(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 581 782**

(51) Int. CI.:

G06Q 20/00 (2012.01)
H04B 1/40 (2006.01)
G06Q 20/02 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.09.2009 E 09815367 (9)**

(97) Fecha y número de publicación de la concesión europea: **29.06.2016 EP 2332092**

(54) Título: **Aparato y método para prevenir el acceso no autorizado a una aplicación de pago instalada en un dispositivo de pago sin contacto**

(30) Prioridad:

22.09.2008 US 99060 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.09.2016

(73) Titular/es:

VISA INTERNATIONAL SERVICE ASSOCIATION (100.0%)
P.O. Box 8999 MS M3-2B
San Francisco, CA 94128-8999, US

(72) Inventor/es:

AABYE, CHRISTIAN;
NGO, HAO y
WILSON, DAVID

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Aparato y método para prevenir el acceso no autorizado a una aplicación de pago instalada en un dispositivo de pago sin contacto

Antecedentes

Las realizaciones de la presente invención se refieren a sistemas, aparatos y métodos para realizar transacciones de pago y, más concretamente, a un sistema y al aparato y método asociado para realizar transacciones de pago utilizando un dispositivo de pago portátil que incluye una aplicación de pago, donde la aplicación de pago se activa en respuesta a los datos suministrados por una fuente fiable, conforme se indica en las reivindicaciones. Las realizaciones de la presente invención se pueden utilizar para realizar transacciones de pago de forma segura para prevenir el acceso no autorizado a los datos de la transacción o a la funcionalidad de la aplicación de pago en ausencia de datos específicos suministrados por la fuente fiable.

Los dispositivos de pago para consumidores son utilizados por millones de personas en todo el mundo para facilitar diversos tipos de transacciones comerciales. En una transacción típica que implica la compra de un producto o servicio en un establecimiento comercial, el dispositivo de pago se presenta en un terminal de punto de venta (POS) ubicado en el establecimiento del comerciante. El POS puede ser un lector de tarjetas o un dispositivo similar capaz de acceder a los datos almacenados en el dispositivo de pago, de forma que estos datos pueden incluir datos de identificación o autenticación, por ejemplo. Los datos leídos por el dispositivo de pago se suministran al sistema de procesamiento de transacciones del comerciante y posteriormente al Adquirente, que es típicamente un banco u otra institución que gestiona la cuenta del comerciante. Los datos proporcionados al Adquirente pueden ser posteriormente suministrados a una red de procesamiento de pago que está en comunicación con procesadores de datos que procesan los datos de la transacción para determinar si la transacción debe ser autorizada por la red y contribuyen a las funciones de tramitación y liquidación en cuenta de las transacciones completadas. La decisión de autorización y las partes de tramitación y liquidación de la transacción también pueden implicar la comunicación y/o transferencia de datos entre la red de procesamiento de pago y el banco o la institución que emitió el dispositivo de pago para el consumidor (conocido como el Emisor).

A pesar de que un dispositivo de pago para el consumidor puede ser una tarjeta de crédito o una tarjeta de débito, también puede adquirir la forma de una tarjeta «inteligente» o un chip «inteligente». Por lo general, una tarjeta inteligente se define como una tarjeta de bolsillo (u otra forma de dispositivo de pago portátil) que tiene integrados un microprocesador y uno o más chips de memoria o que tiene integrados uno o más chips de memoria con lógica no programable. Típicamente la tarjeta de tipo microprocesador puede implementar determinadas funciones de procesamiento de datos como añadir, eliminar o manipular de otro modo la información almacenada en una ubicación de memoria de la tarjeta. Por el contrario, la tarjeta tipo chip de memoria (por ejemplo, una tarjeta telefónica de prepago) típicamente solo puede actuar como un archivo para mantener datos que son manipulados a través de un dispositivo lector de tarjetas para realizar una operación predefinida, como cargar un gasto en un saldo preestablecido almacenado en un registro de la memoria. Las tarjetas inteligentes, a diferencia de las tarjetas de banda magnética (como las tarjetas de crédito estándar), pueden implementar diversas funciones y pueden contener diversos tipos de información en la tarjeta. Por tanto, en algunas aplicaciones puede que no precisen acceder a una base de datos remota a fin de autenticar a un consumidor o crear un registro de datos en el momento de una transacción. Una tarjeta inteligente es un dispositivo semiconductor capaz de realizar la mayoría de las funciones de una tarjeta inteligente (si no todas), pero puede estar integrada en otro dispositivo.

Las tarjetas inteligentes o los chips inteligentes se encuentran disponibles en dos variedades generales: tipo contacto y tipo sin contacto. Una tarjeta inteligente tipo contacto es aquella que incluye un elemento físico (por ejemplo, una banda magnética, un adaptador de contacto) que permite el acceso a los datos y a las capacidades funcionales de la tarjeta, típicamente a través de alguna forma de terminal o lector de tarjetas. Por el contrario, una tarjeta inteligente o un chip inteligente sin contacto es un dispositivo que incorpora un medio de comunicación con un lector de tarjetas o terminal de punto de venta sin necesidad de contacto físico directo. Por tanto, estos dispositivos se pueden «pasar» efectivamente (es decir, que pueden ser leídos por otro dispositivo o intercambiar datos de otro modo con este) acercándolos a un terminal o lector de tarjetas convenientemente configurado. Las tarjetas o chips sin contacto se comunican típicamente con un lector de dispositivos o terminal que utiliza tecnología de RF (radiofrecuencia), donde la proximidad al lector o terminal permite la transferencia de datos entre la tarjeta o el chip y el lector o terminal.

Los dispositivos sin contacto se utilizan en banca y otras aplicaciones, donde ofrecen la ventaja de que no es necesario extraerlos de la cartera o el bolsillo del usuario para participar en una transacción. Una tarjeta o chip sin contacto pueden estar integrados (o incorporados de otro modo) en un dispositivo móvil, como un teléfono móvil o un asistente personal digital (PDA). Por otra parte, dado el creciente interés que generan estos dispositivos, se han desarrollado normas que regulan el funcionamiento y las interfaces para las tarjetas inteligentes sin contacto, tales como la norma ISO 14443.

En una transacción de pago típica, los datos son enviados desde un terminal de punto de venta al Emisor

para autenticar a un consumidor y obtener la autorización para la transacción.

Como parte de los procesos de autenticación o autorización, los datos pueden ser objeto de acceso o procesados por otros elementos del sistema de procesamiento de la transacción (por ejemplo, el Adquirente del comerciante o un procesador de pago que forme parte de la red de procesamiento de pago). Cabe señalar que en algunos casos la autorización para la transacción se puede obtener sin conectar con el Emisor; esto puede ser permitido por los parámetros de gestión del riesgo configurados por el Emisor que se hayan establecido en el dispositivo de pago o la aplicación de pago del consumidor. Si la transacción propuesta es autorizada, entonces el consumidor puede proporcionar otra información al comerciante para completar la transacción. El Emisor o el procesador de datos también pueden devolver datos al consumidor. Estos datos pueden incluir una actualización de los registros de las transacciones para las que se ha utilizado el dispositivo de pago o del saldo actual de una cuenta asociada al dispositivo.

Un dispositivo de pago puede incluir una aplicación de pago que se activa para permitir que un consumidor inicie o realice de otro modo una transacción de pago.

En algunos casos, el dispositivo de pago puede ser un teléfono móvil o un dispositivo similar capaz de comunicar a través de una red inalámbrica y que incluye un elemento sin contacto que se utiliza para realizar la transacción de pago. Típicamente, el elemento sin contacto utiliza una funcionalidad de comunicación de campo cercano (NFC) para comunicar con un lector de dispositivos o terminal de punto de venta para realizar una transacción. Un potencial problema de seguridad que puede surgir con estos dispositivos de pago es que una persona no autorizada puede intentar obtener acceso a la aplicación de pago o a los datos de la transacción utilizando la funcionalidad de comunicación en red inalámbrica del dispositivo de pago para activar la aplicación de pago o para intentar acceder a los datos almacenados en una memoria segura del dispositivo de pago.

Otro potencial problema de seguridad que puede surgir cuando se utiliza un dispositivo de pago que incluye una funcionalidad de comunicación inalámbrica es el de la denegación de la transacción por un ataque al servicio de dispositivo de pago. Una entidad maliciosa podría bloquear efectivamente a un usuario válido evitando su acceso a la aplicación de pago instalada en el dispositivo de pago del usuario, empleando una red inalámbrica para transmitir datos a la aplicación de pago que la aplicación interpretó como un intento incorrecto de introducir los datos de seguridad o el código de acceso del usuario. Un número relativamente pequeño de estos intentos de introducir un código de acceso incorrecto podría provocar que la aplicación bloquee el acceso a las funciones de pago o a los datos de las transacciones, lo que podría suponer un problema para el usuario. Si se realizase un número suficiente de estos intentos maliciosos de acceder a las aplicaciones de pago de múltiples usuarios, es posible que un pequeño número de ellos lograse su objetivo, permitiendo el acceso no autorizado a las aplicaciones de pago de algunos usuarios.

Lo recomendable es un sistema, aparato y método para prevenir el acceso no autorizado a una aplicación de pago instalada en un dispositivo de pago móvil o a los datos de las transacciones almacenados en el dispositivo, en particular en el caso de un dispositivo de pago con funcionalidad de comunicación a través de una red inalámbrica. Las realizaciones de la invención tratan estos y otros problemas de forma individual y colectiva.

Breve resumen

Las realizaciones de la presente invención están dirigidas a un sistema, aparato y método para prevenir el acceso no autorizado a una aplicación de pago instalada en un dispositivo de pago móvil como el reivindicado. En algunas realizaciones, el dispositivo de pago móvil es un teléfono móvil que incluye un elemento sin contacto (como un chip inteligente sin contacto) y con capacidad para la comunicación y transferencia de datos utilizando una red de comunicación inalámbrica y una funcionalidad de comunicación de campo cercano o corto alcance. La invención previene el acceso no autorizado o una denegación efectiva de transacciones por un ataque al servicio, al requerir que los datos de control de acceso se reciban de una fuente fiable, como un controlador o una aplicación responsable de gestionar los datos introducidos desde el teclado de un teléfono, para activar la aplicación de pago o para acceder a los datos almacenados.

En una realización típica, los datos de control del acceso pueden ser un código de acceso o una serie de datos alfanuméricos proporcionados por el controlador en respuesta a un código de acceso introducido por un usuario utilizando el teclado del teléfono. En respuesta a la introducción de los datos del código de acceso por parte del usuario, la invención comunica los datos de seguridad u otros datos de control del acceso a la aplicación de pago (o a un elemento responsable de realizar la función de control del acceso para la aplicación de pago). El código de seguridad y el código de acceso son verificados por la aplicación de pago y, si ambos son válidos, entonces la aplicación de pago y/o los datos de la transacción seguros se ponen a disposición del usuario. El sistema, el aparato y el método de la invención se pueden implementar utilizando un chip inteligente sin contacto y un elemento de transferencia de datos inalámbrico (por ejemplo, una funcionalidad de comunicación de campo cercano (NFC) o tecnología de comunicación de corto alcance similar, etc.) integrados en un dispositivo inalámbrico móvil. Las realizaciones típicas del dispositivo móvil incluyen un teléfono móvil y una PDA.

