comerciante, también se verifican en esta etapa y la transacción se rechaza si estos valores no coinciden con los que se encuentran en la base 19 de datos de números de tarjeta. Si todos los detalles complementarios suministrados son correctos, el mensaje se prepara para su transmisión al banco 13 emisor de la tarjeta del cliente. Si la puerta de enlace 12 de PoP está lógicamente remota al banco emisor de la tarjeta del cliente, la aplicación PoP también modifica el mensaje para asegúrese de que la respuesta al mensaje se enrute de regreso a través de la puerta de enlace 12 PoP en su camino al banco 16 del comerciante. En un mensaje ISO 8583, esto se puede lograr modificando el campo adquiriente en el mensaje.

En el siguiente paso 526, el banco 13 emisor de la tarjeta del cliente recibe el mensaje financiero de la puerta de enlace 12 PoP y lo procesa de la manera normal. La respuesta se envía de vuelta a la puerta de enlace 12 PoP según lo dictado por las alteraciones al mensaje original realizadas por la aplicación PoP antes de su transmisión a dicho banco de clientes. En un paso 528 realizada en la puerta de enlace 12 de PoP, el número de tarjeta del cliente se sustituye una vez más por el número de tarjeta de reemplazo y la respuesta se reenvía al adquiriente, es decir, al banco 16 del comerciante. Esto puede requerir que la aplicación PoP mantenga un registro de mensajes financieros reenviados para permitirle retransmitir la respuesta a la institución financiera correcta.

Tras la recepción de todas las respuestas al mensaje de transacción enviadas desde el banco 13 emisor de la tarjeta del cliente a través de la puerta de enlace 12 PoP, el banco 16 del comerciante finaliza 530 la transacción. Los bienes o servicios solicitados por el cliente se pagan en su totalidad y la transacción se completa 532.

A partir de la descripción anterior, resultará fácilmente evidente para los expertos en la técnica que son posibles muchas variaciones del sistema y método de pago seguro de acuerdo con la invención, que no se limita a las realizaciones descritas. Se han descrito un número de combinaciones de características con referencia a realizaciones específicas de la invención, o partes componentes de la misma, sin embargo, será evidente para el experto que estas diversas características pueden combinarse de otras formas sin dejar de estar dentro del alcance de la invención tal como se define en las reivindicaciones adjuntas.

En particular, será evidente para una persona experta que se pueden realizar muchas modificaciones en el dispositivo 1 PoP, incluida la integración del dispositivo en un teclado de ordenador, teléfono móvil, dispositivo señalador u otro periférico de ordenador similar, sin apartarse del espíritu y alcance de la invención. Además, la puerta de enlace 12 de PoP no necesita ser un dispositivo autónomo, y puede integrarse en una institución financiera emisora de PoP (emisor de PoP) o la red interbancaria.

En otras variaciones, el sitio web del comerciante puede proporcionar soporte adicional para el sistema de pago seguro. Por ejemplo, en lugar de que el cliente 9 deba ingresar su tarjeta y PIN en el dispositivo 1 PoP para activar el software PoP, los campos especiales contenidos dentro de la página de pago, tales como etiquetas HTML que no se visualizan al cliente 9 pueden hacer que el software instalado en el ordenador 8 personal active el dispositivo 1 PoP, que luego solicitará al cliente 1 que ingrese su tarjeta de pago y sus detalles. El software PoP también podría utilizar estos campos especiales para transmitir la información de pago de los clientes y los detalles de envío al comerciante.

Por tanto, se entenderá que la invención podría adoptar muchas formas y tener muchos usos diferentes. Todas estas formas y usos están definidos por el alcance de las reivindicaciones.

