(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 659 723**

(51) Int. CI.:

G06Q 20/02 (2012.01)
G06Q 20/12 (2012.01)
G06Q 20/40 (2012.01)
G07F 7/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.06.2003 E 10183825 (8)**

(97) Fecha y número de publicación de la concesión europea: **13.12.2017 EP 2284784**

(54) Título: **Plataforma mercantil universal para autentificación de pago**

(30) Prioridad:

12.06.2002 US 388094 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.03.2018

(73) Titular/es:

CARDINALCOMMERCE CORPORATION (100.0%)
6119 Heisley Road
Mentor, OH 44060-1837, US

(72) Inventor/es:

KERESMAN, MICHAEL, A.;
SHERWIN, FRANCIS, M. y
BALASUBRAMANIAN, CHANDRA, S.

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Plataforma mercantil universal para autentificación de pago

Esta Solicitud reivindica los beneficios de la Solicitud Provisional de los EE.UU. Nº 60/386.345, presentada el 12 de junio de 2002, la cual se incorpora a la presente memoria en su totalidad como referencia.

Campo

La presente invención se refiere a la técnica de la autentificación. Encuentra particular aplicación en combinación con el hecho de facilitar la autentificación de un individuo para llevar a cabo una transacción comercial segura con una tarjeta de crédito o débito a través de una red de comunicaciones, por ejemplo, la internet, y se describirá con referencia particular a la misma. Ha de apreciarse, sin embargo, que la invención es también trasladable a otras aplicaciones similares.

Antecedentes

El comercio por internet, o comercio electrónico (*e-commerce*) como también es conocido, se refiere a la compra y venta de productos y servicios entre consumidores y comerciantes a través de la internet, o a otros intercambios transaccionales similares de información. La comodidad de hacer compras a través de la internet ha provocado un considerable interés en el comercio electrónico, tanto en lo que respecta a los consumidores como a los comerciantes. Las ventas por internet, o transacciones similares, se han venido llevando a cabo, por lo común, utilizando tarjetas de crédito convencionales tales como Visa®, MasterCard®, Discover®, American Express® u otras similares, o bien tarjetas de débito convencionales, es decir, tarjetas de cheques o tarjetas para cajero automático (ATM –"automated teller machine"–) que acceden directamente a los fondos desde una cuenta depósito asociada u otra cuenta bancaria.

Si bien se utilizan de forma generalizada para transacciones cara a cara, o presenciales, más tradicionales, el uso de estas tarjetas convencionales en asociación con el comercio electrónico presenta ciertas dificultades, incluyendo dificultades concernientes a la autentificación o identificación positiva del tenedor de la tarjeta. Por ejemplo, mantener la confianza en la seguridad por parte del consumidor se ha hecho difícil con las crecientes informaciones de fraude. La aprehensión resultante se ve también alimentada por la incertidumbre del consumidor en lo que respecta a la reputación o integridad de un comerciante con el que está tratando el consumidor. La cuestionable seguridad sobre la información de la tarjeta del consumidor u otra información personal que se facilita, por lo común, conjuntamente con una transacción de comercio electrónico tradicional (por ejemplo, dirección, número de tarjeta, número de teléfono, etc.), sirve para aumentar la aprehensión aún más. Adicionalmente, los tenedores de tarjetas, comerciantes e instituciones financieras están, todos ellos, concernidos acerca de la protección frente a transacciones fraudulentas o de otro modo no autorizadas.

De acuerdo con ello, diversas redes de tarjetas de crédito han venido implementando iniciativas o programas encaminados a la salvaguardia frente al fraude. Por ejemplo, tanto Visa® como MasterCard® dan soporte a iniciativas de autentificación en virtud de las cuales el tenedor de una tarjeta es autentificado por el banco o institución financiera emisora de la tarjeta, esto es, el banco emisor. La Figura 1 ilustra una de tales iniciativas de autentificación proporcionadas a modo de ejemplo. Como se muestra en este ejemplo, un consumidor / tenedor de tarjeta 10, por ejemplo, que se sirve de un buscador web adecuado o soporte similar, está realizando una compra en línea, por ejemplo, a través de la internet, a un comerciante 20. Como se conoce en la técnica, la cadena de tratamiento del pago en el terminal trasero que se ilustra incluye una pasarela de pago opcional 30, la institución financiera o banco adquiriente 32 del comerciante, la red 34 de la tarjeta de crédito y el banco emisor 36.

A la hora del "checkout" o comprobación de salida, el consumidor 10 selecciona un método de pago apropiado basándose en las iniciativas a las que da soporte el comerciante 20. Llegados a este punto, el consumidor rellena el formulario de comprobación de salida en línea, que incluye una opción de pago, el número de la tarjeta de crédito, la fecha de caducidad, etc. Basándose en la información del pago, el comerciante 20, a través de una unidad insertable 22 instalada en su servidor, hace pasar un mensaje de petición de verificación de alta (VEReq –"verify enrollment request"–) a un directorio 38 situado en un servidor, por ejemplo, que se hace funcionar adecuadamente por la red 34 de la tarjeta de crédito. El directorio 38 incluye una base de datos que asocia a los comerciantes participantes con sus bancos adquirientes, así como una base de datos que asocia intervalos de números de tarjeta con emplazamientos o direcciones, por ejemplo, direcciones del localizador de recursos universal (URL –"universal resource locator"–), de servidores de autentificación de bancos emisores, por ejemplo, el servidor de autentificación 40 para el banco emisor 36. El mensaje de VEReq es una petición para verificar el alta de la tarjeta en el programa de autentificación, y contiene el número de tarjeta proporcionado por el consumidor 10.

Basándose en el intervalo de números de tarjeta almacenado en el directorio, el mensaje de VEReq será enviado a la dirección de URL apropiada para el servidor 40, que devuelve al comerciante 20, a través del directorio 38, una respuesta al mismo, es decir, una respuesta de alta de verificación (VERes –"verify enrollment response"–). Es decir, el servidor 40 verificará el estado de alta de la tarjeta y responderá con un mensaje de VERes al directorio 38, que se hace pasar entonces de vuelta al componente de unidad insertable 22 del comerciante.

Basándose en el mensaje de VERes (esto es, si es positivo), el componente de unidad insertable 22 del comerciante redirigirá el buscador del tenedor de la tarjeta al servidor 40 haciéndole pasar un mensaje de petición de autentificación de pagador (PAReq –"payer authentication request"–) generado por el componente de unidad insertable 22 del comerciante. El consumidor 10 completa entonces el procedimiento de autentificación directamente con el servidor 40. El servidor de autentificación 40 autentifica al consumidor / tenedor 10 de tarjeta y responde al comerciante 20 con un mensaje de respuesta de autentificación de pagador (PARes –"payer authentication response"–), que incluye una firma digital. El componente de unidad insertable 22 del comerciante valida la firma digital del PARes y extrae el estado de autentificación y otros datos especificados que se ha de utilizar por parte del comerciante 20 durante el procedimiento de autorización del pago llevado a cabo a través de la cadena de tratamiento del pago de terminal trasero. Por ejemplo, el comerciante 20 envía una autorización / transacción de venta a su pasarela de pago 30, conjuntamente con los elementos de datos recibidos desde el PARes. La pasarela de pago 30 encamina los datos al banco adquiriente 32 basándose en la especificación del adquisidor. El banco adquiriente 32 envía entonces los datos a través de la red 34 de tarjeta de crédito apropiada, al banco emisor 36 para su asiento.