Otros objetos y ventajas de la presente invención resultarán evidentes para un experto en la técnica tras revisar la descripción detallada de la presente invención y las figuras incluidas.

Breve descripción de los dibujos

La Fig. 1 es un diagrama esquemático que ilustra un sistema de procesamiento de transacciones que puede ser utilizado con algunas realizaciones de la presente invención;

La Fig. 2 es un diagrama esquemático funcional que ilustra los componentes primarios de un sistema que puede ser utilizado para prevenir el uso no autorizado de una aplicación de pago instalada en un dispositivo móvil, de acuerdo con algunas realizaciones de la presente invención;

La Fig. 3 es un diagrama esquemático funcional que ilustra los componentes primarios de un dispositivo móvil, como un teléfono móvil, que puede ser utilizado como parte del sistema y el método de la invención;

La Fig. 4 es un diagrama esquemático funcional que ilustra determinados elementos funcionales que pueden estar presentes en un aparato que puede ser utilizado para implementar el método de la invención para prevenir el acceso no autorizado a una aplicación de pago instalada en un dispositivo de pago móvil; y

La Fig. 5 es un diagrama de flujo que ilustra una realización del método de la invención o del proceso para prevenir el uso no autorizado de una aplicación de pago instalada en un dispositivo de pago móvil.

Descripción detallada

Las realizaciones de la presente invención están dirigidas a un sistema, aparato y método para prevenir el uso no autorizado de una aplicación de pago instalada en un dispositivo de pago móvil como el reivindicado. En algunas realizaciones, el dispositivo de pago móvil puede ser un teléfono móvil o un asistente personal digital que incluye un elemento de tipo sin contacto. El elemento de tipo sin contacto puede incluir una aplicación de pago y un área de almacenamiento de datos segura, a pesar de que uno de estos elementos o ambos pueden estar integrados en otras partes del dispositivo de pago móvil.
En algunas realizaciones, la invención funciona solicitando la presentación de los datos de seguridad secretos a la aplicación de pago para su verificación antes de que un usuario pueda utilizar la aplicación de pago o acceder a los registros de la transacción. En algunas realizaciones, los datos de seguridad secretos se proporcionan a la aplicación de pago por un controlador, una interfaz o una aplicación que gestiona la operación de una fuente fiable incluida en el dispositivo de pago. Típicamente, la fuente fiable es un dispositivo o elemento que recibe los datos introducidos por el usuario y, en respuesta a esto, la fuente fiable o un controlador para la fuente fiable proporciona esos datos introducidos y los datos de seguridad secretos a la aplicación de pago para su verificación. Entre los ejemplos de una fuente fiable adecuada se incluyen un teclado, una huella dactilar u otro lector de datos biométricos, un micrófono, etc. Un servidor remoto que almacena los datos de control del acceso también puede funcionar en su totalidad o en parte como una fuente fiable.

En un escenario típico, un usuario proporciona los datos de identificación adecuados a la fuente fiable, que posteriormente proporciona los datos de identificación y los datos de seguridad secretos a la aplicación de pago. La aplicación de pago verifica la validez de los datos de seguridad secretos y de los datos de identificación introducidos por el usuario y, en respuesta, permite al usuario acceder a las funciones de la aplicación de pago. Al requerir que los datos de identificación introducidos por el usuario (como un código de acceso, huella digital, huella de voz, etc.) y los datos de seguridad secretos sean suministrados a la aplicación de pago a través de una fuente fiable verificable, la presente invención elimina efectivamente la capacidad de una entidad maliciosa de acceder a la aplicación de pago o a los registros de transacción segura a través del envío de datos falsos o no verificables a través de una red de comunicación inalámbrica al dispositivo de pago. En el caso de un servidor remoto que funcione como fuente fiable, el servidor puede recibir los datos introducidos por el usuario a través de una red de comunicación adecuada y, en respuesta, proporcionar los datos de seguridad secretos al dispositivo de pago para su verificación por parte de la aplicación de pago. Por otra parte, en algunos ejemplos, el servidor remoto puede devolver tanto los datos secretos como los datos introducidos por el usuario al dispositivo de pago como parte de un único mensaje o paquete de datos, de forma que la aplicación de pago después utiliza ese único mensaje o paquete de datos para realizar las dos partes de la operación de verificación de datos necesaria para permitir el acceso a la aplicación de pago.

La presente invención se implementa típicamente en el contexto de una transacción de pago; por tanto, antes de describir una o más realizaciones de la invención con más detalle, se presentará una breve explicación de las entidades que participan en el procesamiento y la autorización de una transacción de pago y sus funciones en el proceso de autorización.

La Figura 1 es un diagrama esquemático que ilustra un sistema de procesamiento de transacciones que puede ser utilizado con algunas realizaciones de la presente invención; Típicamente, una transacción de pago electrónica es autorizada si el consumidor que realiza la transacción es convenientemente

autenticado (es decir, si se verifica su identidad y su uso válido de una cuenta de pago) y si el consumidor dispone de crédito o fondos suficientes para realizar la transacción. Por el contrario, si la cuenta del consumidor no dispone de crédito o fondos suficientes, o si el dispositivo de pago del consumidor se encuentra en una lista negativa (por ejemplo, se ha indicado que posiblemente ha sido robada o utilizada de manera fraudulenta) entonces la transacción de pago electrónico no será autorizada. En la siguiente descripción, un «Adquirente» es típicamente una entidad empresarial (por ejemplo, un banco comercial) que mantiene una relación comercial con un comerciante concreto. Un «Emisor» es típicamente una entidad empresarial (por ejemplo, un banco) que emite un dispositivo de pago (como una tarjeta de crédito o débito) para un consumidor. Algunas entidades pueden realizar las funciones tanto de Emisor como de Adquirente.

La Figura 1 ilustra los elementos funcionales primarios que participan típicamente en el procesamiento de una transacción de pago y en el proceso de autorización de dicha transacción. Tal y como se muestra en la Figura 1, en una transacción de pago típica, un consumidor que desea adquirir un bien o servicio a un comerciante utiliza un dispositivo de pago portátil del consumidor 20 para proporcionar los datos de la transacción de pago que podrán ser utilizados como parte del proceso de verificación del consumidor o de autorización de la transacción. El dispositivo de pago portátil del consumidor 20 puede ser una tarjeta de débito, una tarjeta de crédito, una tarjeta inteligente, un dispositivo móvil que contiene un chip sin contacto, u otra forma de dispositivo adecuado.

El dispositivo de pago portátil del consumidor se presenta a un lector de dispositivos o terminal de punto de venta (POS) 22 capaz de acceder a los datos almacenados en el dispositivo de pago. Los datos de la cuenta (así como cualesquiera datos requeridos del consumidor) son comunicados al comerciante 24 y en última instancia al sistema de procesamiento de datos/transacciones del comerciante 26. Como parte del proceso de autorización realizado por el comerciante, el sistema de procesamiento de transacciones del comerciante 26 puede acceder a la base de datos del comerciante 28, que típicamente almacena datos relativos al cliente/consumidor (como resultado de un proceso de registro con el comerciante, por ejemplo), el dispositivo de pago del consumidor y el historial de transacciones del consumidor con el comerciante.

El sistema de procesamiento de transacciones del comerciante 26 típicamente se comunica con el Adquirente 30 (que gestiona las cuentas del comerciante) como parte del proceso general de autenticación o autorización. El sistema de procesamiento de transacciones del comerciante 26 y/o el Adquirente 30 proporciona los datos a la Red de Procesamiento de Pago 34, que entre otras funciones participa en los procesos de tramitación y liquidación que forman parte del procesamiento general de la transacción. La comunicación y la transferencia de datos entre el sistema de procesamiento de transacciones del comerciante 26 y la Red de Procesamiento de pago 34 se producen típicamente por medio de un intermediario, como un Adquirente 30. Como parte del proceso de verificación del consumidor o autorización de la transacción, la Red de Procesamiento de pago 34 puede acceder a la base de datos de la cuenta 36, que típicamente contiene información relativa al historial de pago de la cuenta del consumidor, contracargos o historial de conflictos en transacciones, solvencia, etc. La Red de Procesamiento de pago 34 se comunica con el Emisor 38 como parte del proceso de autenticación o autorización, donde el Emisor 38 es la entidad que emitió el dispositivo de pago al consumidor y gestiona la cuenta del consumidor. Los datos del consumidor o de la cuenta del consumidor se almacenan típicamente en una base de datos del cliente/consumidor 40 a la que puede acceder el Emisor 38 como parte de los procesos de autenticación, autorización o gestión de la cuenta. Cabe señalar que en lugar de estar almacenados en una base de datos de la cuenta 36, o además de ello, los datos de la cuenta del consumidor pueden estar incluidos o formar parte de otro modo de la base de datos del cliente/consumidor 40.

En una operación estándar, se genera un mensaje de solicitud de autorización durante la compra por parte del consumidor de un bien o servicio en un punto de venta (POS), utilizando un dispositivo de pago portátil del consumidor. En algunas realizaciones, el dispositivo de pago portátil del consumidor puede ser un teléfono inalámbrico o un asistente personal digital que incorpora una tarjeta o un chip sin contacto. La tarjeta o el chip sin contacto pueden comunicar con el terminal de punto de venta utilizando una funcionalidad de comunicación de campo cercano (NFC). El mensaje de solicitud de autorización es enviado típicamente desde el lector de dispositivos/POS 22 a través del sistema de procesamiento de datos del comerciante 26 al Adquirente 30 del comerciante, a una red de procesamiento de pago 34 y posteriormente a un Emisor 38. Un «mensaje de solicitud de autorización» puede incluir una solicitud de autorización para realizar una transacción de pago electrónico y datos pertinentes para determinar si se debe aceptar la solicitud. Por ejemplo, el mensaje puede incluir uno o más de los elementos siguientes: el número de cuenta de pago del titular de la cuenta, el código de moneda, el importe de la venta, el sello de la transacción del comerciante, la ciudad del aceptador, el estado/país del aceptador, etc. Un mensaje de solicitud de autorización puede ser protegido utilizando un método de cifrado seguro (por ejemplo, SSL de 128 bits o equivalente) para prevenir el acceso no autorizado a los datos de la cuenta o transacción.

Una vez que el Emisor recibe el mensaje de solicitud de autorización, el Emisor determina si la transacción debe ser autorizada y envía un mensaje de respuesta de autorización a la red de procesamiento de pago para indicar si la transacción está o no autorizada. A continuación, el sistema de

procesamiento de pago envía el mensaje de respuesta de autorización al Adquirente. El Adquirente envía después el mensaje de respuesta al Comerciante. De este modo, el Comerciante sabe si el Emisor ha autorizado la transacción y, por tanto, si se puede completar dicha transacción.