REIVINDICACIONES

1. Un sistema para la autenticación por una institución financiera emisora de tarjetas de información de identificación de un usuario titular de una tarjeta de una red pública de datos, el sistema comprende:

un dispositivo (1) de entrada de datos segura conectado a la red (10) pública de datos a través de un ordenador (8) personal; y
un dispositivo de puerta de enlace (12) conectado a la red pública de datos y a una red (15) privada de datos utilizada para transmitir mensajes entre instituciones (13/16) financieras;
en donde el dispositivo de entrada segura de datos es un dispositivo periférico relativo al ordenador personal y comprende una carcasa (2) que encierra componentes del dispositivo de entrada segura de datos que incluye:

una interfaz (7) de transmisión de datos para proporcionar la transmisión de datos entre el dispositivo de entrada segura de datos y el ordenador personal,
medios para que el usuario ingrese información identificativa de una tarjeta emitida por la institución financiera,
medios para que el usuario ingrese el número de identificación personal [PIN] del usuario,
medios para mantener un esquema de cifrado y una clave de cifrado,
medios para cifrar la información de identificación y el PIN, utilizando el esquema de cifrado y la clave de cifrado mantenidos, para una transmisión segura, y
medios para transmitir la información de identificación cifrada y el PIN de manera segura, a través de la interfaz (7) de transmisión de datos entre el dispositivo de entrada segura de datos y el ordenador personal, a través de la red pública de datos al dispositivo de puerta de enlace, en donde la carcasa (2) es configurada para evitar el acceso no autorizado a los componentes del dispositivo de entrada segura de datos encerrado dentro de la carcasa; y

en donde el dispositivo de puerta de enlace incluye medios para transmitir la información de identificación a la institución financiera emisora de la tarjeta y para recibir una respuesta de aprobación de la institución financiera emisora de la tarjeta a través de la red de datos privados;
en donde la respuesta de aprobación proporciona autenticación de la información de identificación por parte de la institución financiera emisora de la tarjeta;
en donde el dispositivo de puerta de enlace incluye además medios para generar un número de tarjeta de reemplazo al recibir la respuesta de aprobación de la institución emisora de la tarjeta y en donde el número de identificación bancaria del número de tarjeta de reemplazo se selecciona de manera que:

la transacción de pago se enruta a través del dispositivo de puerta de enlace en la red de datos privada antes de enviarse a la institución financiera emisora de la tarjeta, o
la transacción de pago se dirige a través de la red de datos privada al dispositivo de puerta de enlace identificando el dispositivo de puerta de enlace como una institución emisora de la tarjeta del número de tarjeta de reemplazo.

2. El sistema de la reivindicación 1, en donde la red pública de datos es internet.

3. El sistema de una cualquiera de las reivindicaciones anteriores, en donde la red de datos privada es una red interbancaria utilizada para la transferencia de datos de transacciones electrónicas.

4. El sistema de la reivindicación 3, en donde la red de datos privada se proporciona a través de una red dedicada operada con el único propósito de realizar transacciones financieras electrónicas.

5. El sistema de la reivindicación 3, en donde la red de datos privada es una red privada virtual operada con el propósito de realizar transacciones financieras electrónicas a través de una red de datos pública de servidor.

6. El sistema de una cualquiera de las reivindicaciones anteriores, en donde el dispositivo de entrada segura de datos incluye además:

un lector de tarjetas para leer información relevante almacenada en la tarjeta del usuario; y un teclado para permitir que el usuario ingrese datos en el sistema.

7. El sistema de la reivindicación 6, en donde el dispositivo de entrada segura de datos comprende además:

una unidad (3) de procesamiento y un visualizador (4).

8. El sistema de la reivindicación 6 o la reivindicación 7, en donde el lector de tarjetas puede leer una o ambas tarjetas de tipo "tarjeta inteligente" ISO 7816 o de tipo "banda magnética" ISO 7811.

9. El sistema de una cualquiera de las reivindicaciones anteriores en donde dicha información de identificación incluye uno o más de:

el número de cuenta principal asociado con la tarjeta;
la fecha de caducidad de la tarjeta; y
el PIN del usuario asociado con la tarjeta.