Cuando se utilizan iniciativas de autentificación tales como la del ejemplo antes mencionado, la red de la tarjeta de crédito a menudo garantiza a los comerciantes que toman parte que las transacciones fraudulentas y otras devoluciones de cargo, como se conocen en la técnica, no serán responsabilidad de los comerciantes, siempre y cuando se hayan venido observando los protocolos especificados. Sin embargo, se depositan cargas considerables sobre los comerciantes a la hora de participar en las iniciativas de autentificación. Por ejemplo, la instalación convencional de la unidad insertable del comerciante puede añadir un oneroso abuso de los recursos, esto es, potencia de computación, memoria, capacidad de almacenamiento de datos, etc., que el comerciante preferiría, de otro modo, dedicar a otras tareas. A menudo, el componente de unidad insertable puede ser extremadamente grande y/o engorroso a la hora de implementarse en el servidor del comerciante. Es más, para un comerciante que participa en una pluralidad de tales programas de autentificación para múltiples redes de tarjetas de crédito, la carga puede hacerse así de grande, esto es, requerir un componente de unidad insertable independiente para cada iniciativa de autentificación de un individuo a la que desean dar soporte, especialmente teniendo en cuenta que cada red de tarjetas de crédito puede tener su propios protocolos y campos de datos particulares que se emplean en los respectivos mensajes, requisitos de formateo de datos específicos, etc.

Por otra parte, los comerciantes son responsables de permanecer al corriente de los protocolos de iniciativa, que pueden cambiar periódicamente. Es decir, a medida que los protocolos de autentificación son actualizados y/o modificados por las respectivas redes de tarjetas de crédito, los comerciantes son, de la misma manera, responsables de actualizar y/o modificar sus componentes de unidad insertable para reflejar las actualizaciones y/o cambios a que obligan las redes de tarjetas de crédito.

La presente invención contempla un nuevo y mejorado sistema y/o método que supera los problemas antes referidos y otros.

Compendio

De acuerdo con la invención, se proporciona un sistema que tiene las características de la reivindicación 1.

De acuerdo con un aspecto de la presente invención, se proporciona un sistema para dar soporte al tratamiento de autentificación de transacciones comerciales llevadas a cabo a través de una red de comunicaciones, entre consumidores y comerciantes. Los consumidores utilizan, cada uno de ellos, uno de una pluralidad de tipos diferentes de instrumentos de pago, de tal manera que el instrumento de pago que se está utilizando bien está dado de alta, o bien no está dado de alta, en un programa de autentificación que se adapta a uno de una pluralidad de protocolos de autentificación prescritos para la respectiva pluralidad de tipos diferentes de instrumentos de pago. El sistema incluye: una capa de conexión para conectar con los comerciantes con el fin de intercambiar comunicaciones con ellos, de tal manera que la capa de conexión recibe de los comerciantes información de pago para las transacciones, incluyendo la información de pago para cada transacción un número que identifica el instrumento de pago concreto que se está utilizando; una capa de unidad insertable, que incluye una pluralidad de componentes de unidad insertable, de tal modo que cada componente de unidad insertable administra uno diferente de los programas de autentificación de acuerdo con los protocolos de autentificación prescritos, a fin de obtener una determinación de autentificación para las transacciones; y una capa de distribución, que reside entre la capa de conexión y la capa de unidad insertable, de tal manera que la capa de distribución encamina las comunicaciones entre la capa de conexión y componentes de unidad insertable seleccionados de la capa de unidad insertable, de forma tal, que la información de pago para cada transacción es encaminada al componente de unidad insertable responsable de administrar el programa de autentificación para el instrumento de pago particular que se utiliza para esa transacción.

De acuerdo con aún otro aspecto de la presente invención, se proporciona un sistema para procesar la autentificación de un consumidor que está utilizando uno de entre una pluralidad de tipos diferentes de instrumentos de pago para llevar a cabo una transacción comercial a través de una red de comunicaciones, con un comerciante. El instrumento de pago que se está utilizando bien está dado de alta, o bien no está dado de alta, en un programa de autentificación que se adapta a uno de entre una pluralidad de protocolos de autentificación prescritos para la

pluralidad respectiva de tipos diferentes de instrumentos de pago, por parte de las redes de pago que dan soporte a los mismos. El sistema incluye: medios para obtener del comerciante información de pago para la transacción, de tal manera que la información del pago incluye un número que identifica el instrumento de pago concreto que se está utilizando; medios para determinar a partir de la información del pago el tipo de instrumento de pago que se está utilizando; medios para obtener una determinación de autentificación para la transacción de acuerdo con los protocolos de autentificación prescritos para el tipo determinado de instrumento de pago que se está utilizando; y medios para remitir de vuelta al comerciante la determinación de autentificación obtenida.

Numerosas ventajas y beneficios de la presente invención resultarán evidentes para las personas con conocimientos ordinarios de la técnica a partir de lectura y comprensión de la presente memoria.

Breve descripción de los dibujos

La presente invención puede tomar forma en diversos componentes y disposiciones de componentes, y/o en diversas etapas y disposiciones de etapas. Los dibujos son únicamente para propósitos de ilustrar realizaciones preferidas, y no han de interpretarse como limitativos de la invención.

La Figura 1 es un diagrama de bloques que ilustra una transacción de comercio electrónico típica que se lleva a cabo de acuerdo con una iniciativa / programa de autentificación proporcionado a modo de ejemplo, de una red de tarjetas de crédito.

La Figura 2 es una ilustración esquemática que muestra una vista general de alto nivel de un tratamiento proporcionado a modo de ejemplo de una transacción comercial autentificada de acuerdo con aspectos de la presente invención.

La Figura 3 es un diagrama de bloques que ilustra un servidor de comerciante proporcionado a modo de ejemplo, y un sistema de tratamiento de autentificación de comerciante proporcionado a modo de ejemplo, de acuerdo con aspectos de la presente invención.

Descripción detallada de realizaciones preferidas

Por claridad y simplicidad, la presente memoria hará referencia a elementos de red estructurales y/o funcionales, entidades y/o instalaciones, normas, protocolos y/o servicios relevantes, y otros componentes que son comúnmente conocidos en la técnica, sin ninguna explicación detallada adicional por lo que respecta a su configuración o funcionamiento, excepto en la medida en que los mismos hayan sido modificados o alterados de acuerdo con, y/o para adaptarse a, aspectos de la presente invención.

De acuerdo con una realización preferida, la presente invención sirve como sistema de tratamiento de comerciante centralizado para pagos autentificados, que permite a un comerciante adaptarse de forma segura y fácil a la autentificación de consumidores y/o tenedores de tarjetas de acuerdo con una variedad de iniciativas de autentificación implementadas por redes de tarjetas de crédito, y procesar las transacciones electrónicas a través de cualquier red de pago utilizando una única plataforma. También hace posible a los comerciantes procesar estos pagos con independencia de la red de pago a través de la cual hayan de ser encaminados, con una única implementación. En otra versión, esto se lleva a cabo utilizando software de comunicación ‘de cliente delgado’ [de bajo nivel de tratamiento] que enlaza la información con un sistema de tratamiento de autentificación de comerciante (MAPS –“merchant authentication processing system”–) centralizado bajo demanda. Es más, este les permite a ellos o a una fuente de fondos utilizar la infraestructura de tratamiento de pago subyacente para procesar sus instrumentos de crédito / débito en los emplazamientos del comerciante que toma parte.

Las ventajas con respecto a las fuentes de fondos son: la capacidad de autentificar a los usuarios y de procesar todas las transacciones electrónicas a través de una única plataforma; la capacidad de procesar sin interrupciones los pagos utilizando cualquier red de pago dada; una reducción en los costes de tratamiento; uso incrementado de su instrumento de crédito / débito; aceptación incrementada de su instrumento de crédito / débito; la capacidad de enviar peticiones de pago y de autorización autentificadas a cualquier red; la facultad de recibir estadísticas detalladas acerca del comportamiento de compra de los consumidores. De la misma manera, existen ventajas para el comerciante, que incluyen: la capacidad de adecuarse a, participar en, y disfrutar de, los beneficios de una variedad de iniciativas de autentificación; la capacidad de autentificar a consumidores que utilizan diferentes vehículos de pago o tarjetas de crédito, con lo que se evita perder ventas; y la protección frente al fraude, si bien no están limitadas por estas.