En un momento posterior, se puede realizar un proceso de tramitación y pago a través de los elementos del sistema de procesamiento de pago/transacción que se ilustra en la Figura 1. Un proceso de tramitación implica el intercambio de datos financieros entre un Adquirente y un Emisor para facilitar el cargo de una transacción en la cuenta de un consumidor y la reconciliación de la posición de liquidación del consumidor. La tramitación y la liquidación se pueden producir de forma simultánea o como procesos separados.

La Red de Procesamiento de Pago 34 puede incluir subsistemas de procesamiento de datos, redes y otros medios de implementación de operaciones utilizados para respaldar y prestar servicios de autorización, servicios de archivo de excepción, y servicios de tramitación y liquidación para las transacciones de pago. Un ejemplo de Red de Procesamiento de Pago puede incluir VisaNet. Las Redes de Procesamiento de pago como VisaNet son capaces de procesar transacciones de tarjetas de crédito, transacciones de tarjetas de débito y otros tipos de transacciones comerciales. VisaNet, en concreto, incluye un sistema VIP (Visa Integrated Payments) que procesa solicitudes de autorización de transacciones y un sistema Base II que realiza servicios de tramitación y liquidación de transacciones.

La Red de Procesamiento de pago 34 puede incluir un servidor. Un servidor es típicamente un ordenador o cluster de ordenadores de gran potencia. Por ejemplo, el servidor puede ser una gran unidad central de procesamiento, un conjunto de miniordenadores o un grupo de servidores que funcionan como una unidad. En un ejemplo, el servidor puede ser el servidor de una base de datos conectado a un servidor web. La Red de Procesamiento de pago 34 puede utilizar cualquier combinación adecuada de redes alámbricas o inalámbricas, incluyendo internet, para permitir la comunicación y la transferencia de datos entre elementos de la red. Entre otras funciones, la Red de Procesamiento de pago 34 puede ser responsable de garantizar que un consumidor sea autorizado para realizar una transacción (a través de un proceso de autenticación), confirmar la identidad de una parte de una transacción (por ejemplo, mediante la recepción de un número de identificación personal), confirmar una línea de crédito o saldo suficiente para permitir una compra, o reconciliar el importe de una compra con la cuenta del cliente (mediante la introducción de un registro del importe de la transacción, la fecha, etc.).

El dispositivo de pago del consumidor 20 puede adoptar una de múltiples formas adecuadas. Tal y como se ha mencionado, el dispositivo portátil del consumidor puede ser un dispositivo móvil que incorpora un elemento sin contacto, como un chip para almacenar datos de pago (por ejemplo, un número BIN, número de cuenta, etc.) e incluye un elemento de transferencia de datos de comunicación de campo cercano (NFC), como una antena, un diodo emisor de luz, un láser, etc. El dispositivo portátil del consumidor también puede incluir un dispositivo de llavero (como Speedpass™ comercializado por Exxon-Mobil Corp.), etc. El dispositivo que contiene la tarjeta o el chip sin contacto, u otro elemento de almacenamiento de datos, puede ser un teléfono celular (móvil), un asistente personal digital (PDA), un dispositivo buscapersonas, un transpondedor o similares. El dispositivo portátil del consumidor también puede incorporar la capacidad de realizar funciones de débito (por ejemplo, una tarjeta de débito), funciones de crédito (por ejemplo, una tarjeta de crédito), o funciones de valor almacenado (por ejemplo, una tarjeta de valor almacenado o prepago).

En realizaciones de la invención que incluyen un elemento sin contacto (por ejemplo, un chip sin contacto y un elemento de transferencia de datos de comunicación de campo cercano) integrado en un teléfono móvil inalámbrico o un dispositivo similar, el elemento sin contacto se puede comunicar con un lector de dispositivos o terminal de punto de venta del Comerciante utilizando un método de comunicación de corto alcance, como una funcionalidad de comunicación de campo cercano (NFC). Los ejemplos de estas tecnologías NFC o comunicaciones de corto alcance similares incluyen la norma ISO 14443, RFID, Bluetooth™ y métodos de comunicación por infrarrojos.

La Figura 2 es un diagrama esquemático funcional que ilustra los componentes primarios de un sistema 100 que puede ser utilizado para prevenir el uso no autorizado de una aplicación de pago instalada en un dispositivo móvil, según algunas realizaciones de la presente invención. Tal y como se muestra en la Figura 2, un sistema 100 incluye un dispositivo móvil 102 que tiene capacidades de comunicación inalámbrica 122. El dispositivo móvil 102 puede ser un teléfono móvil inalámbrico, PDA, ordenador portátil, dispositivo buscapersonas, etc. En una realización típica, el dispositivo móvil 102 es un teléfono celular, aunque como se ha señalado, la implementación de la presente invención no se limita a esta realización, dado que el dispositivo móvil que funciona como dispositivo de pago puede adoptar cualquier forma adecuada cuyo uso resulte cómo para el consumidor. Naturalmente, si el dispositivo móvil no es un teléfono celular o una forma similar de dispositivo de comunicación inalámbrica, entonces es posible que el dispositivo móvil no ofrezca capacidad de comunicación a través de una red inalámbrica o celular. En el caso de un teléfono celular como dispositivo móvil 102, el dispositivo incluye la circuitería del dispositivo móvil 104 (teléfono celular) que permite algunas funciones de telefonía. Entre otras funciones, la circuitería del dispositivo móvil 104 permite que el dispositivo móvil 102 se comunique inalámbricamente con el sistema celular (por ejemplo, un portador inalámbrico) 120 a través de una red celular 122.

El dispositivo móvil 102 incluye asimismo un elemento sin contacto 106, típicamente implementado en forma de un chip semiconductor. El elemento sin contacto 106 puede incluir un elemento de almacenamiento de datos seguro 110, a pesar de que el elemento de almacenamiento de datos seguro 110 también se puede implementar como un elemento separado del elemento sin contacto 106. El elemento sin contacto 106 incluye un elemento de transferencia de datos (NFC) (por ejemplo, transmisión de datos) de comunicación de campo cercano 105, como una antena o transductor. La funcionalidad de comunicación de campo cercano permite que un lector de dispositivo o terminal de punto de venta intercambie datos (o realice operaciones) con el elemento sin contacto 106 como parte o durante la preparación de una transacción de pago. En algunas realizaciones, el elemento sin contacto 106 puede estar integrado con los elementos del dispositivo móvil 102. En este caso, los datos o las instrucciones de control pueden ser opcionalmente transmitidos a través de una red celular 122 e intercambiados con un elemento sin contacto 106 (o solicitados a este) por medio de una interfaz del elemento sin contacto 108. En esta situación, la interfaz del elemento sin contacto 108 funciona para permitir el intercambio de datos y/o instrucciones de control entre la circuitería del dispositivo móvil 104 (y, por consiguiente, la red celular) y el elemento sin contacto 106. Por tanto, el elemento sin contacto 106 puede incluir capacidad de almacenamiento de datos en forma de una memoria o almacenamiento de datos seguro 110 al que se puede acceder a través de la funcionalidad de comunicación de campo cercano o interfaz 108 para permitir la implementación de funciones de lectura, escritura y eliminación de datos, por ejemplo.

El almacenamiento de datos seguro 110 puede ser utilizado por el dispositivo móvil 102 para almacenar parámetros operativos u otros datos utilizados en el funcionamiento del dispositivo. El almacenamiento de datos seguro 110 también puede ser utilizado para almacenar otros datos para los que se desea una seguridad mejorada, tales como, datos de transacciones, datos de cuentas personales, datos de identificación, datos de autenticación, datos de control de acceso para el funcionamiento de una aplicación o dispositivo, etc. Tal y como se ha mencionado, el almacenamiento de datos seguro 110 puede ser implementado en forma de un chip que está separado y aparte del elemento sin contacto 106, o alternativamente, puede ser una sección de memoria de un chip que forma parte del elemento sin contacto 106. Cabe señalar asimismo que el almacenamiento de datos seguro y/o elemento sin contacto incluido en el dispositivo móvil puede ser un elemento extraíble o puede estar integrado en el dispositivo móvil. Entre los ejemplos de elementos extraíbles se incluyen tarjetas SIM, tarjetas de memoria flash y otros dispositivos adecuados.

El dispositivo móvil 102 también puede incluir una o más aplicaciones 109, donde las aplicaciones 109 se implementan en forma de uno o más de los elementos siguientes: software, firmware o hardware. Las aplicaciones 109 se utilizan para implementar diversas funciones deseadas por un consumidor, donde estas funciones pueden incluir, a título meramente enunciativo, operaciones de transacciones de comercio electrónico, operaciones de transacciones de pago, etc. Típicamente, las aplicaciones 109 representan procesos u operaciones que están dedicados a una función específica que proporciona valor añadido para el consumidor y que no forma parte del funcionamiento estándar del dispositivo (es decir, no forma parte de las funciones de telefonía estándar, por ejemplo). Tal y como se muestra en la figura, las aplicaciones 109 pueden intercambiar datos con el almacenamiento de datos seguro 110 (a través de una interfaz del elemento sin contacto 108) y también pueden ser capaces de intercambiar datos con la circuitería del dispositivo móvil 104. Una aplicación típica 109 a efectos de la presente invención es una aplicación de pago que permite a un consumidor realizar el pago de una transacción, donde la transacción se realiza en su totalidad o en parte utilizando el dispositivo móvil. En este ejemplo, el almacenamiento de datos seguro 110 puede contener datos de autenticación, datos de identificación del consumidor, datos de registro de las transacciones, datos del saldo de la cuenta, etc. Las aplicaciones 109 se almacenan típicamente como una serie de instrucciones ejecutables en memoria 107, que también pueden incluir el almacenamiento de datos 113. Un procesador accede a la memoria 107 para cargar y descargar las instrucciones y los datos necesarios para ejecutar las instrucciones para realizar las funciones de las aplicaciones. Cabe señalar que a efectos de la presente invención, una aplicación de pago puede estar incluida en una región de almacenamiento de datos del dispositivo móvil que forma parte (o está separada) de la región de almacenamiento de datos incluida en el elemento sin contacto.