10. El sistema de una cualquiera de las reivindicaciones anteriores, en donde la información de identificación se transmite utilizando un formato de mensaje de transacción estándar que cumple con ISO 8583.

11. El sistema de la reivindicación 10, en donde el mensaje ISO 8583 usado es uno de un mensaje de presentación financiera '0200' y un mensaje de autorización '0104'.

12. El sistema de una cualquiera de las reivindicaciones anteriores, en donde el dispositivo de puerta de enlace también incluye medios para transmitir la respuesta de aprobación al dispositivo de entrada segura de datos.

13. El sistema de la reivindicación 12, en donde el dispositivo de entrada segura de datos incluye además medios para derivar de la respuesta de aprobación una prueba verificable de que la información de identificación del cliente ha sido autenticada por la institución financiera emisora de la tarjeta.

14. El sistema de la reivindicación 13, en donde dicha prueba es un bloque de datos de autenticación, que consta de datos calculados de manera segura a partir de la aprobación enviada desde el banco emisor de la tarjeta.

15. El sistema de la reivindicación 14, en donde el bloque de datos es un cifrado completo o truncado del mensaje de aprobación derivado usando una clave de cifrado almacenada de forma segura dentro del dispositivo de entrada segura de datos.

16. El sistema de una cualquiera de las reivindicaciones precedentes, en donde el número de tarjeta de reemplazo se transmite al dispositivo de entrada segura de datos a través de la red pública de datos.

17. El sistema de la reivindicación 16, en donde el número de tarjeta de reemplazo se genera dinámicamente para su uso en una única transacción.

18. El sistema de la reivindicación 16, en donde el número de tarjeta de reemplazo se mantiene y se usa para múltiples transacciones.

19. El sistema de cualquiera de las reivindicaciones 16 a 18, en donde los detalles complementarios de una transacción también se transmiten al dispositivo de puerta de enlace mediante el dispositivo de entrada segura de datos, y en donde dichos detalles complementarios incluyen uno o más del monto de la transacción y una identificación del comerciante.

20. El sistema de la reivindicación 19, en donde dichos detalles complementarios se transmiten al dispositivo de puerta de enlace en el mensaje de transacción que lleva la información de identificación.

21. El sistema de una cualquiera de las reivindicaciones 16 a 20, en donde el dispositivo de puerta de enlace incluye además:

medios para recibir mensajes de transacciones de pago de la red de datos privada;
medios para modificar mensajes de transacciones de pago recibidos; y
medios para transmitir dichos mensajes de transacciones de pago modificados a la institución financiera emisora de la tarjeta;
mediante el cual el dispositivo de puerta de enlace puede sustituir los números de tarjeta reales por números de tarjetas de reemplazo antes de transmitir los mensajes de transacciones de pago recibidos a la institución financiera emisora de la tarjeta.

22. El sistema de una cualquiera de las reivindicaciones 16 a 21, en donde el dispositivo de puerta de enlace incluye además una base de datos de números de tarjetas de reemplazo que incluyen los números de tarjetas reales correspondientes y detalles de transacciones complementarias.

23. Un método para la autenticación por parte de una institución financiera emisora de tarjetas de información de identificación de un usuario titular de una tarjeta de una red pública de datos, que comprende los pasos de:

proporcionar un dispositivo de entrada segura de datos conectado a la red pública de datos a través de un ordenador (8) personal en donde el dispositivo de entrada segura de datos es un dispositivo periférico en relación con el ordenador personal y en donde los componentes del dispositivo de entrada segura de datos están encerrados dentro de una carcasa configurada para evitar el acceso no autorizado a los componentes, en donde los componentes del dispositivo de entrada segura de datos que están encerrados dentro de la carcasa incluyen una interfaz (7) de transmisión de datos para proporcionar la transmisión de datos entre el dispositivo de entrada segura de datos y el ordenador personal, medios para que el usuario ingrese información de identificación de una tarjeta emitida por la institución financiera, medios para que el usuario ingrese el número de identificación personal [PIN] del usuario, medios para mantener un esquema de cifrado y una clave de cifrado, medios para cifrar la información de identificación y el PIN, utilizando el esquema de cifrado mantenido y la clave de cifrado, para una transmisión segura, y los medios para transmitir la información de identificación cifrada y el PIN de manera segura, a través de la interfaz (7) de transmisión de datos entre el dispositivo de entrada segura de datos y el ordenador personal, a través de la red pública de datos al dispositivo de puerta de enlace;