El enfoque detallado en la presente memoria proporciona una solución segura, regulable en escala y modular para que los comerciantes participen en, y den soporte a, diversas iniciativas de autentificación de pago, tales como, por ejemplo, la 3-D Secure Verified by Visa (VbV) (verificación segura 3-D por Visa), de Visa, y la SecureCode and/or Secure Payment Application (SPA) (aplicación de código seguro y/o de pago seguro) de MasterCard. Estas proporcionan a las pasarelas de pago, adquisidores, proveedores de servicios de comerciantes (MSP –“merchant service providers”–) y organizaciones de ventas independientes (ISO) una manera fácil y eficaz de proporcionar a sus comerciantes medios para la autentificación del tenedor de una tarjeta, según se definen por diversos programas de autentificación, por ejemplo, el VbV, SecureCode, SPA, etc.

Haciendo referencia a la Figura 2, se ilustra en ella esquemáticamente una vista general de alto nivel de una transacción comercial proporcionada a modo de ejemplo, que se lleva a cabo de acuerdo con un aspecto de la presente invención. Por medio de una computadora, un consumidor 50 compra de un comerciante en línea 60, utilizando un instrumento de pago seleccionado. Una vez que se ha completado la transacción, se envían los detalles de la transacción desde el comerciante 60 a un proveedor de servicios de tratamiento de transacciones (TPSP –"transaction processing service provider"–) 70, el cual formatea y encamina los diversos mensajes y adopta otras acciones definidas en nombre del comerciante 60, de conformidad con los protocolos de autentificación prescritos por la red de tratamiento de pago a la que pertenece el instrumento de pago que se está utilizando para la transacción. Por ejemplo, tal como se muestra, existe una red de tratamiento de pago 70 con tarjeta de ATM, una primera red de tratamiento de pago 72 con tarjeta de crédito, para un primer tipo o marca de tarjeta de crédito, una segunda red de tratamiento de pago 74 con tarjeta de crédito, para un segundo tipo o marca de tarjeta de crédito, una red de tratamiento de pago 76 con tarjeta de cheques, y una red de tratamiento 78 de tarjeta de crédito de etiqueta privada, todas las cuales dan soporte, opcionalmente, a diferentes protocolos de autentificación. Tal como se muestra, el TPSP 70 obtiene, opcionalmente, transacciones del comerciante y las distribuye a las redes de tratamiento de pago asociadas, por ejemplo, para su autentificación directa por la entidad que emite el instrumento de pago utilizado en la transacción. Habiendo obtenido una determinación de autentificación, el proveedor de servicios de autentificación 70 remite entonces esta determinación de vuelta al comerciante 60, de tal manera que puede ser incluida cuando la transacción se facilita, por parte del comerciante 60, a la infraestructura de tratamiento de pago subyacente establecida, por ejemplo, a través de una pasarela de pago opcional 80.

Más concretamente, con referencia a la Figura 3, se muestran en ella un servidor 100 proporcionado a modo de ejemplo, que es hecho funcionar por un comerciante en línea, o bajo conexión, y un sistema de tratamiento de autentificación de comerciante (MAPS –"merchant authentication processing system"–) 200 proporcionado a modo de ejemplo. El servidor 100 de comerciante incluye una función de tratamiento de comprobación de salida 102, una función de tratamiento de pago 104 y una operativa 106 de cliente delgado destinadas a proporción una interrelación de colaboración entre el servidor 100 y el MAPS 200. El servidor 100 alberga, de forma adecuada, un sitio web accesible, a través de una red de comunicaciones (por ejemplo, la internet), por los consumidores / tenedores de tarjetas, a fin de llevar a efecto transacciones comerciales, esto es, adquirir bienes y/o servicios. Es decir, un consumidor / tenedor de tarjeta que utiliza un buscador web apropiado o aplicación similar puede conectarse al servidor 100 a través de la internet para realizar compras en el sitio web albergado.

De manera adecuada, cuando un consumidor / tenedor de tarjeta está realizando compras, se invoca la función de tratamiento de comprobación de salida 102, con lo que se proporciona al buscador web del consumidor una página web de comprobación de salida por la cual se establece y/o presenta la cantidad de la transacción (esto es, la cantidad total del pago debido), y se recoge la información del pago. La función de tratamiento de comprobación de salida 102 da soporte al pago con una pluralidad de tipos diferentes de instrumentos de pago, por ejemplo, tarjetas de crédito y/o de débito, pertenecientes a diferentes redes de tratamiento de pago, por ejemplo, Visa®, MasterCard®, etc. Es decir, el consumidor / tenedor de tarjeta selecciona, opcionalmente, el tipo concreto de instrumento de pago que se va a utilizar para la transacción comercial de entre una pluralidad de tipos de instrumento de pago a que se da soporte. Adicionalmente, la función de tratamiento de comprobación de salida 102 se utiliza también para recoger del consumidor / tenedor de tarjeta el número de la tarjeta, la fecha de caducidad y otros datos relevantes.

La función de tratamiento de pago 104 facilita las transacciones completadas a la infraestructura de tratamiento de pago subyacente establecida (esto es, pasarela de pago, banco adquiriente, red de tratamiento del pago, banco emisor, etc.) de la forma habitual según se haya prescrito por las diversas redes de tratamiento de pago.

El cliente delgado 106 del comerciante se utiliza para comunicar elementos de datos de la transacción, tales como el número de tarjeta, la cantidad de la transacción, etc., entre el sitio web del comerciante y el MAPS 200. El cliente delgado no está al corriente de la lógica o protocolos de tratamiento específicos prescritos para cada iniciativa de autentificación de pago. De forma adecuada, el cliente delgado 106 es un pequeño componente de software instalado en el servidor 100 del comerciante, de aproximadamente 50 kilobytes de tamaño. Alternativamente, se dispone también de las siguientes opciones para conectarse al MAPS 200, a fin de atender a diferentes comerciantes dependiendo del volumen de tratamiento de transacciones del comerciante, su experiencia técnica, la disponibilidad de recursos y las normas de software: (i) una implementación 'de conexión fácil', como se denomina en la presente memoria, esto es, un cliente con comerciante sin software, y (ii) una implementación 'de conexión directa', como se denomina en esta memoria, es decir, una integración directa dentro del MAPS 200. Sin embargo, esta solución de cliente delgado proporciona al comerciante un objeto de software delgado (esto es, pequeño) (por ejemplo, de aproximadamente 50 kilobytes), que se utiliza por el comerciante para comunicarse con el MAPS 200. Utilizando el cliente delgado 106, el comerciante puede participar dentro de las diversas iniciativas de autentificación de pago, por ejemplo, VbV, SPA, etc., sin necesidad de una reprogramación significativa del servidor 100 o del sitio web. De forma adecuada, el cliente delgado 106 se encuentra disponible como objeto de COM o componente de Java que está integrado con el proceso de gestión de transacción establecido del comerciante.

El software de cliente delgado es utilizado por los comerciantes para comunicarse de forma segura con el MAPS. El software de cliente delgado se utiliza para formatear pares de nombre / valor en el formato de mensaje de MAPS

requerido, y para comunicar de forma segura el mensaje al sistema de MAPS. El cliente delgado no mantiene ninguna lógica de tratamiento comercial específica para autentificación de pago. El cliente delgado da soporte a las siguientes características: comunicación segura al MAPS 200, formateo de datos al formato de mensaje específico del MAPS, y habilitación de los comerciantes para acceder a los datos de respuesta.