El elemento sin contacto 106 es capaz de transferir y recibir datos utilizando un elemento de transferencia de datos 105 que implementa funcionalidad de comunicación de campo cercano 112, típicamente según un protocolo estandarizado o mecanismo de transferencia de datos (identificado como ISO 14443/NFC en la figura). La funcionalidad de comunicación de campo cercano 112 es una funcionalidad de comunicación de corto alcance; entre los ejemplos se incluyen ISO 14443, RFID, Bluetooth™, infrarrojos, y otras funcionalidades de transferencia de datos que pueden ser utilizadas para intercambiar datos entre el dispositivo móvil 102 y un lector de dispositivos o terminal de punto de venta 130, que se encuentra típicamente ubicado en el establecimiento de un Comerciante. Por tanto, en algunas realizaciones, el dispositivo móvil 102 es capaz de comunicar y transferir datos y/o instrucciones de control a través tanto de una red celular 122 como de una funcionalidad de comunicación de campo cercano 112, a pesar de que las comunicaciones y la transferencia de datos a través de la red celular no sean necesarias para implementar determinadas realizaciones de la presente invención. En la situación en la que el dispositivo de pago móvil tiene funcionalidad de comunicación y transferencia de datos a través de la red celular, las realizaciones de la presente invención pueden ofrecer un nivel de seguridad adicional para prevenir el

acceso no autorizado a la aplicación de pago y a los datos de la transacción por parte de una entidad maliciosa que use la red inalámbrica para proporcionar datos al dispositivo móvil.

El sistema 100 incluye asimismo un Adquirente 132 que está en comunicación con el Comerciante o con el lector de dispositivos o terminal de punto de venta 130 del Comerciante. El Adquirente 132 está en comunicación con la Red de Procesamiento de pago 134 y, tal y como se ha descrito, puede intercambiar datos con la Red de Procesamiento de pago 134 como parte del proceso de autorización de las transacciones. La Red de Procesamiento de pago 134 también está en comunicación con el Emisor 136. Tal y como se ha descrito, el Emisor 136 puede intercambiar datos con la Red de Procesamiento de pago 134 como parte de un proceso de autenticación, autorización de la transacción o reconciliación de la transacción.

El sistema 100 también puede incluir la Pasarela Móvil 138, que es capaz de conectar el sistema o la red celular (inalámbrica) a una segunda red (típicamente una red alámbrica como internet) y permitir la transferencia de datos entre las redes. La Pasarela Móvil 138 puede realizar las operaciones de procesamiento de datos necesarias para permitir la transferencia eficiente de datos entre los dos tipos de redes, incluyendo, a título meramente enunciativo, el reformateado de datos u otro procesamiento para tener en cuenta las diferencias de los protocolos de red. La Pasarela Móvil 138 también puede realizar operaciones de procesamiento de datos para permitir la transferencia de datos más eficiente entre las redes y los dispositivos conectados a cada tipo de red, por ejemplo a efectos de mejorar la capacidad de un consumidor para utilizar los datos recibidos en un dispositivo móvil. Tal y como se muestra en la figura, en algunas realizaciones la Pasarela Móvil 138 está conectada a la Red de Procesamiento de pago 134, que está conectada al Adquirente 130. Cabe señalar que resultan posibles otras realizaciones, como aquellas en las que la Pasarela Móvil 138 está conectada al Emisor 136, y donde el Adquirente 130 está conectado al Emisor 136 (tal y como sugieren las líneas discontinuas de la Figura 2). De forma similar, el Emisor 136 puede incluir la capacidad de funcionamiento como Pasarela Móvil 138.

El dispositivo de pago móvil puede ser cualquier dispositivo que incluye una aplicación de pago, donde la aplicación de pago se utiliza para iniciar o participar de otro modo en una transacción de pago. En algunas realizaciones, el dispositivo de pago móvil puede incluir un elemento sin contacto que tiene capacidad de comunicación y transferencia de datos utilizando un método de comunicación de campo cercano o comunicaciones de corto alcance similar. Por otra parte, el dispositivo móvil puede incluir la capacidad de comunicar y transferir datos utilizando una red inalámbrica, como una red de telefonía celular. En esta situación, las realizaciones de la presente invención pueden reducir o eliminar el riesgo de que una entidad maliciosa puede proporcionar datos o comandos a través de la red inalámbrica, en un intento de obtener acceso a la aplicación de pago, sus funciones, o a los datos de la transacción almacenados en el dispositivo de pago.

Un ejemplo de un dispositivo de pago móvil que puede ser utilizado para implementar las realizaciones de la presente invención es un teléfono móvil inalámbrico equipado con una funcionalidad NFC. La Figura 3 es un diagrama esquemático funcional que ilustra los componentes primarios de un dispositivo portátil del consumidor (por ejemplo, el elemento 102 de la Figura 2), como un teléfono móvil, que puede ser utilizado como parte del sistema y los métodos de la invención. Tal y como se ilustra en la Figura 3, el dispositivo móvil 302 puede incluir la circuitería que se utiliza para permitir determinadas funciones de telefonía y otras funciones del dispositivo. Los elementos funcionales responsables de permitir estas funciones pueden incluir un procesador 304 para ejecutar instrucciones que implementan las funciones y operaciones del dispositivo. El procesador 304 puede acceder al almacenamiento de datos 312 (u otro elemento o región de memoria adecuado) para recuperar instrucciones o datos utilizados para ejecutar las instrucciones.

Se pueden utilizar elementos de entrada/salida de datos 308 para permitir que un usuario introduzca datos (vía micrófono, teclado, pantalla táctil, detector de huellas, dispositivo de introducción de datos biométricos, por ejemplo) o para recibir datos salientes (a través de una pantalla 306 o un altavoz, por ejemplo). Tal y como se describirá, en algunas realizaciones de la presente invención, uno o más de los elementos de introducción de datos (o un controlador para el elemento de introducción de datos) pueden funcionar como «fuente fiable» que proporciona «datos secretos» a una aplicación de pago en respuesta a la introducción de un código de acceso por parte de un usuario. Los datos secretos y el código de acceso son posteriormente utilizados por la aplicación de pago para autenticar al usuario y permitir el acceso a las funciones de la aplicación de pago. El elemento de comunicación 310 puede ser utilizado para permitir la transferencia de datos entre el dispositivo 302 y una red inalámbrica (vía una antena 318, por ejemplo) para ayudar a activar las funciones de telefonía y transferencia de datos. Tal y como se ha descrito con respecto a la Figura 2, el dispositivo 302 también puede incluir una interfaz del elemento sin contacto 314 para permitir la transferencia de datos entre el elemento sin contacto 316 y otros elementos del dispositivo, donde el elemento sin contacto 316 puede incluir una memoria segura y un elemento de transferencia de datos de comunicación de campo cercano. El elemento sin contacto puede implementar una funcionalidad de comunicación de campo cercano que permite la comunicación y la transferencia de datos entre el dispositivo 302 y un lector de dispositivos o POS que forma parte de un sistema de procesamiento de transacciones de pago.

El almacenamiento de datos 312 puede ser una memoria que almacena datos y puede adoptar cualquier

forma conveniente, incluyendo un chip de memoria, unidad de disco, memoria flash, etc. La memoria puede ser utilizada para almacenar datos tales como la información de autenticación o identificación del usuario, la información de la cuenta del usuario, los datos de la transacción, etc. La información financiera almacenada puede incluir información como los datos de la cuenta bancaria, el número de identificación del banco (BIN), la información del número de cuenta de la tarjeta de crédito o débito, la información del saldo de la cuenta, la fecha de caducidad, información del consumidor como el nombre, la fecha de nacimiento, etc. Cabe señalar que estos datos pueden ser almacenados alternativa o adicionalmente en un elemento de almacenamiento de datos seguro, como el almacenamiento de datos seguro 110 de la Figura 2 o una memoria segura similar que forma parte del elemento sin contacto 316. Tal y como se ha descrito, el almacenamiento de datos 312 también puede contener instrucciones que cuando son ejecutadas por el procesador 304 implementan operaciones o procesos que forman parte del funcionamiento del dispositivo o de las aplicaciones instaladas en el dispositivo.

El almacenamiento de datos 312 o un elemento de memoria seguro que forma parte del elemento sin contacto 316 puede incluir una aplicación de pago que se activa a fin de iniciar o facilitar de otro modo una transacción de pago. La aplicación de pago puede acceder al elemento de almacenamiento de datos para obtener datos utilizados para participar en una transacción de pago o para registrar o actualizar un registro de datos para una transacción. La aplicación de pago puede comunicar e intercambiar datos con otros elementos del dispositivo 302 como resultado de una interfaz de programas de aplicación (API) u otra forma de interfaz adecuada, o como resultado de interacciones con un controlador o una aplicación que funciona para recibir datos introducidos por un usuario y proporciona los datos recibidos a la aplicación de pago.

La aplicación de pago puede realizar una o más operaciones o procesos de autenticación o verificación antes de permitir que un usuario acceda a las funciones de la aplicación de pago o a los datos asociados con la aplicación de pago. En las realizaciones de la presente invención, estas operaciones o procesos de autenticación o verificación pueden incluir la verificación de que una fuente fiable ha proporcionado a la aplicación de pago datos secretos, y que tanto los datos secretos como el código de acceso proporcionado por el usuario (u otros datos de identificación o autenticación facilitados por el usuario) son válidos. Si tanto los datos secretos como los datos de identificación o autenticación facilitados por el usuario son válidos, entonces las funciones de la aplicación de pago se «desbloquearán», «activarán» o estarán disponibles de otro modo para el usuario.

La Figura 4 es un diagrama esquemático funcional que ilustra determinados elementos funcionales que pueden estar presentes en un aparato que puede ser utilizado para implementar el método de la invención para prevenir el acceso no autorizado a una aplicación de pago instalada en un dispositivo de pago móvil. Los elementos funcionales ilustrados en la Figura 4 pueden ser implementados en forma de uno de los elementos siguientes: software, firmware o hardware.

Si se implementan en forma de software, los elementos se pueden implementar en forma de instrucciones almacenadas en un medio legible por ordenador que pueden ser ejecutadas por un procesador. Los elementos funcionales ilustrados en la Figura 4 forman típicamente parte de un dispositivo de pago móvil, como un teléfono móvil, PDA, ordenador portátil, etc. Cabe señalar que si los datos secretos son almacenados en un servidor remoto y proporcionados desde ese servidor al dispositivo de pago móvil, entonces determinados elementos ilustrados en la Figura 4 pueden residir en el servidor, con el dispositivo móvil y el servidor comunicándose a través de una red de comunicaciones adecuada (como una red inalámbrica o celular).

Como se ha señalado, en realizaciones de la presente invención, el método de la invención implica controlar el acceso a la aplicación de pago instalada en un dispositivo de pago. La aplicación de pago permite a un usuario realizar pagos de bienes o servicios y acceder a los datos incluidos en los registros de transacciones que pueden ser almacenados en el dispositivo. La aplicación de pago puede realizar una o más operaciones de control de acceso o seguridad antes de permitir que un usuario acceda a la aplicación de pago o a los datos de la transacción. Típicamente, las operaciones de control de acceso o seguridad actúan como una forma de validación o verificación del usuario, e implican determinar que ciertos datos presentados a la interfaz del usuario de la aplicación de pago son válidos o se ha verificado su autenticidad. Los datos presentados a la interfaz del usuario de la aplicación de pago son típicamente proporcionados por un dispositivo de introducción de datos del usuario. Sin embargo, tal y como se ha señalado, es posible que una entidad maliciosa intente obtener acceso no autorizado a la aplicación de pago proporcionando datos a la interfaz del usuario de la aplicación de pago (a través de una interfaz de red inalámbrica, por ejemplo). Las realizaciones de la presente invención previenen que estos intentos prosperen y también previenen que los intentos fallidos resulten en una denegación del servicio para el usuario.