proporcionar un dispositivo de puerta de enlace conectado a la red pública de datos y a una red de datos privada utilizada para transmitir mensajes entre instituciones financieras;
el usuario ingresa información de identificación de una tarjeta emitida por la institución financiera emisora de la tarjeta en el dispositivo seguro de entrada de datos;
el usuario ingresa el número de identificación personal [PIN] del usuario; cifrar la información de identificación y el PIN para una transmisión segura; transmitir la información de identificación cifrada y el PIN de una manera segura a través de la red pública de datos al dispositivo de puerta de enlace a través de una interfaz (7) de transmisión de datos del dispositivo de entrada segura de datos para proporcionar la transmisión de datos entre el dispositivo de entrada segura de datos y el ordenador personal;
transmitir la información de identificación a la institución financiera emisora de la tarjeta; y
recibir una respuesta de aprobación de la institución financiera emisora de la tarjeta a través de la red de datos privada;
en el que la respuesta de aprobación proporciona autenticación de la información de identificación por parte de la institución financiera emisora de la tarjeta;
generar un número de tarjeta de reemplazo al recibir la respuesta de aprobación de la institución emisora de la tarjeta; y
seleccionando el número de identificación bancaria del número de la tarjeta de reemplazo de manera que:
la transacción de pago se enruta a través del dispositivo de puerta de enlace en la red de datos privada antes de enviarse a la institución financiera emisora de la tarjeta, o la transacción de pago se dirige a través de la red de datos privada al dispositivo de puerta de enlace identificando el dispositivo de puerta de enlace como institución emisora de tarjeta del número de tarjeta de reemplazo.