De forma adecuada, la arquitectura del cliente delgado 106 incluye una capa de petición 110 y una capa de respuesta 112 que se asientan encima de una capa 114 de formateo de mensajes, que se asienta encima de una capa de comunicación 116. La capa de petición 110 proporciona una interfaz a la que puede accederse por parte del sitio web del comerciante para proporcionar datos al cliente delgado 106 en la forma de pares de nombre / valor. La capa de petición 110 también expone funciones para que el comerciante envíe mensajes a un MAPS 200 concreto. La capa de respuesta 112 proporciona una interfaz para remitir de vuelta las respuestas al sitio web, por ejemplo, remitidas de vuelta como una respuesta de llamada a función a una instrucción de envío de mensaje. La capa 114 de formateo de mensajes formatea y traduce el tráfico entre las capas de petición y de respuesta, 110 y 112, que emplean el formato de pares de nombre / valor, y la capa de comunicación 116, que emplea, de manera adecuada, un formato XML para comunicarse con el MAPS 200. La capa de comunicación 116 proporciona capacidad de conexión con el MAPS 200, por ejemplo, a través del HTTPS (esto es, el protocolo de transferencia de hipertexto sobre capa de base segura (SSL –“secure socket layer”–) –“hypertext transfer protocol over SSL”–).

El MAPS 200 es un componente nuclear dentro del sistema. El MAPS 200 proporciona a los comerciantes la capacidad funcional de participación en los diversos programas de autentificación e iniciativas diferentes a los que dan soporte las redes de tratamiento de pago. De forma adecuada, la arquitectura del MAPS 200 es extensible al soporte de las entregas existentes y otras nuevas de iniciativas de pago ya existentes, sin que ello requiera una reescritura total del software, y, de la misma manera, se adapta a la adición de nuevas iniciativas de autentificación. Esta solución conduce a una fácil implementación en el nivel del sitio web del comerciante, esto es, aquel en el que la lógica de tratamiento y la gestión de los mensajes prescritas por las iniciativas son controladas en un emplazamiento central, en lugar de en el nivel del comerciante individual. Es decir, cualesquiera cambios o adiciones implementados no afectan a los comerciantes individuales.

El MAPS 200 proporciona una infraestructura segura para procesar transacciones, basada en especificaciones de iniciativa de autentificación para pago. El MAPS 200 proporciona software extensible que puede dar soporte sin interrupciones a revisiones futuras de las iniciativas de autentificación de pago ya existentes y de nuevas iniciativas de autentificación de pago. Preferiblemente, el MAPS 200 proporciona una abstracción completa en cuanto a cómo se implementa cada iniciativa de autentificación de pago, por lo que se proporciona un único emplazamiento central para cualesquiera cambios. De forma adecuada, el MAPS 200 se programa con software de Java para proporcionar la capacidad funcional descrita. La arquitectura de software del MAPS incluye las siguientes capas: una capa 210 de capacitación de conexión que se asienta encima de una capa 220 de distribución de mensajes, la cual se asienta encima de una capa 230 de unidad insertable, y una capa 240 de conexión externa. La capa de conexión externa 240 proporciona una interfaz genérica que es utilizada por el MAPS 200 para comunicarse con los recursos exteriores, por ejemplo, el directorio o elemento similar según se prescribe por los diversos protocolos de autentificación.

La capa de capacitación de conexión 210 proporciona una capa genérica para que entidades externas tales como comerciantes se conecten a una transacción de autentificación de pago específica y la procesen. La capa de capacitación de conexión 210 da soporte a los siguientes conectadores: un servidor HTTPS 212; un ‘conectador directo’ 214, tal y como se denomina en esta memoria; y un ‘conectador fácil’ 216, tal y como se denomina en esta memoria; así como ‘otro conectador’ 218 opcional, tal y como se denomina en esta memoria.

El servidor HTTPS 212 recibe y/o envía mensajes de HTTP y los comunica hacia y/o desde la capa 220 de distribución de mensajes. Este conectador se utiliza por parte cliente delgado 106 para comunicarse con el MAPS 200. El conectador directo 214 proporciona una interfaz de Java que puede ser utilizada por un comerciante, que se integra con el MAPS 200 utilizando la solución de conexión directa. Este conectador expone las interfaces de Java apropiadas que pueden ser utilizadas por el comerciante durante la integración. Los mensajes recibidos / enviados utilizando este conectador son también comunicados hacia / desde la capa 220 de distribución de mensajes. El conectador fácil 216 proporciona un servidor web que se utiliza para comunicarse con el distribuidor de mensajes y también para comunicarse con el tenedor de la tarjeta. Este conectador actúa como interfaz con el tenedor de la tarjeta para llevar a cabo la capacidad funcional de comerciante y actúa como interfaz con el distribuidor de mensajes para comunicar los mensajes relevantes. De forma adecuada, el otro conectador 218 permite a la capa de capacitación de conexión 210 ser expandida para dar soporte a otras opciones de comunicación y de integración personalizada.

La implementación de múltiples tipos de conectador proporciona a los comerciantes múltiples maneras de integrarse y participar en el seno de las diversas iniciativas de autentificación. Al proporcionar múltiples soluciones de integración, es posible dar soporte a una amplia variedad de comerciantes, dependiendo de la experiencia técnica del comerciante, de la disponibilidad de recursos y del volumen de tratamiento de transacciones. Es decir, además de la solución de cliente delgado, se encuentran también disponibles, opcionalmente, para los comerciantes una solución ‘de conexión directa’ y una ‘de conexión fácil’.

La solución de conexión directa se proporciona a los comerciantes que insisten en, o, de otro modo, desean, albergar y gestionar el producto; tales comerciantes, por ejemplo, pueden ser comerciantes con un elevado volumen de transacciones y/o comerciantes que tienen los recursos técnicos necesarios para albergar y gestionar el producto. El comerciante puede utilizar llamadas de Java directas para actuar como interfaz con el MAPS 200 y comunicar los mensajes de XML apropiados. La interfaz de conexión directa se encuentra también disponible a través de un servidor de base local proporcionado como parte del MAPS 200. Los comerciantes que utilizan una plataforma de software distinta de la Java pueden hacer uso del servidor de base local. Con la solución de conexión directa, los comerciantes aportan su propio hardware y/o software. En el extremo opuesto del espectro, la solución de conexión fácil se proporciona como una solución de integración sin software para los comerciantes que no desean instalar el cliente delgado 106. Utilizando la solución de conexión fácil, el comerciante redirige al tenedor de la tarjeta al servidor web de conexión fácil del MAPS. El servidor web actúa en representación del sitio web del comerciante y se comunica con el MAPS 200 para proporcionar el tratamiento apropiado para la iniciativa de autentificación apropiada. Con esta solución, el comerciante redirige al tenedor de la tarjeta utilizando POST de HTTPS y recibe las respuestas en un URL de respuesta especificado. Los redireccionamientos de HTTP han de llevarse a cabo por medio del buscador del tenedor de la tarjeta. Utilizando la solución de conexión fácil, el comerciante puede poner una nota apropiada una vez que el tenedor de la tarjeta / consumidor ha proporcionado al comerciante los datos de pago apropiados, tales como un número de tarjeta de crédito, una fecha de caducidad, etc. El comerciante recibe la respuesta de autentificación en el URL especificado, dentro de un campo de URL de respuesta designado en la nota.

La capa 220 de distribución de mensajes es un componente dentro de la arquitectura de software que facilita la regulación en escala, la redundancia y una elevada disponibilidad y velocidad de tratamiento de las transacciones. De forma adecuada, la capa 220 de distribución de mensajes se ha desarrollado utilizando especificaciones de la Edición para Empresas de Java 2 (J2EE –"Java 2 Enterprise Edition"–) relativas al tratamiento de las transacciones. Es preferible una aplicación de distribución de mansajes de pequeña impronta, configurada para encaminar mensajes de XML a componentes de unidad insertable específicos de la capa 230 de unidad insertable para un tratamiento adecuado de las transacciones.