En las realizaciones, la presente invención funciona para limitar el acceso a las operaciones de control del acceso o seguridad de la aplicación de pago (es decir, la validación del usuario), al requerir que los datos sean proporcionados por un «dispositivo fiable». En las realizaciones de la presente invención, un dispositivo fiable es un dispositivo de introducción de datos del usuario (o un controlador o dispositivo conectado al dispositivo de introducción de datos del usuario) que forma típicamente parte del dispositivo que contiene la aplicación de pago. En algunas realizaciones, la presente invención previene que los

datos sean introducidos para las funciones u operaciones de validación del usuario de la aplicación de pago, a menos que los datos hayan sido proporcionados por un elemento del dispositivo de pago. Por otra parte, a fin de prevenir que una persona no autorizada para el uso del dispositivo de pago consiga acceder introduciendo datos a través del dispositivo de introducción de datos del usuario que proporciona los datos a la aplicación de pago, las realizaciones de la presente invención utilizan dos tipos de datos de control de seguridad para la aplicación de pago. El primero son los datos introducidos por el usuario, que adoptan la forma de datos personales adecuados para el tipo de elemento de introducción de datos implicado. Por ejemplo, los datos personales pueden ser un código de acceso, un número de identificación personal, una huella digital, una huella de voz, etc. asociados a un usuario autorizado concreto. El segundo tipo de datos son «datos secretos», que son datos proporcionados por el elemento de introducción de datos (o un controlador para el elemento de introducción de datos o, en algunos ejemplos, un servidor remoto) en respuesta a la recepción de los datos personales del usuario. El código o los datos secretos son desconocidos para un usuario y pueden ser generados cuando sea necesario para proporcionar seguridad (por ejemplo, de forma periódica, tras un determinado número de transacciones, para cada transacción, etc.). Tanto los datos personales como los datos secretos deben ser verificados como válidos para que un usuario pueda acceder a las funciones u operaciones de la aplicación de pago. Esta disposición previene que una entidad maliciosa intente activar la aplicación de pago proporcionando datos a través de la red inalámbrica (dado que la aplicación de pago solamente se puede activar a través de los datos proporcionados por un elemento del dispositivo de pago u otra fuente fiable) y también previene que alguien que robe o encuentre un dispositivo de pago perdido pueda activar la aplicación de pago (dado que los datos personales del usuario válidos deberán ser utilizados para proporcionar los datos secretos a la aplicación de pago).

Tal y como se muestra en la Figura 4, el dispositivo de pago puede incluir un elemento de introducción de datos del usuario 402. El elemento de introducción de datos del usuario 402 puede adoptar cualquier forma adecuada, incluyendo, a título meramente enunciativo, un teclado, un micrófono, un sensor o detector de huellas dactilares, una pantalla táctil, un sensor de datos biométricos, etc. En algunas realizaciones, el elemento de introducción de datos del usuario 402 sirve como «fuente fiable» que recibe los datos introducidos por un usuario y en respuesta a ello proporciona los datos y los «datos secretos» a la aplicación de pago. En otras realizaciones, el elemento de introducción de datos del usuario 402 puede servir para introducir los datos de identificación del usuario, con un controlador que actúa como fuente fiable que controla el suministro de los datos secretos. La transmisión de los datos introducidos por un usuario en el elemento de introducción de datos 402 a otros elementos del dispositivo de pago (como la aplicación de pago) puede ser controlada o activada de otro modo por el controlador de fuente fiable o API 404. El controlador de fuente fiable o API 404 puede adoptar cualquier forma adecuada capaz de recibir datos del elemento de introducción de datos 402 y de realizar operaciones de procesamiento de datos para transmitir los datos introducidos, una forma de los datos introducidos, o los datos generados en respuesta a los datos introducidos a la aplicación de pago 408. Por otra parte, el controlador de fuente fiable o API 404 puede ejecutar o provocar la ejecución de una aplicación o instrucciones que realizan la totalidad o parte de las funciones del controlador o API 404. Estas funciones u operaciones pueden incluir el procesamiento de los datos introducidos por un usuario para verificar su autenticidad o la generación de otros datos en respuesta a los datos introducidos (como un código hash, por ejemplo), donde los datos generados pueden ser utilizados para permitir el acceso a los datos secretos o para permitir el acceso a las funciones de la aplicación de pago. A pesar de que estas funciones u operaciones pueden ser realizadas por el controlador de fuente fiable o API, cabe señalar que estas funciones u operaciones no son necesarias para implementar todas las realizaciones de la presente invención.

A fin de proporcionar los datos secretos a la aplicación de pago en respuesta a los datos introducidos por el usuario, el controlador de fuente fiable o API 404 puede acceder al almacenamiento de los datos secretos 406 para obtener los datos secretos almacenados en el mismo. Los datos secretos pueden adoptar cualquier forma adecuada, incluyendo, a título meramente enunciativo, una cadena de datos, una cadena de caracteres alfanuméricos, etc. En algunas realizaciones, los datos secretos pueden ser una cadena de datos de ocho bytes. En algunas realizaciones, los datos secretos pueden ser generados para cada intento de uso de la aplicación de pago y eliminados después de cada uso de la aplicación de pago. En otras realizaciones, los datos secretos pueden ser los mismos para múltiples usos de la aplicación de pago o para un periodo de tiempo predeterminado. Típicamente, al almacenamiento de los datos secretos 406 accede el controlador de fuente fiable o API 404 en respuesta a la introducción por parte del usuario de los datos correctos de autenticación o identificación en el elemento de introducción de datos del usuario 402. El controlador de fuente fiable o API 404 puede realizar una operación de verificación o validación con los datos introducidos por el usuario (por ejemplo, para verificar la autenticidad de un código PIN o cadena de datos) o puede transmitir los datos introducidos a otros elementos ilustrados en la figura sin realizar un proceso de verificación o validación.

El controlador de fuente fiable o API 404 actúa para proporcionar los datos introducidos por el usuario (u otros datos generados en respuesta a la introducción de estos datos) y los datos secretos almacenados en el almacenamiento de los datos secretos 406 a la aplicación de pago 408. La aplicación de pago 408 recibe los datos proporcionados y realiza una o más operaciones de verificación o validación sobre los datos recibidos. Por ejemplo, el Módulo de Verificación de Datos del Usuario y Datos Secretos 410 puede

recibir los datos introducidos por el usuario y los datos secretos del controlador de fuente fiable o API 404. A continuación, el Módulo de Verificación 410 puede realizar procesamientos de datos, pruebas, comparaciones de datos o cualquier otra forma adecuada de operación de verificación o validación de datos, a fin de determinar si tanto los datos introducidos por el usuario como los datos secretos son válidos. Estas operaciones de verificación o validación de datos pueden incluir el acceso a los datos almacenados en el almacenamiento de datos seguro 412 para obtener datos con los que se comparan los datos introducidos por el usuario y los datos secretos o para obtener datos que se utilizan de otro modo como parte del proceso de verificación o validación. Si se verifica la validez tanto de los datos introducidos por el usuario como de los datos secretos, entonces se permite el acceso del usuario a las funciones de la aplicación de pago 414. Este acceso puede incluir el uso de diversas funcionalidades u operaciones de la aplicación de pago, así como el acceso a los datos de las transacciones o de las cuentas almacenados en el dispositivo de pago móvil.

La Figura 5 es un diagrama de flujo que ilustra una realización 500 del método de la invención o del proceso para prevenir el uso no autorizado de una aplicación de pago instalada en un dispositivo de pago móvil. Los pasos o fases del proceso ilustrados en la figura pueden ser implementados en forma de un proceso o rutina independiente, o como parte de un proceso o rutina más general. Cabe señalar que cada paso o fase del proceso ilustrado puede ser implementado como un aparato que incluye un procesador que ejecuta una serie de instrucciones, un método o un sistema, entre otras realizaciones.

Tal y como se muestra en la figura, en un caso de ejemplo, en la fase 502a un usuario presenta su dispositivo de pago a un lector de dispositivos o terminal de punto de venta (POS) o intenta de otro modo activar una aplicación de pago instalada en el dispositivo de pago. Por ejemplo, el usuario puede «pasar», «deslizar» o presentar de otro modo su dispositivo de pago ante el lector de dispositivos para intentar iniciar una transacción de pago utilizando una funcionalidad de comunicación de campo cercano o corto alcance del dispositivo. Esto se puede realizar iniciando la comunicación entre el lector de dispositivos o POS y el dispositivo de pago, a fin de provocar la activación de la aplicación de pago. Esta activación puede ocurrir como resultado de que el lector de dispositivos o TVP transfiera datos o un comando al dispositivo de pago (por ejemplo, realizando lo que equivale a una activación por una clave o una tecla), sea automáticamente o como respuesta al hecho de que un consumidor haya seleccionado el icono de una aplicación de pago en un lector de dispositivos o en la pantalla del POS, por ejemplo. El usuario también puede intentar lanzar o activar la aplicación de pago pulsando una tecla o utilizando otra forma de introducción de datos.

En respuesta al intento del usuario de utilizar la aplicación de pago, al usuario se le presenta una interfaz de usuario. La interfaz de usuario puede incluir cualquier combinación adecuada de elementos para permitir que un usuario interactúe con y use la funcionalidad de la aplicación de pago. En un ejemplo de uso, la interfaz del usuario solicitará al usuario que introduzca los datos de identificación del usuario u otra forma de datos personales (fase 504) en un dispositivo de introducción de datos adecuado (por ejemplo, elemento 402 de la Figura 4).

Los datos de identificación del usuario pueden adquirir cualquier forma adecuada y esta dependerá en cierta medida del dispositivo de introducción de datos que se vaya a utilizar para proporcionar los datos solicitados. Entre los ejemplos de tipos de datos de identificación del usuario y de los correspondientes dispositivos de introducción de datos se incluyen, a título meramente enunciativo, un teclado para la introducción de una cadena de datos alfanuméricos (como un PIN o un código de acceso del usuario), un lector de huellas digitales para introducir la huella digital del usuario, un micrófono para introducir una huella de voz del usuario, una pantalla táctil para introducir una secuencia de iconos o imágenes gráficas, etc. Cabe señalar que en algunas realizaciones de la presente invención, el dispositivo de introducción de datos o un controlador para las funciones del dispositivo de introducción de datos funciona como «dispositivo fiable».