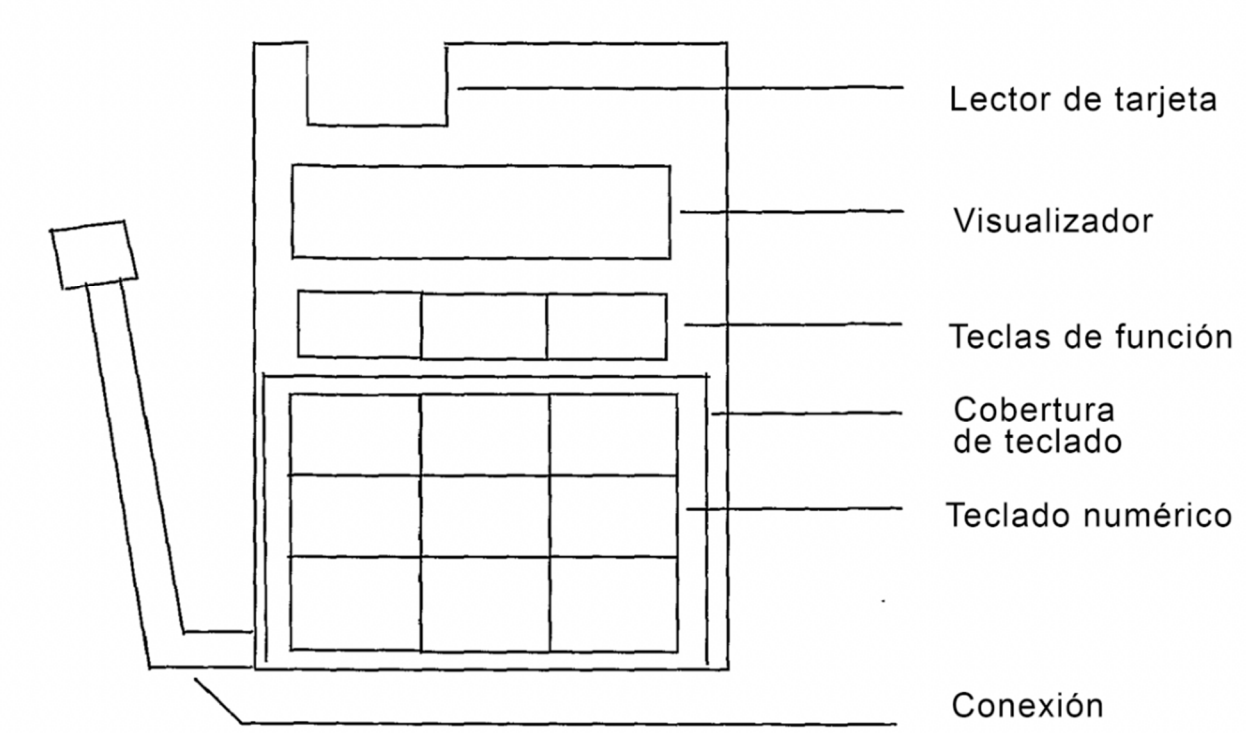

Figura 1: Dibujo ilustrativo del dispositivo de punto de pago

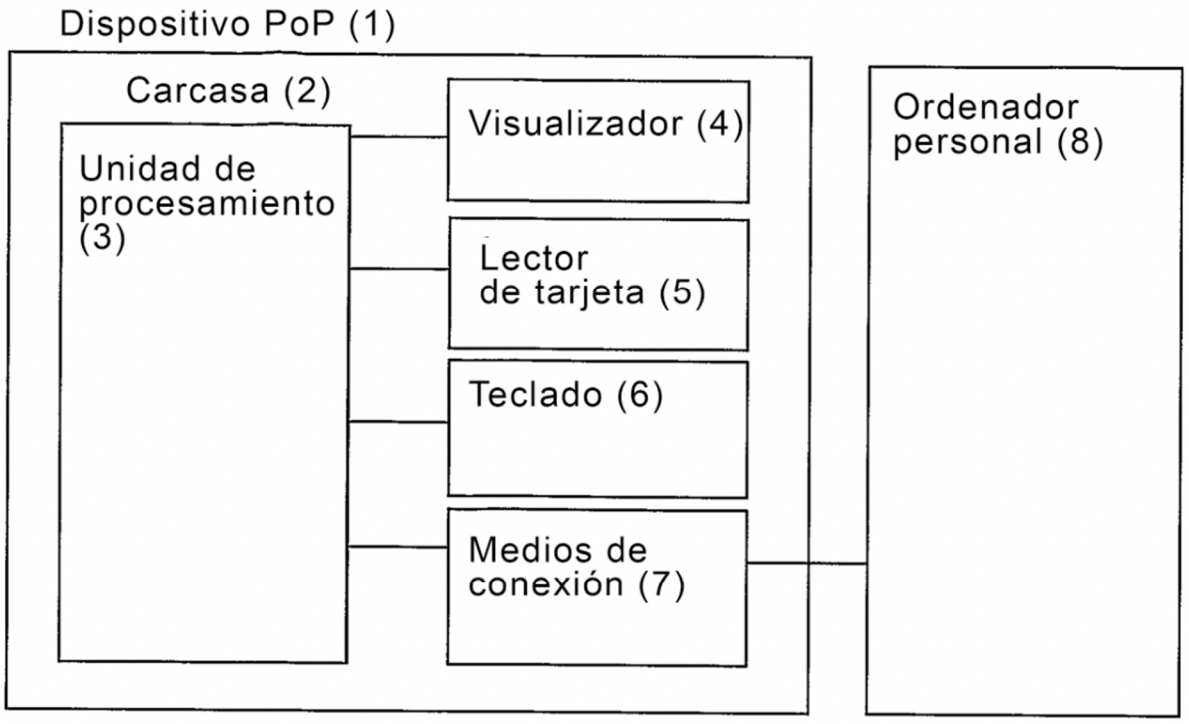

Figura 2: Diagrama de bloques lógico del dispositivo de punto de pago