La capa 230 de unidad insertable incluye una pluralidad de componentes de unidad insertable 232 de iniciativa para autentificación individuales, que se encuentran a la escucha de la capa 220 de distribución de mensajes, a la espera de un tipo de mensaje específico. El componente de unidad insertable 232 respectivo es activado por la capa 220 de distribución de mensajes, que envía mensajes al componente de unidad insertable 232 especificado basándose en el tipo de instrumento de pago que se está utilizando para la transacción que se está procesando. Por ejemplo, como se muestra, el MAPS 200 incluye, opcionalmente, componentes de unidad insertable 232 para Visa®, MasterCard® y otros instrumentos de pago. Es de destacar que los componentes de unidad insertable 232 son actualizados, intercambiados de otro modo manipulados libre y fácilmente, según se desee para adecuarse a una nueva versión de iniciativas de autentificación ya existentes, o bien componentes de unidad insertable adicionales son libre y fácilmente añadidos para adaptarse a nuevas iniciativas, sin necesidad de ninguna alteración adicional en el MAPS 200 o en el lado del comerciante. De esta manera, los comerciantes se mantienen automáticamente de conformidad con las últimas iniciativas de autentificación, sin tener que volver a trabajar los protocolos de tratamiento de autentificación en su servidor 100. Por otra parte, a medida que se introducen y/o se desean otras mejoras en el tratamiento del pago, por ejemplo, la conversión de moneda, pueden desarrollarse, de la misma manera, componentes de unidad insertable acordes y sencillamente añadirse a la capa 230 de unidad insertable del MAPS 200, con lo que se proporciona al comerciante la capacidad funcional de tratamiento de pago concreta.

De manera adicional, la capa 230 de unidad insertable también da soporte, opcionalmente, a diversas aplicaciones de gestión y/o administrativas (no mostradas). Por ejemplo, puede ponerse a disposición de los proveedores de servicios del comerciante (MSPs –"merchant service providers"–) un módulo de aplicación de registro de comerciantes, a fin de registrar a sus comerciantes dentro de las iniciativas de autentificación de pago apropiadas. De forma adecuada, la aplicación de registro de comerciantes ofrece una aplicación basada en web en la que los comerciantes, basándose en comunicaciones recibidas desde sus MSPs, pueden registrarse ellos mismos y descargar software apropiado y documentación de integración relacionada. La aplicación de registro de comerciantes también proporciona un control basado en clave de registro / licencia al MSP, de tal manera que el MSP puede comunicar una clave de licencia al comerciante, que se utilizará para autentificar al comerciante durante el registro y la descarga. Opcionalmente, los elementos de datos recogidos de los comerciantes pueden ser personalizados según se desee por el MSP.

Una aplicación de administración de MSP opcional proporciona al MSP una aplicación basada en web que se utiliza para administrar a los comerciantes. La aplicación de administración de MSP puede, por ejemplo, proporcionar las siguientes características: habilitar / inhabilitar a los comerciantes para el uso del MAPS 200; mantener la información del perfil del comerciante; etc. Se accede, opcionalmente, a la aplicación de administración de MSP directamente a través de interfaces de programa de aplicación (APIs –"application program interfaces"–) basados en XML/HTTP, que pueden también ser utilizados para integrarse con otros sistemas. De manera adicional, una aplicación de autoservicio de comerciante permite al comerciante acceder a su información de perfil a través de la web. Por ejemplo, la aplicación de autoservicio de comerciante ofrece, opcionalmente, las siguientes características: autogestión del perfil; acceso al historial de transacciones; acceso a los registros de mensaje primarios relacionados

con los procedimientos de autentificación; etc. Puede accederse, similarmente, a la aplicación de autoservicio de comerciante directamente a través de APIs basados XML/HTTP, que se utilizan también, opcionalmente, para integrarse con otros sistemas.

Como otra opción, una aplicación de informe a MSP proporciona una aplicación basada en web para que los MSPs vean listados de transacciones consolidadas e individuales. Por ejemplo, pueden proporcionarse, opcionalmente, los siguientes informes como parte de la aplicación de informe a MSP: informes de volumen de cuenta / dólares de transacciones consolidadas; informes de transacciones individuales; registros de mensaje primarios; informes de registro de comerciantes y/u otros informes personalizados.

Como se apreciará por las personas con conocimientos ordinarios de la técnica, el MAPS 200 proporciona un método para autentificar a un consumidor utilizando uno de una pluralidad de tipos diferentes de instrumentos de pago (por ejemplo, tarjetas de crédito / débito), con el fin de llevar a cabo una transacción comercial a través de una red de comunicaciones con un comerciante que emplea el MAPS 200. El instrumento de pago puede bien estar dado de alta, o bien no estar dado de alta, en un programa de autentificación de conformidad con uno de una pluralidad de protocolos de autentificación prescritos para la pluralidad respectiva de tipos diferentes de instrumentos de pago, por redes de pago que dan soporte a los mismos.

De forma adecuada, mediante la solución de cliente delgado (o, alternativamente, las soluciones de conexión directa o de conexión fácil), el MAPS 200 obtiene del servidor 100 del comerciante información de pago para la transacción. De manera adecuada, la información del pago incluye un número que identifica el instrumento de pago concreto que se está utilizando (esto es, el número de la tarjeta de crédito), una fecha de caducidad, detalles de la transacción (es decir, la cantidad de la transacción, etc.) y otros datos pertinentes. En el caso de la solución de cliente delgado, la información del pago se obtiene del sitio o página web del comerciante a través de la capa de petición 110, en forma de pares de nombre / valor. La capa de petición 110 hace pasar la información del pago a la capa 114 de formateo de mensajes, que la traduce a un mensaje formateado en XML y hace pasar este a la capa de comunicación 116. La capa de comunicación 116 hace pasar entonces el mensaje en el formato XML al MAPS 200, a través del servidor HTTPS 212 de la capa de capacitación de conexión 210.

Al recibir la información del pago, el MAPS 200 determina el tipo de instrumento de pago que se está utilizando a partir de la información de pago. En particular, la red de tratamiento de pago a la que pertenece la tarjeta de crédito / debido puede determinarse por el número de la tarjeta, como se conoce en la técnica.

Opcionalmente, el MAPS 200 la determina a partir del estado de alta del instrumento de pago concreto que se está utilizando para la transacción. Por ejemplo, el MAPS 200 puede mantener una memoria caché local o base de datos de números de tarjeta que identifica los instrumentos de pago dados de alta para su participación en los diversos programas y/o iniciativas de autentificación. Si el instrumento de pago concreto que se está utilizando no está dado de alta en un programa de autentificación particular para el tipo determinado de instrumento de pago, entonces puede ponerse fin al tratamiento en este punto, de manera que el MAPS 200 remite un mensaje o datos de ‘no dado de alta’ de vuelta al cliente delgado 106 instalado en el servidor 100 del comerciante. De acuerdo con ello, el cliente delgado 106 hace pasar esta información a la función de tratamiento de pago 104 para ser empaquetada con los datos de transacción, a fin de facilitar la transacción, completada, a la infraestructura de tratamiento de pago subyacente establecida. Ha de apreciarse que el mensaje o datos de ‘no dado de alta’ que se remite de vuelta, al igual que toda la información remitida de vuelta al comerciante, son proporcionados por el MAPS 200 a través del cliente delgado 106 (esto es, a través de la capa de comunicación 116, de la capa 114 de formateo de mensajes y de la capa de respuesta 112), de tal manera que emergen ya formateados y/o de otro modo de conformidad con los protocolos de autentificación apropiados prescritos, de modo que el comerciante no tiene que manipular los datos adicionalmente, antes de facilitarlos a la infraestructura de tratamiento de pago subyacente establecida.