En la fase 506, los datos de identificación del usuario son introducidos y proporcionados a un controlador para el dispositivo fiable (u otro elemento que realiza la misma función u otras equivalentes). Tal y como se ha señalado, en algunas realizaciones el dispositivo fiable es el receptor de los datos introducidos por el usuario o es un elemento que recibe los datos del elemento de la interfaz del usuario en el que se introducen los datos. En estos casos, el controlador del dispositivo fiable es una aplicación, API u otro elemento adecuado responsable de proporcionar una interfaz y/o de permitir la transferencia de datos entre el dispositivo fiable y otros elementos del dispositivo de pago (por ejemplo, elemento 404 de la Figura 4). En algunas realizaciones, el dispositivo fiable está asociado con los datos secretos que se utilizan como parte del proceso de verificación/validación del usuario necesario para permitir el acceso a la aplicación de pago. Los datos secretos proporcionan una forma de autenticación para el dispositivo fiable y se pueden almacenar en un elemento de almacenamiento de datos seguro (por ejemplo, el elemento 406 de la Figura 4). En respuesta a la introducción de datos de identificación del usuario, el controlador del dispositivo fiable proporciona los datos de identificación del usuario (o datos generados en respuesta a la introducción de estos datos, como un código hash, etc.) y los datos secretos a la aplicación de pago (fase 508; por ejemplo, elemento 408 de la Figura 4). La aplicación de pago recibe los datos proporcionados por el controlador del dispositivo fiable (fase 510) y realiza una o más operaciones de verificación/validación de datos con los datos recibidos (por ejemplo, estas operaciones pueden ser

realizadas por el módulo de verificación de datos del usuario y datos secretos 410 de la Figura 4).

La aplicación de pago realiza una o más operaciones de verificación/validación de datos con los datos recibidos para determinar si se facilitará al usuario el acceso a las funciones de la aplicación de pago y/o a los datos de la transacción. Las operaciones de verificación/validación de datos pueden incluir cualquier forma adecuada de prueba, comparación u otro procesamiento de datos, y pueden incluir la comparación con los datos almacenados en un dispositivo de almacenamiento de datos seguro, como el elemento 412 de la Figura 4. En algunas realizaciones, la aplicación de pago intentará en primer lugar autenticar los datos de autenticación del dispositivo fiable, es decir, los datos secretos (fase 512). Esto se puede realizar comparando los datos secretos recibidos del controlador del dispositivo fiable con una copia de los datos secretos almacenados en el dispositivo de almacenamiento de datos seguro al que se puede acceder a través de la aplicación de pago (por ejemplo, elemento 412 de la Figura 4). Si los datos secretos recibidos se verifican como válidos, entonces la aplicación de pago podrá intentar a continuación verificar los datos de identificación introducidos por el usuario (fase 514; esto también se puede realizar comparando los datos de identificación del usuario recibidos con una copia de los datos previamente almacenada). Si los datos recibidos se verifican como válidos (es decir, tanto los datos secretos como los datos de identificación del usuario son válidos), entonces se facilita al usuario el acceso a la funcionalidad de la aplicación de pago (fase 516, la aplicación de pago es «activada» para el usuario; por ejemplo, elemento 414 de la Figura 4). Al usuario se le puede permitir adicional o alternativamente el acceso a los datos o registros de la transacción. Si los datos secretos o los datos de identificación del usuario se verifican como no válidos o no se pueden autenticar por otro motivo, entonces se denegará el acceso al usuario a la aplicación de pago y/o a los datos de la transacción (fase 515).

Las operaciones de verificación/validación de datos pueden ser realizadas con los datos recibidos en cualquier orden; es decir, que los datos de identificación del usuario pueden ser verificados con anterioridad a la verificación de los «datos secretos» o, tal y como se muestra en la Figura 5, los «datos secretos» pueden ser verificados con anterioridad a la verificación de los datos de identificación del usuario. Por otra parte, los datos de identificación del usuario se pueden verificar adicional o alternativamente en la fase 504 o en otra fase adecuada, es decir antes de que el controlador del dispositivo fiable proporcione los datos secretos a la aplicación de pago.

A pesar de que se ha descrito una realización de la invención en la que un elemento del dispositivo de pago contiene o es responsable de controlar la presentación de los «datos secretos» a la aplicación de pago, existen otros métodos posibles. Por ejemplo, la introducción de un código de acceso del usuario u otros datos del usuario en un dispositivo de pago móvil (como un teléfono móvil) puede provocar que el dispositivo se comunique con un servidor remoto u otra ubicación de almacenamiento de datos utilizando una red de comunicación adecuada. El servidor remoto o la ubicación de almacenamiento de datos podrán almacenar los datos secretos u otros datos necesarios para permitir la activación de la aplicación de pago. Por ejemplo, el intento de un usuario de activar una aplicación de pago instalada en el dispositivo de pago puede provocar que al usuario se le solicite que introduzca los datos de verificación del usuario, cuya introducción podrá provocar que la aplicación de pago o el dispositivo se comunique con un servidor remoto (como una pasarela móvil) a través de una red inalámbrica. En respuesta a la recepción de los datos introducidos por el usuario, el servidor remoto podrá verificar que los datos introducidos son correctos y, en respuesta, proporcionar los datos secretos a través de la red inalámbrica al dispositivo de pago móvil. Una vez recibidos por el dispositivo, la aplicación de pago podrá realizar un proceso de autenticación de los dos tipos de datos (los datos introducidos por el usuario y los datos secretos recibidos del servidor remoto). Si se verifica que ambos tipos de datos son válidos o auténticos, entonces el usuario podrá acceder a las funciones de la aplicación de pago. Cabe señalar que en algunos ejemplos, el servidor remoto puede devolver tanto los datos secretos como los datos introducidos por el usuario al dispositivo de pago como parte de un único mensaje o paquete de datos, de forma que la aplicación de pago después utiliza ese único mensaje o paquete de datos para realizar las dos partes de la operación de verificación de datos necesaria para permitir el acceso a la aplicación de pago.

Cabe señalar que los datos introducidos por el usuario en el dispositivo de pago (como el teclado de un teléfono móvil) pueden ser verificados en el dispositivo antes de enviar una solicitud al servidor remoto para que proporcione los datos secretos o que esta solicitud se puede activar a través de la introducción de los datos del usuario (donde la verificación se produce en el servidor remoto o más adelante en la propia aplicación de pago). Asimismo, a pesar de que se ha descrito el uso de una pasarela móvil, se pueden almacenar los datos secretos en otra forma de servidor remoto. Por ejemplo, un servidor remoto operado por el Emisor puede almacenar los datos secretos. Por otra parte, a pesar de que se ha descrito el uso de la red inalámbrica o celular como canal para la transmisión de datos secretos al dispositivo móvil, se pueden utilizar otros canales apropiados. Estos canales incluyen la comunicación utilizando el lector de dispositivos o terminal de punto de venta, por ejemplo (en cuyo caso se podría utilizar un método de comunicación de campo cercano u otro tipo de comunicación de corto alcance). Cabe señalar que la presente invención anteriormente descrita se puede implementar en forma de lógica de control utilizando software informático de forma modular o integrada. Basándose en la divulgación y las enseñanzas del presente documento, una persona con los conocimientos habituales de la técnica entenderá y apreciará otras maneras y/o métodos de implementar la presente invención utilizando hardware y una combinación de hardware y software.

Cualesquiera de las funciones o componentes de software descritos en la presente solicitud podrán ser implementados como código de software que se ejecutará en un procesador utilizando cualquier lenguaje informático adecuado, como Java, C++ o Perl, empleando, por ejemplo, técnicas convencionales u orientadas a un objeto. El código de software puede ser almacenado como una serie de instrucciones o comandos en un medio legible por ordenador, como una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), un medio magnético como un disco duro o un disquete, o un medio óptico como un CD-ROM. Cualquiera de estos medios legibles por ordenador se puede encontrar en un único aparato informático o puede estar presente en diferentes aparatos informáticos de un sistema o red.

A pesar de que se han descrito detalladamente determinadas realizaciones de ejemplo y de que se han mostrado en los dibujos adjuntos, se entenderá que estas realizaciones se ofrecen únicamente a título ilustrativo y que no pretenden tener carácter restrictivo para el conjunto de la invención. Por tanto, esta invención no se limitará a las construcciones y disposiciones concretas mostradas y descritas, puesto que los expertos en la técnica idearán muchas otras modificaciones.

A efectos del presente, se entenderá que el uso de «un», «una», «el» o «la» implica «al menos uno», salvo que se indique específicamente lo contrario.

REIVINDICACIONES

1. Un dispositivo de pago móvil (102) en forma de un teléfono móvil, asistente personal digital o un ordenador portátil que se puede utilizar para recibir datos de una interfaz de red inalámbrica, que comprende:

un procesador;

una aplicación de pago (109, 408) instalada en el dispositivo de pago móvil;

una memoria (107); y

una serie de instrucciones almacenadas en la memoria (107), que cuando son ejecutadas por el procesador, implementa un método para:

solicitar a un usuario que introduzca los datos de identificación del usuario; y recibir los datos de identificación del usuario de un dispositivo de introducción de datos (402) que forma parte del dispositivo de pago móvil (102);

el dispositivo de pago móvil **caracterizado por** comprender un controlador de fuente fiable (404) configurado para controlar el envío de datos secretos en respuesta a la recepción de los datos de identificación del usuario desde el dispositivo de introducción de datos (402) mediante:

la verificación de la autenticidad de los datos de identificación del usuario;

el acceso a un almacenamiento de datos secretos (406) que está separado de la aplicación de pago y conectado al dispositivo de introducción de datos (402) a través del controlador de fuente fiable (404) para obtener los datos secretos en respuesta a la introducción de los datos de identificación del usuario en el dispositivo de introducción de datos (402), donde los datos secretos son: proporcionados por y asociados con el dispositivo de introducción de datos (402), desconocidos para el usuario, diferentes de los datos de identificación del usuario y utilizados para autenticar el dispositivo de introducción de datos (402); y

el suministro de los datos de identificación del usuario y de los datos secretos para la aplicación de pago (109, 408) en el dispositivo de pago móvil (102);

donde la aplicación de pago (109, 408) está configurada para verificar: la validez de los datos secretos comparando los datos secretos recibidos del controlador de fuente fiable (404) con una copia de los datos secretos almacenados en un almacenamiento de datos seguros (412) de la aplicación de pago; y la validez de los datos de identificación del usuario, comparando los

datos de identificación del usuario recibidos con una copia de los datos previamente almacenada; y

si tanto los datos secretos como los datos de identificación del usuario son válidos, facilitar al usuario el acceso a la aplicación de pago (109, 408); y si los datos secretos proporcionados y asociados con el dispositivo de introducción de datos (402) o los datos de identificación del usuario no son válidos, evitar al usuario el acceso a la aplicación de pago (109, 408).

2.El dispositivo de pago móvil de la reivindicación 1, donde el dispositivo (102) incluye un elemento sin contacto (106).

3.El dispositivo de pago móvil (102) de la reivindicación 2, donde el elemento

sin contacto (106) incluye una funcionalidad de comunicación inalámbrica.