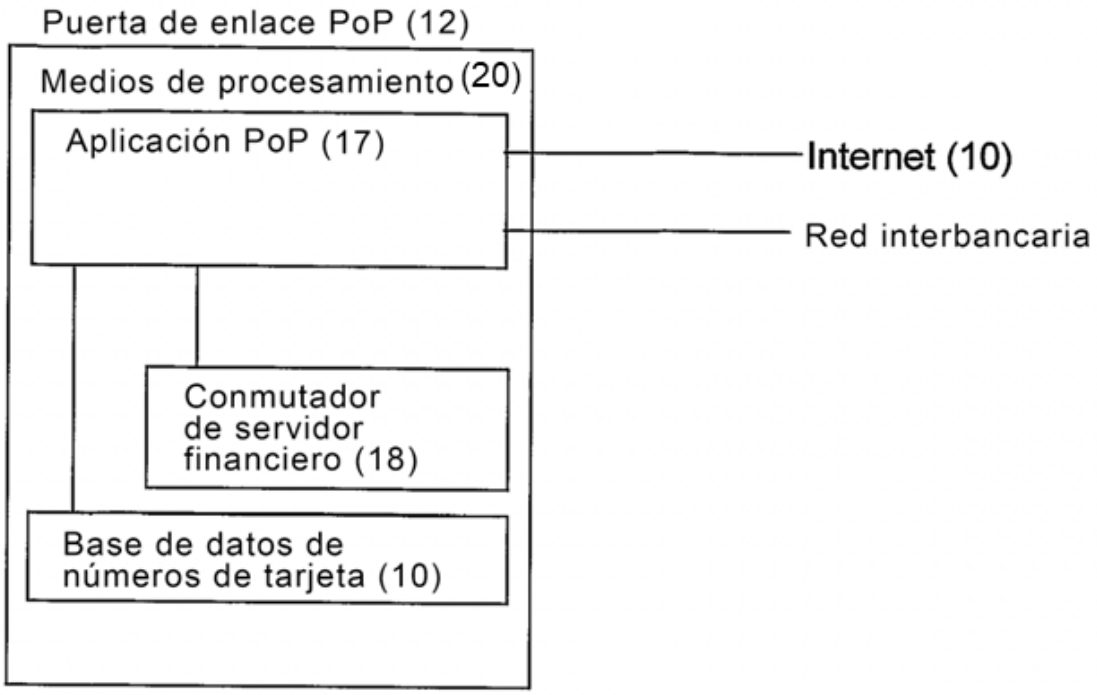
Puerta de enlace PoP (12)
Medios de procesamiento (20)
Aplicación PoP (17)
Internet (10)
Red interbancaria
Conmutador de servidor financiero (18)
Base de datos de números de tarjeta (10)