Alternativamente, si el instrumento de pago concreto que se está utilizando está dado de alta en un programa de autentificación para el tipo determinado de instrumento de pago, entonces la información del pago se hace pasar a la capa 220 de distribución de mensajes, la cual la encamina al componente de unidad insertable 232 de la capa 230 de unidad insertable. El componente de unidad insertable 232 maneja entonces, administra y/o de otro modo ejecuta los procedimientos establecidos prescritos para el programa de autentificación respectivo, que emplean los protocolos y/o lógica apropiados para obtener una determinación de autentificación para la transacción. Por ejemplo, el componente de unidad insertable 232 formatea y encamina mensajes de conformidad con los protocolos de autentificación prescritos para el tipo determinado de instrumento de pago que se está utilizando. Una vez obtenida la determinación de autentificación, el MAPS 200 remite de vuelta la misma al servidor 100 del comerciante.

De manera adecuada, los componentes de unidad insertable 232 son programados para administrar cualquiera de una variedad de protocolos de autentificación, tal como pueden haberse prescrito para diferentes tipos de instrumentos de pago a los que se da soporte por parte de las diversas redes de tratamiento de pago. Por ejemplo, para dar acomodo a una iniciativa de autentificación concreta, un componente de unidad insertable 232 particular formatea y encamina, opcionalmente, un mensaje a una entidad emisora, por ejemplo, un banco emisor que ha emitido el instrumento de pago concreto que se está utilizando para la transacción, solicitando a la entidad emisora que confirme el estado de alta del instrumento de pago concreto que se está utilizando para la transacción. Al obtener una respuesta al mensaje de petición de alta desde la entidad emisora, la información puede ser remitida de

vuelta al servidor 100 del comerciante de la misma manera que si el MAPS 200 hubiera llevado a cabo, él mismo, la comprobación del alta.

Adicionalmente, una vez determinado el estado de alta como positivo, el componente de unidad insertable 232 operativo formatea y encamina, opcionalmente, un segundo mensaje al comerciante, de tal manera que el consumidor / tenedor de la tarjeta es redirigido a la entidad emisora para completar su autentificación directamente con esta, con lo que se realiza la determinación de autentificación. Una respuesta que contiene la determinación de autentificación realizada por la entidad emisora, es entonces remitida de vuelta de conformidad con las instrucciones de encaminamiento contenidas en el segundo mensaje, del modo que se obtienen por el MAPS 200. De forma adecuada, las instrucciones de encaminamiento incluyen un localizador de recursos universal (URL) que dirige la respuesta de vuelta al MAPS 200. Opcionalmente, el componente de unidad insertable 232 verifica que se ha obtenido la respuesta al segundo mensajes desde la entidad emisora, por ejemplo, al comprobar una firma digital incorporada a la respuesta. El MAPS 200 está también, opcionalmente, equipado para detectar y/o evaluar cualitativamente el nivel y/o el tipo de autentificación empleados para llegar a la determinación de autentificación, y esta información puede ser comunicada al comerciante o a terceros.

A fin de adaptarse adicionalmente a otra iniciativa de autentificación seleccionada, un componente de unidad insertable 232 concreto es, opcionalmente, programado de manera tal, que el MAPS 200 está equipado para añadir dinámicamente uno o más campos de datos a la página web del comerciante, al objeto de llevar la página web del comerciante a conformidad con protocolos de autentificación prescritos para el tipo determinado de instrumento de pago. De manera adicional, pueden añadirse dinámicamente otros elementos y/o campos de datos, opcionalmente, por ejemplo, para proporcionar conversión de moneda, etc.

De manera adecuada, el MAPS 200 incluye, adicionalmente, una base de datos (no mostrada) en la que se mantienen registros históricos de transacciones procesadas por el MAPS 200. Puede accederse entonces, opcionalmente, a los registros históricos por parte de los comerciantes o MSPs para llevar a cabo operaciones de proceso auditor y/o de reconciliación.

Ha de apreciarse que la anterior descripción y las figuras que la acompañan son de naturaleza meramente ejemplar. En particular, pueden emplearse otras configuraciones de hardware y/o de software concebibles para una persona con conocimientos ordinarios de la técnica, para llevar a efecto la presente invención, y puede, de la misma manera, darse soporte a otras iniciativas de autentificación de pago similares, esto es, distintas de las VbV y SPA proporcionadas a modo de ejemplo, sin apartarse del alcance de la presente invención. No obstante, la arquitectura descrita en la presente memoria alcanza ciertos beneficios. Por ejemplo, la disponibilidad de múltiples soluciones de implementación (esto es, de cliente delgado, de conexión directa y de conexión fácil) permite un ajuste personalizado a una variedad de comerciantes equipados de distintas maneras, basándose en su volumen de tratamiento de transacciones, experiencia técnica, recursos de software y/o de hardware, etc. Por otra parte, el MAPS 200 centralizado elimina el lastre que, de otro modo, se colocaría sobre el servidor 100 del comerciante al tener que dar soporte a múltiples iniciativas de tratamiento de pago, proporcionando una abstracción sustancialmente completa por lo que respecta a las reglas y lógica de tratamiento de la iniciativa de autentificación de pago concreta, y, con su capa de unidad insertable 230 extensible, procura disponibilidad a múltiples iniciativas de autentificación de pago con una única implementación en el lado del comerciante.

Adicionalmente, en el caso de que el comerciante emplee un MSP para llevar a cabo tareas de tratamiento de pago y/u otras relacionadas con estas en nombre del comerciante, debe apreciarse que el MSP puede, efectivamente, ponerse en el lugar del comerciante en lo que se refiere al MAPS 200. Por ejemplo, en lugar de instalar el cliente delgado 106 en el servidor 100 del comerciante individual, este puede ser instalado en el servidor del MSP, que puede utilizarlo en representación de un único comerciante o de múltiples comerciantes a los que da servicio el MSP. Es decir, la información y/o los datos hacia y/o desde los respectivos comerciantes serán, primeramente, encaminados a través del servidor de MSP, en el que son expuestos a, y/o interaccionan con, el cliente delgado 106 instalado en él, esencialmente de la misma manera que se ha descrito en lo anterior.

La invención se ha descrito con referencia a las realizaciones preferidas. Obviamente, se les ocurrirán a otros modificaciones y alteraciones con la lectura y la comprensión de esta memoria. Es la intención que la invención sea interpretada de manera que incluya todas estas modificaciones y alteraciones, en la medida en que entren dentro del alcance de las reivindicaciones que se acompañan y de los equivalentes de las mismas.

REIVINDICACIONES

1.- Un sistema para tratar la autentificación de un consumidor (50) a través de una computadora de un sistema de tratamiento de autentificación de comerciante, MAPS, centralizado, (200), el cual utiliza uno de una pluralidad de tipos diferentes de instrumentos de pago para llevar a cabo una transacción comercial a través de una red de comunicaciones, con un servidor (100) que es hecho funcionar por un comerciante en línea, de tal manera que el instrumento de pago que se está utilizando bien está dado de alta, o bien no está dado de alta, en un programa de autentificación de conformidad con uno de una pluralidad de protocolos de autentificación prescritos para la pluralidad respectiva de tipos diferentes de instrumentos de pago por parte de las redes de pago (70, 72, 74, 76, 78) que dan soporte a los mismos, de tal modo que el sistema comprende:

el servidor (100), que incluye una de una pluralidad de soluciones de integración disponibles, de tal modo que las soluciones de integración disponibles incluyen un cliente delgado (106), una conexión directa y una conexión fácil,

de manera que el cliente delgado (106) es susceptible de hacerse funcionar para formatear pares de nombre / valor en XML, de acuerdo con un formato de mensaje de MAPS requerido, y comunicar de forma segura el mensaje al MAPS (200) mediante HTTPS, de tal modo que el cliente delgado (106) es un objeto de COM o un componente de Java,

de forma que la conexión directa es una conexión con la que el comerciante puede utilizar llamadas de Java directas para actuar como interfaz con el MAPS (200) y comunicar mensajes de XML, y