4.El dispositivo de pago móvil (102) de la reivindicación 1, donde los datos secretos son generados para cada intento de utilizar la aplicación de pago (109, 408), tras un número predeterminado de intentos de utilizar la aplicación de pago (109, 408) o cuando haya transcurrido una cantidad de tiempo predeterminada desde la anterior generación de datos secretos.

5.Un método para prevenir el acceso no autorizado a la aplicación de pago (109, 408) instalada en un dispositivo de pago móvil (102) en forma de un teléfono móvil, asistente personal digital o un ordenador portátil que se puede utilizar para recibir datos de una interfaz de red inalámbrica, que consiste en:

solicitar a un usuario que introduzca los datos de identificación del usuario;

recibir los datos de identificación del usuario de un dispositivo de introducción de datos (402) que

forma parte del dispositivo de pago móvil (102), donde el método **se caracteriza por**:

un controlador de fuente fiable (404) configurado para controlar el envío de datos secretos en respuesta a la recepción de los datos de identificación del usuario desde el dispositivo de introducción de datos (402) mediante:

la verificación de la autenticidad de los datos de identificación del usuario;

el acceso a un dispositivo de almacenamiento de datos secretos (406) que está separado de la aplicación

de pago y conectado al dispositivo de introducción de datos (402) a través del controlador de fuente fiable (404) para obtener los datos secretos en respuesta a la introducción de los datos de identificación del usuario en el dispositivo de introducción de datos (402), donde los datos secretos son proporcionados por y asociados con el dispositivo de introducción de datos (402), desconocidos para el usuario, diferentes de los datos de identificación del usuario y utilizados para autenticar el dispositivo de introducción de datos (402); y

el suministro de los datos de identificación del usuario y de los datos secretos para la aplicación de pago (109, 408) en el dispositivo de pago móvil (102);

donde la aplicación de pago (109, 408) está configurada para verificar: la validez de los datos secretos comparando los datos secretos recibidos del controlador de fuente fiable (404) con una copia de los datos secretos almacenados en un almacenamiento de datos seguros (412) de la aplicación de pago; y la validez de los datos de identificación del usuario, comparando los datos de identificación del usuario recibidos con una copia de los datos previamente almacenada; y

si tanto los datos secretos como los datos de identificación del usuario son válidos, facilitar al usuario el acceso a la aplicación de pago (109, 408); y si los datos secretos asociados con el dispositivo de introducción de datos (402) o los datos de identificación del usuario no son válidos, evitar al usuario el acceso a la aplicación de pago (109, 408).

6.El método de la reivindicación 5, donde los datos secretos son una cadena de datos.

7.El método de la reivindicación 6, donde la cadena de datos es una cadena de datos alfanumérica.

8.El método de la reivindicación 5, que comprende también la generación de datos secretos para cada intento de utilizar la aplicación de pago (109, 408), tras un número predeterminado de intentos de utilizar la aplicación de pago (109, 408) o cuando haya transcurrido una cantidad de tiempo predeterminada desde la anterior generación de datos secretos.

9.El método de la reivindicación 5, que comprende también determinar que un usuario está intentando utilizar la aplicación de pago mediante la detección de un lector de dispositivos o un terminal de punto de venta, o la recepción de los datos introducidos desde un elemento de introducción de datos (402) del dispositivo de pago móvil (102).

10.Un elemento de almacenamiento de datos en el que se almacena una serie de instrucciones ejecutables por un procesador incluido en un dispositivo de pago móvil (102), donde, cuando son ejecutadas por el procesador, las instrucciones implementan un método según cualquiera de las reivindicaciones 5 a 9.

11.El dispositivo de pago móvil de la reivindicación 1, donde los datos de identificación del usuario son uno de los elementos siguientes: un código de acceso, un número de identificación personal, una cadena de datos alfanumérica, una huella digital o una huella de voz.

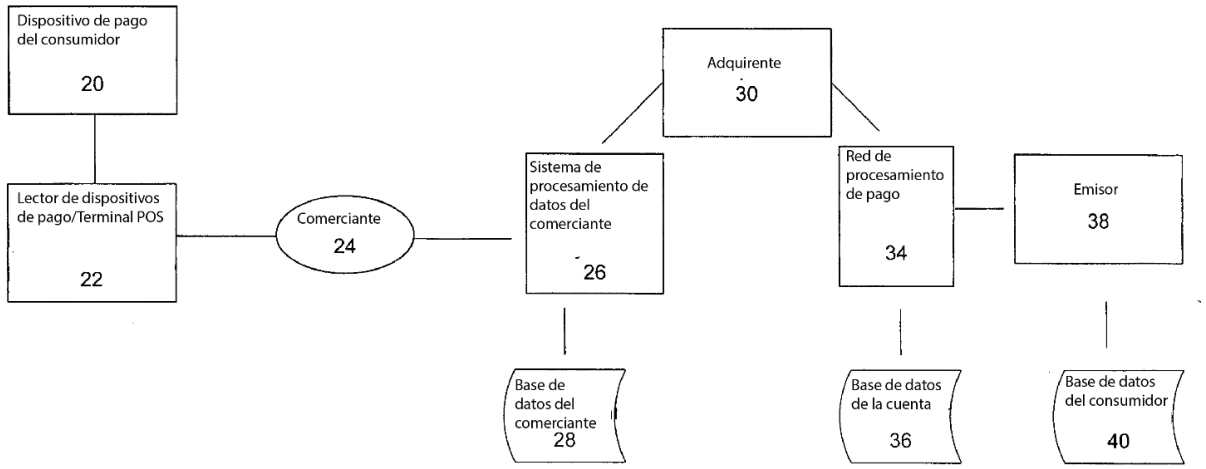

Dispositivo de pago del consumidor
20
Lector de dispositivos de pago/Terminal POS
22
Comerciante
24
Adquirente
30
Sistema de procesamiento de datos del comerciante
26
Red de procesamiento de pago
34
Emisor
38
Base de datos del comerciante
28
Base de datos de la cuenta
36
Base de datos del consumidor
40

FIG. 1

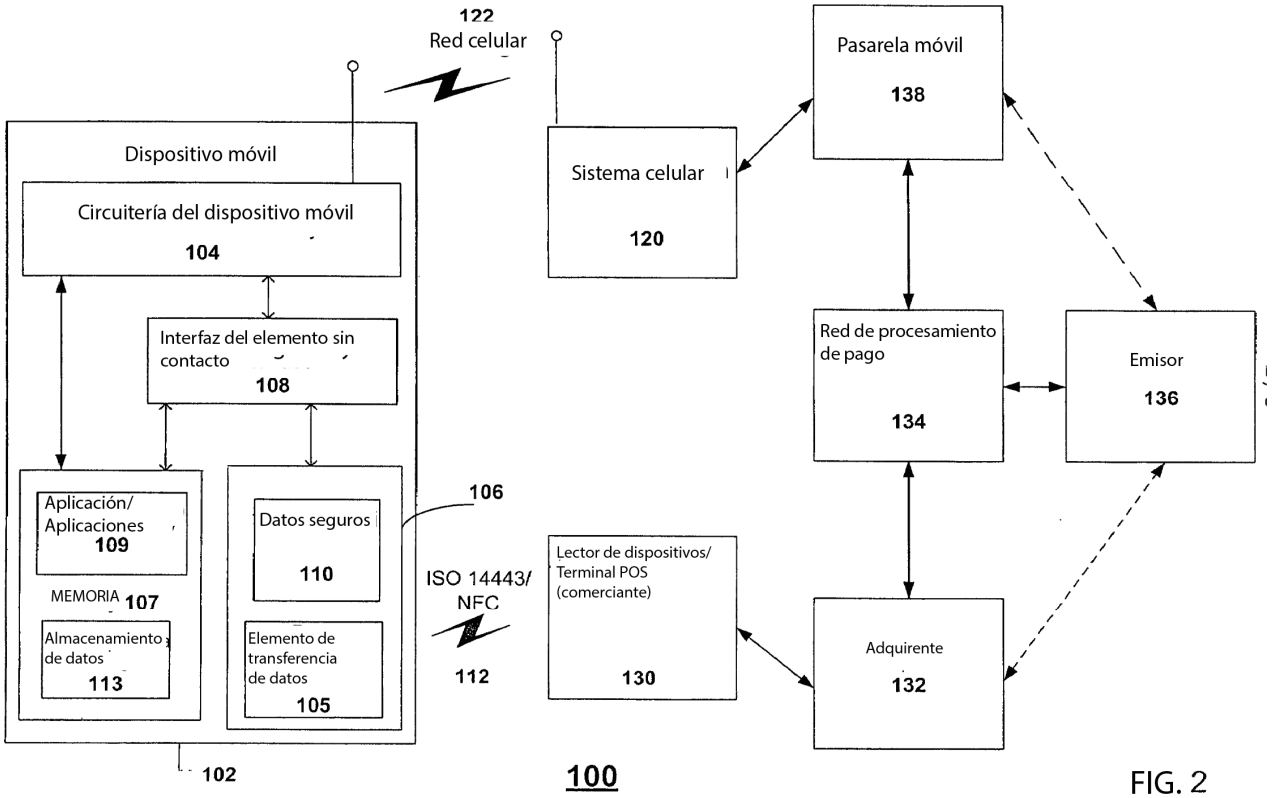

122
Red celular
Dispositivo móvil
Circuitería del dispositivo móvil
104
Interfaz del elemento sin contacto
108
Aplicación/ Aplicaciones
109
MEMORIA 107
Almacenamiento de datos
113
Datos seguros
110
Elemento de transferencia de datos
105
106
ISO 14443/ NFC
112
102
Sistema celular
120
Pasarela móvil
138
Red de procesamiento de pago
134
Emisor
136
Lector de dispositivos/ Terminal POS (comerciante)
130
Adquirente
132
100