Figura 3

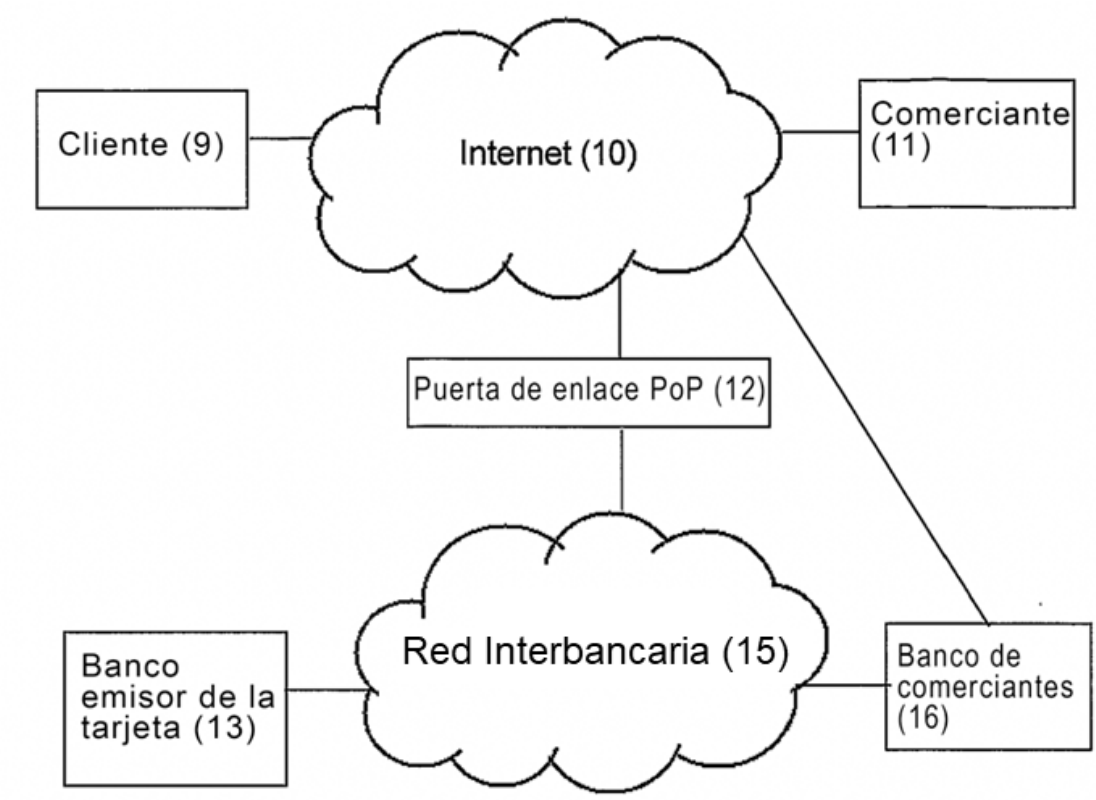

Figura 4: Resumen esquemático del punto de pago

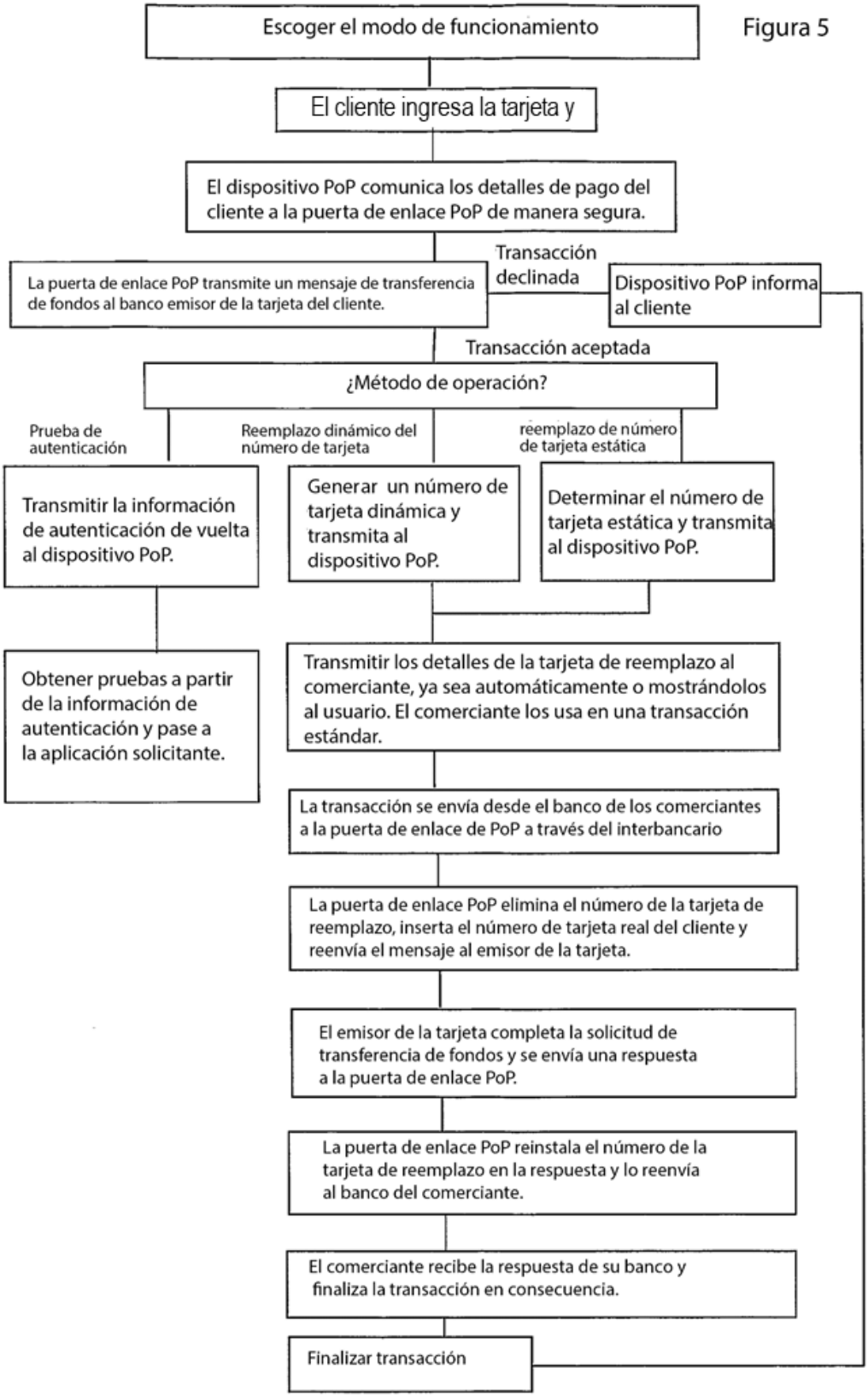
Escoger el modo de funcionamiento
El cliente ingresa la tarjeta y
El dispositivo PoP comunica los detalles de pago del cliente a la puerta de enlace PoP de manera segura.
La puerta de enlace PoP transmite un mensaje de transferencia de fondos al banco emisor de la tarjeta del cliente.
Transacción declinada
Dispositivo PoP informa al cliente
Transacción aceptada
¿Método de operación?
Prueba de autenticación
Reemplazo dinámico del número de tarjeta
reemplazo de número de tarjeta estática
Transmitir la información de autenticación de vuelta al dispositivo PoP.
Generar un número de tarjeta dinámica y transmita al dispositivo PoP.
Determinar el número de tarjeta estática y transmita al dispositivo PoP.
Obtener pruebas a partir de la información de autenticación y pase a la aplicación solicitante.
Transmitir los detalles de la tarjeta de reemplazo al comerciante, ya sea automáticamente o mostrándolos al usuario. El comerciante los usa en una transacción estándar.
La transacción se envía desde el banco de los comerciantes a la puerta de enlace de PoP a través del interbancario
La puerta de enlace PoP elimina el número de la tarjeta de reemplazo, inserta el número de tarjeta real del cliente y reenvía el mensaje al emisor de la tarjeta.
El emisor de la tarjeta completa la solicitud de transferencia de fondos y se envía una respuesta a la puerta de enlace PoP.
La puerta de enlace PoP reinstala el número de la tarjeta de reemplazo en la respuesta y lo reenvía al banco del comerciante.
El comerciante recibe la respuesta de su banco y finaliza la transacción en consecuencia.
Finalizar transacción

Figura 5