de tal manera que la conexión fácil es una conexión con la que el comerciante puede redirigir al consumidor (50) utilizando postes de HTTPS a través del buscador del consumidor, a un servidor web de conexión fácil del MAPS (200), y puede recibir respuestas en un URL de respuesta específico, de tal modo que el servidor web actúa en representación del comerciante y se comunica con el MAPS (200) para proporcionar un tratamiento adecuado para una iniciativa de autentificación apropiada,

siendo el servidor (100) susceptible de hacerse funcionar para obtener información de pago para la transacción del consumidor (50) y remitir la información de pago al MAPS (200) utilizando la solución de integración incluida; y

de forma que el MAPS (200) incluye un servidor HTTPS (212), un servidor de conectador directo (214) y una capa (220) de distribución de mensajes, configurada para encaminar mensajes de XML a componentes de unidad insertable específicos de una capa insertable (230), de tal modo que la capa de unidad insertable (230) incluye una pluralidad de componentes de unidad insertable de iniciativa de autentificación individual, de tal manera que el MAPS (200) es susceptible de hacerse funcionar para:

obtener la información de pago para la transacción del servidor (100), de tal forma que dicha información de pago incluye un número que identifica el instrumento de pago concreto que se está utilizando;

determinar el tipo de instrumento de pago que se está utilizando a partir de la información de pago, de forma que un componente de unidad insertable específico (232) es activado por la capa (220) de distribución de mensajes, que envía mensajes al componente de unidad insertable (232) especificado basándose en el tipo de instrumento de pago que se está utilizando para la transacción, de modo que el componente de unidad insertable específico (232) formatea y encamina los mensajes de acuerdo con protocolos de autentificación prescritos para el instrumento de pago concreto que se está utilizando;

obtener una determinación de autentificación de una de las redes de pago (70, 72, 74, 76, 78) para la transacción de acuerdo con los protocolos de autentificación prescritos para el tipo determinado de instrumento de pago que se está utilizando; y

remitir de vuelta la determinación de autentificación obtenida al servidor (100).

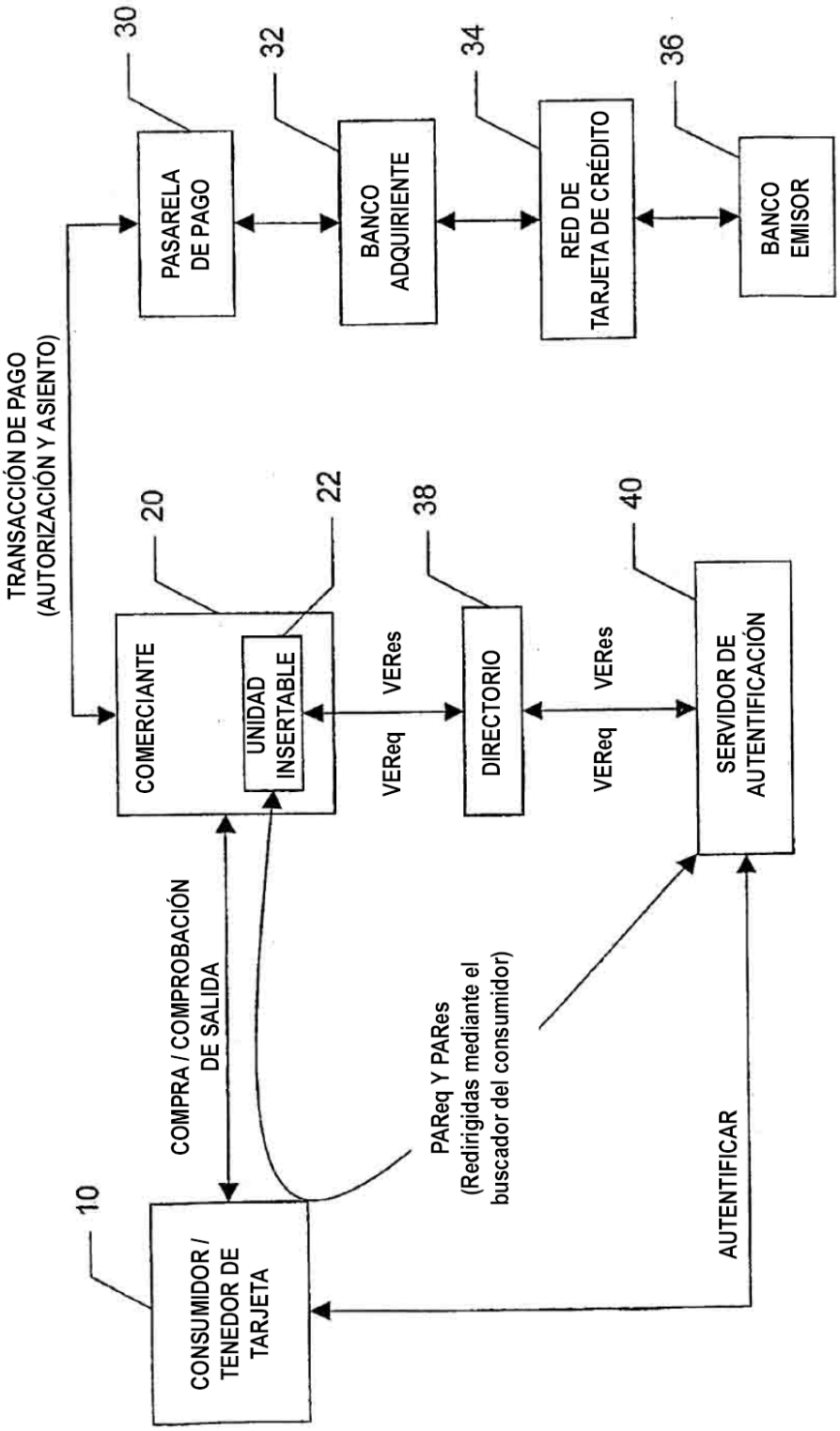
30
32
34
36
PASARELA DE PAGO
BANCO ADQUIRIENTE
RED DE TARJETA DE CRÉDITO
BANCO EMISOR
TRANSACCIÓN DE PAGO (AUTORIZACIÓN Y ASIENTO)
20
22
38
40
COMERCIANTE
UNIDAD INSERTABLE
VEReq
VERes
DIRECTORIO
VEReq
VERes
SERVIDOR DE AUTENTIFICACIÓN
COMPRA / COMPROBACIÓN DE SALIDA
PAReq Y PARes (Redirigidas mediante el buscador del consumidor)
AUTENTIFICAR
10
CONSUMIDOR / TENEDOR DE TARJETA