FIG. 2

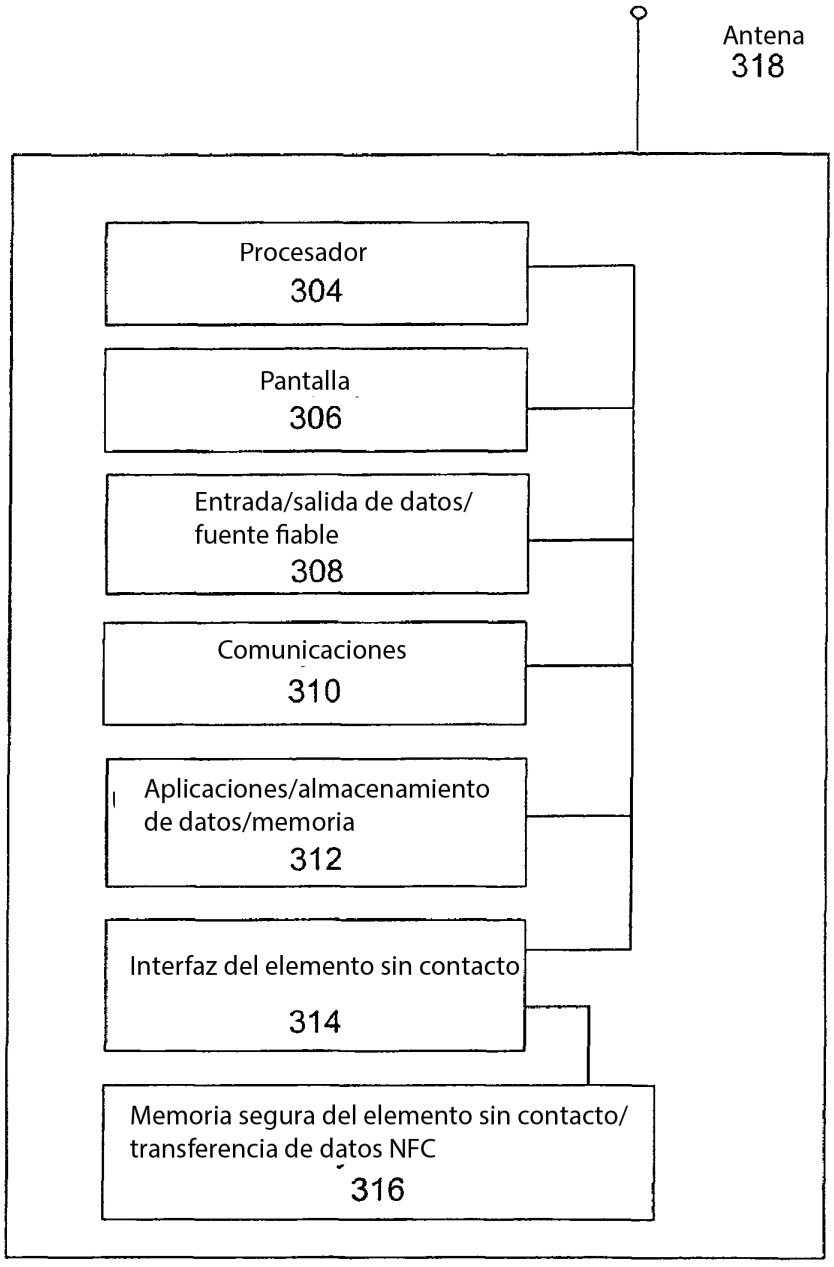

Antena
318
Procesador
304
Pantalla
306
Entrada/salida de datos/
fuente fiable
308
Comunicaciones
310
Aplicaciones/almacenamiento
de datos/memoria
312
Interfaz del elemento sin contacto
314
Memoria segura del elemento sin contacto/
transferencia de datos NFC
316
302

FIG. 3

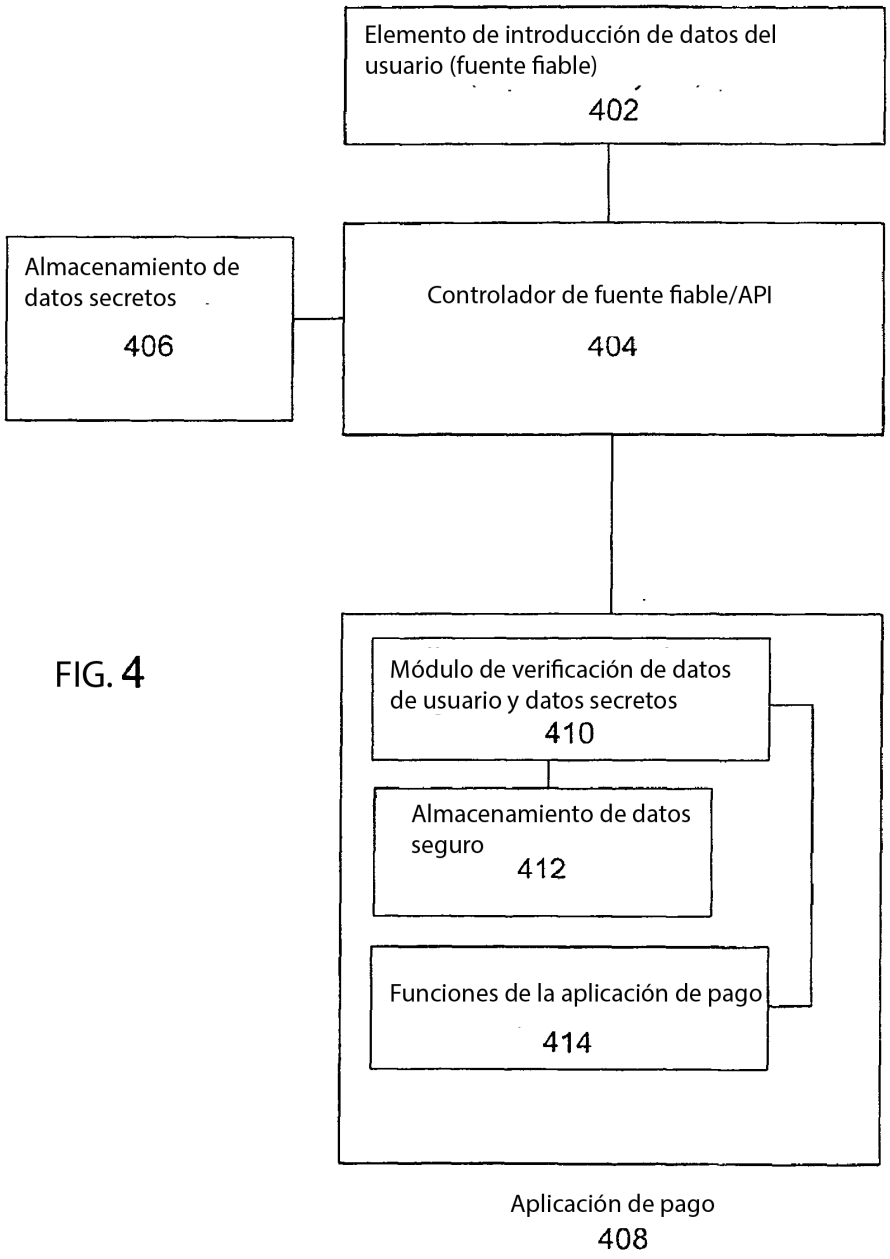
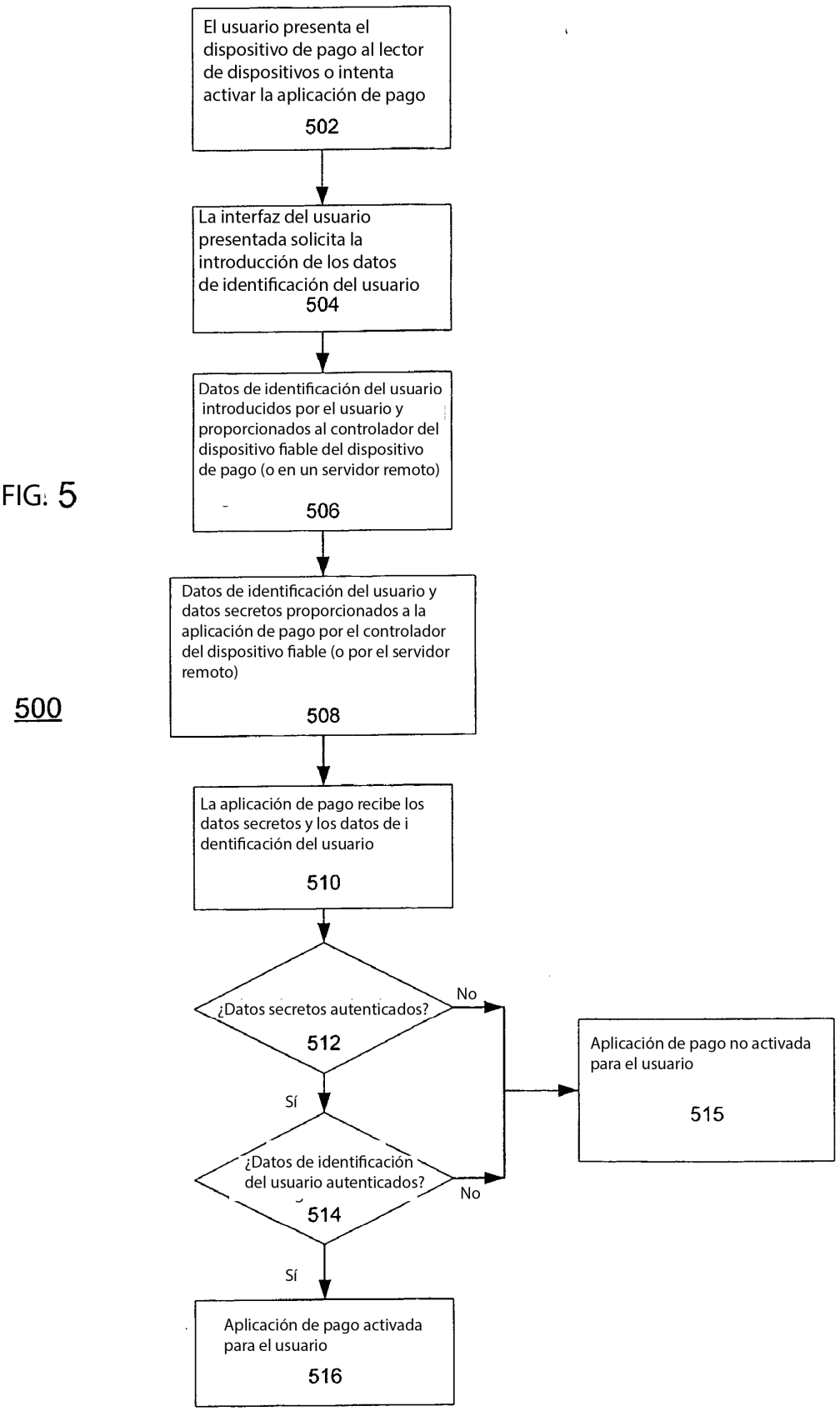

Elemento de introducción de datos del usuario (fuente fiable)
402
Almacenamiento de datos secretos
406
Controlador de fuente fiable/API
404
Módulo de verificación de datos de usuario y datos secretos
410
Almacenamiento de datos seguro
412
Funciones de la aplicación de pago
414
Aplicación de pago
408

FIG. 4

FIG. 5


500
El usuario presenta el dispositivo de pago al lector de dispositivos o intenta activar la aplicación de pago
502
La interfaz del usuario presentada solicita la introducción de los datos de identificación del usuario
504
Datos de identificación del usuario introducidos por el usuario y proporcionados al controlador del dispositivo fiable del dispositivo de pago (o en un servidor remoto)
506
Datos de identificación del usuario y datos secretos proporcionados a la aplicación de pago por el controlador del dispositivo fiable (o por el servidor remoto)
508
La aplicación de pago recibe los datos secretos y los datos de i dentificación del usuario
510
¿Datos secretos autenticados?
512
No
Sí
¿Datos de identificación del usuario autenticados?
514
No
Sí
Aplicación de pago no activada para el usuario
515
Aplicación de pago activada para el usuario
516