FIGURA 1

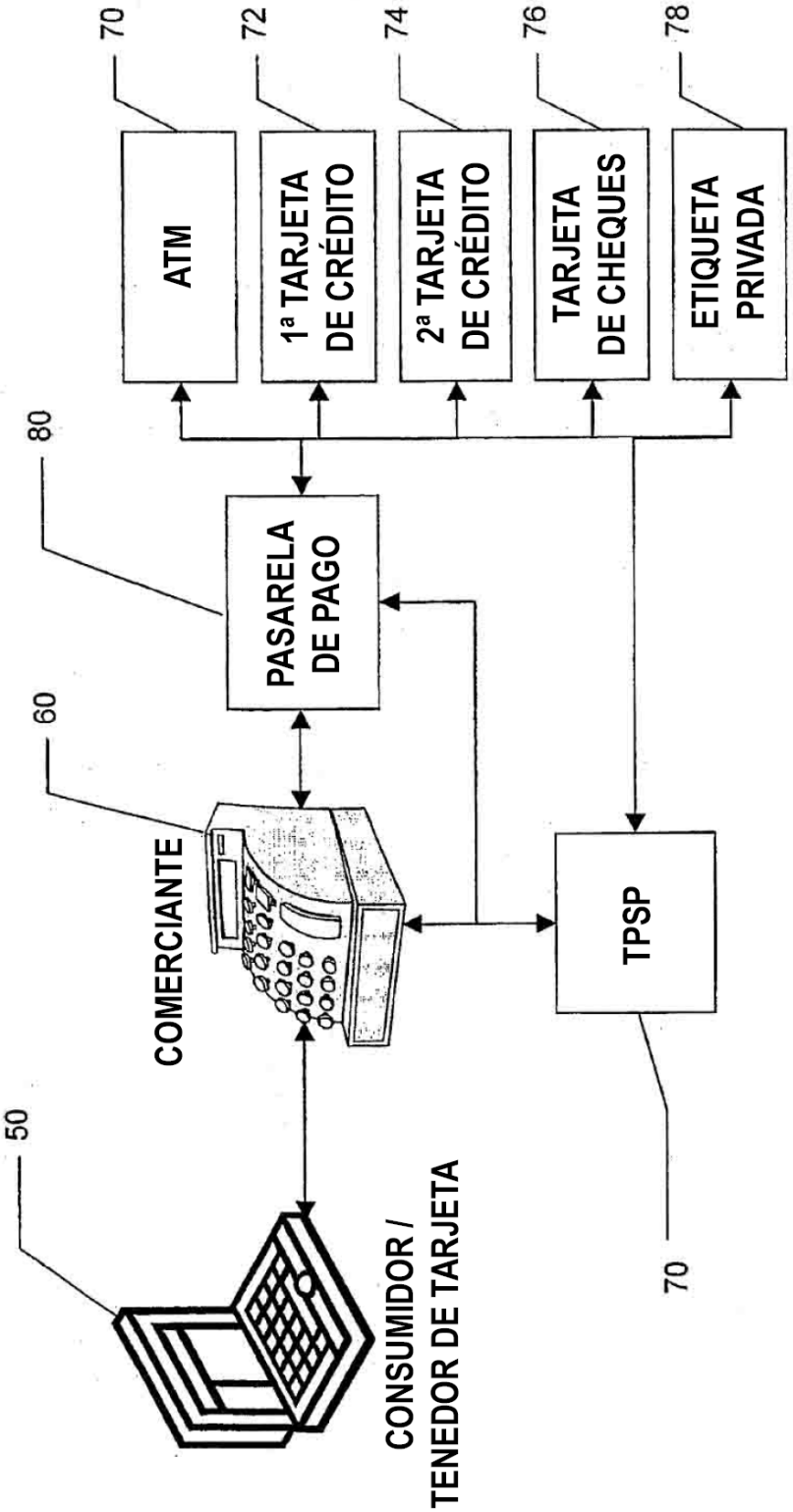
70
72
74
76
78
ATM
1ª TARJETA DE CRÉDITO
2ª TARJETA DE CRÉDITO
TARJETA DE CHEQUES
ETIQUETA PRIVADA
80
PASARELA DE PAGO
60
COMERCIANTE
TPSP
70
50
CONSUMIDOR / TENEDOR DE TARJETA

FIGURA 2

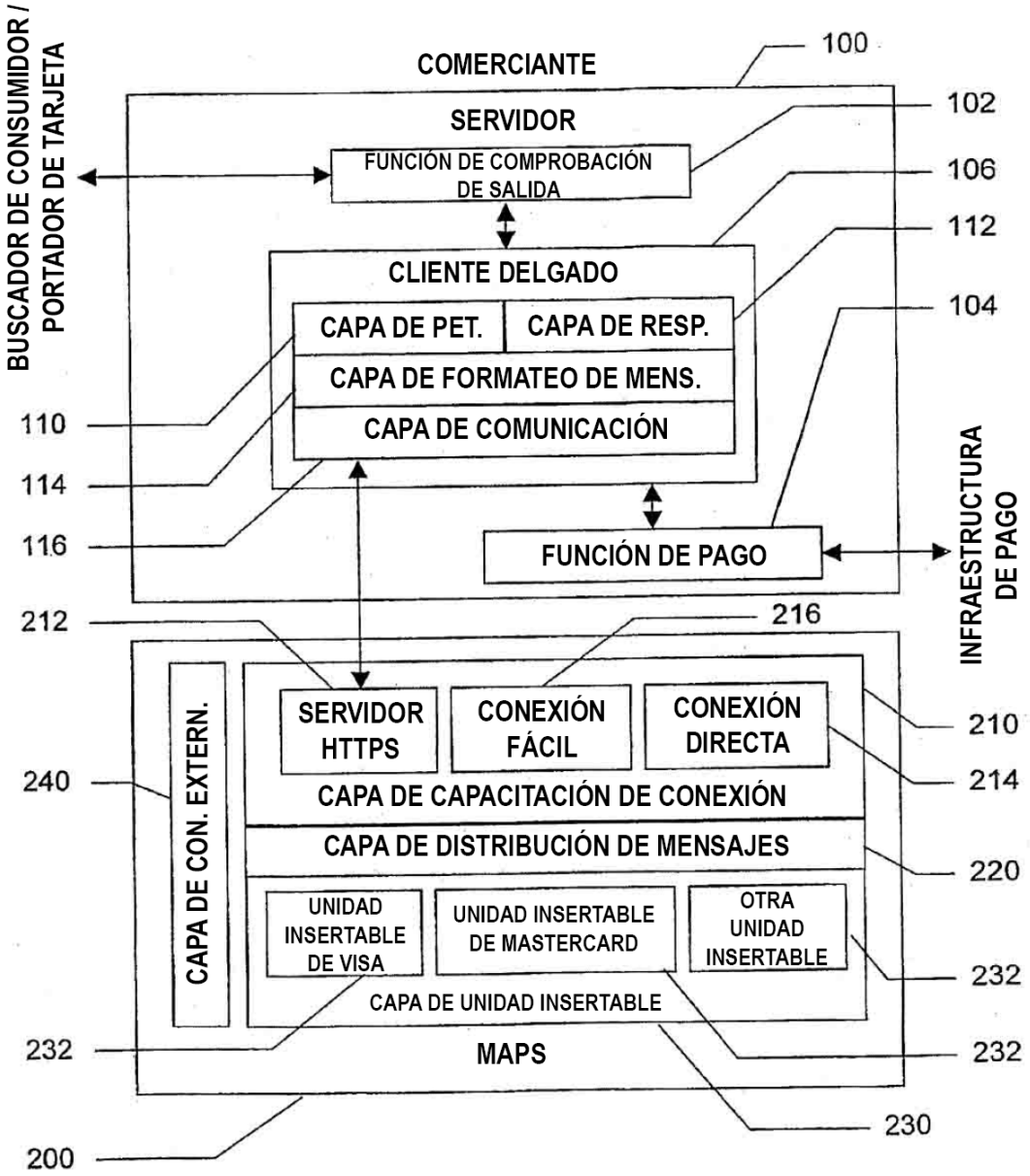
BUSCADOR DE CONSUMIDOR / PORTADOR DE TARJETA
COMERCIANTE
100
SERVIDOR
102
FUNCIÓN DE COMPROBACIÓN DE SALIDA
106
112
CLIENTE DELGADO
104
CAPA DE PET.
CAPA DE RESP.
CAPA DE FORMATEO DE MENS.
CAPA DE COMUNICACIÓN
110
114
116
FUNCIÓN DE PAGO
INFRAESTRUCTURA DE PAGO
212
216
SERVIDOR HTTPS
CONEXIÓN FÁCIL
CONEXIÓN DIRECTA
210
214
240
CAPA DE CON. EXTERN.
CAPA DE CAPACITACIÓN DE CONEXIÓN
CAPA DE DISTRIBUCIÓN DE MENSAJES
220
UNIDAD INSERTABLE DE VISA
UNIDAD INSERTABLE DE MASTERCARD
OTRA UNIDAD INSERTABLE
232
CAPA DE UNIDAD INSERTABLE
232
MAPS
232
230
200

FIGURA 3