

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 707 370**

51 Int. Cl.:

**G06Q 20/00** (2012.01)

**H04B 1/40** (2015.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **22.09.2009** E 17169575 (2)

97 Fecha y número de publicación de la concesión europea: **07.11.2018** EP 3232386

54 Título: **Método de ejecutar transacciones con dispositivos de pago sin contacto que usan operaciones de pre-pulsación y de dos pulsaciones**

30 Prioridad:

**22.09.2008 US 99060 P**

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

**03.04.2019**

73 Titular/es:

**VISA INTERNATIONAL SERVICE ASSOCIATION  
(100.0%)  
900 Metro Center Blvd. Mail Stop: M1-5NW  
Foster City, CA 94404-2775, US**

72 Inventor/es:

**AABYE, CHRISTIAN;  
NGO, HAO y  
WILSON, DAVID**

74 Agente/Representante:

**ROEB DÍAZ-ÁLVAREZ, María**

ES 2 707 370 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Método de ejecutar transacciones con dispositivos de pago sin contacto que usan operaciones de pre-pulsación y de dos pulsaciones

5 Esta solicitud reivindica la prioridad de la solicitud de patente provisional de Estados Unidos N.º 61/099060, titulada "Contactless Phone With Secret Data", presentada el 22 de septiembre de 2008.

**Antecedentes**

10 El documento US 2008/064383 se refiere a un sistema y método de gestión de aplicación remota en terminales de datos inalámbricos usando un agente de gestión dinámico y bibliotecas de enlace dinámico proporcionadas por la aplicación. Las aplicaciones de terceros en un dispositivo inalámbrico pueden comunicarse y controlarse por un servidor de gestión remoto mediante una interfaz de enchufe de cliente de gestión.

15 El documento WO 2007/145540 describe un método de generar una ficha de autenticación usando una aplicación basada en criptografía descargada en un dispositivo de telefonía móvil y un método de autenticar una transacción en línea usando tal ficha. El método puede emplearse en un método de autenticación de dos factores utilizando una contraseña de usuario y una ficha de autenticación. El método permite proporcionar un método de autenticación de dos factores mediante un amplio intervalo de dispositivos de telefonía móvil que operan bien en línea o fuera de línea. Otros sistemas y métodos de autenticación también se divulgan.

20 El documento US 2005/187873 describe un sistema y método de teléfono móvil de inicializar, en un servidor de transacción segura (STS), un software de pago móvil con un parámetro de autenticación de software, como un software de pago móvil auténtico; proporcionar una correlación STS entre una entrada de identificación personal (PIE) y el software de pago móvil auténtico; instalar, en un teléfono móvil, el software de pago móvil auténtico; y enviar, por un usuario, la PIE al software de pago móvil auténtico instalado para generar según la PIE y el parámetro de autenticación de software una transacción monetaria sin efectivo de teléfono móvil autenticable segura y transformada sobre la red de teléfono móvil, como una cartera inalámbrica de teléfono móvil del usuario del teléfono móvil. La transacción monetaria sin efectivo autenticable de teléfono móvil se realiza según un protocolo de vista de acuerdo.

25 El documento US 2004/030601 describe un sistema para facilitar pagos electrónicos en un entorno de servicio alimentario usando un dispositivo móvil. El dispositivo móvil interactúa con un lector de proximidad para verificar al usuario tras la entrada en un establecimiento alimentario y el resto de la transacción tal como ordenar artículos y pagar dichos artículos se logra usando mensajes.

30 El documento US 2008/0508014 describe métodos, sistemas y productos de programa informático para la provisión sobre el aire de tarjetas blandas en dispositivos con capacidades de comunicaciones inalámbricas. Según un método, una aplicación de provisión de tarjeta blanda se ejemplifica en un dispositivo con capacidades de comunicaciones inalámbricas. Un número de tarjeta para una tarjeta blanda deseada a proporcionar en el dispositivo se obtiene desde un usuario del dispositivo. El número de tarjeta se comunica a un servidor de configuración de aprovisionamiento sobre una interfaz de aire. Unos desafíos específicos de servidor de tarjetas correspondientes al número de tarjeta y una dirección de red de servidor de servidor de aprovisionamiento se obtienen desde el servidor de configuración de aprovisionamiento. Los desafíos se presentan al usuario, y las respuestas del usuario a los desafíos se reciben. Una conexión se realiza con el servidor de servidor de aprovisionamiento correspondiente a la dirección de red. Las respuestas del desafío se comunican al servidor de servidor de aprovisionamiento. Los datos de personalización de tarjeta blanda para activar la tarjeta blanda se reciben desde el servidor de servidor de aprovisionamiento. La tarjeta blanda se proporciona para el uso en el dispositivo basándose en los datos de personalización.

35 Las realizaciones de la presente invención se refieren a sistemas, aparatos y métodos para ejecutar transacciones de pago, y más específicamente, a un sistema y un aparato y método asociados para ejecutar transacciones de pago usando un dispositivo de pago que incluye un elemento sin contacto (tal como un chip de circuito embebido en un dispositivo móvil inalámbrico) interactuando con un lector de dispositivos o terminal de punto de venta usando un proceso de pre-pulsación o de dos pulsaciones, individualmente o en combinación. Las realizaciones de la invención pueden usarse para realizar transacciones de pago, ejecutar actualizaciones de emisor de datos almacenados en un dispositivo de pago, o permitir la configuración de funciones u operaciones de un dispositivo de pago, entre otros posibles usos.

40 Los dispositivos de pago de consumidor se usan por millones de personas en todo el mundo para facilitar los diversos tipos de transacciones comerciales. En una transacción típica que involucra la compra de un producto o servicio en una localización de comerciante, el dispositivo de pago se presenta en un terminal de punto de venta ("terminal POS") localizado en el lugar de negocios del comerciante. El terminal POS puede ser un lector de tarjetas o un dispositivo similar que es capaz de acceder a los datos almacenados en el dispositivo de pago, donde estos datos pueden incluir, por ejemplo, datos de identificación o autenticación. Los datos leídos desde el dispositivo de

pago se proporcionan al sistema de procesamiento de transacciones del comerciante y a continuación al adquirente, que normalmente es un banco u otra institución que gestiona la cuenta del comerciante. A continuación, los datos proporcionados al adquirente pueden proporcionarse a una red de procesamiento de pagos que está en comunicación con los procesadores de datos que procesan los datos de transacción para determinar si la transacción debería autorizarse por la red y asistir en las funciones de liberación y liquidación de cuentas para las transacciones completadas. La decisión de autorización y las partes de liberación y liquidación de la transacción también pueden implicar la comunicación y/o la transferencia de datos entre la red de procesamiento de pagos y el banco o institución que emitió el dispositivo de pago al consumidor (conocido como emisor).

A pesar de que un dispositivo de pago de consumidor puede ser una tarjeta de crédito o tarjeta de débito, también puede tomar la forma de una tarjeta o chip "inteligente". Una tarjeta inteligente se define, en general, como una tarjeta de bolsillo (u otra forma de dispositivo de pago portátil) que está embebida en un microprocesador y uno o más chips de memoria, o está embebida en uno o más chips de memoria con lógica no programable. La tarjeta de tipo microprocesador normalmente puede implementar ciertas funciones de procesamiento de datos, tales como añadir, eliminar o manipular de otro modo la información almacenada en una localización de memoria en la tarjeta. Por el contrario, la tarjeta de tipo chip de memoria (por ejemplo, una tarjeta de teléfono de prepago) normalmente solo puede actuar como un archivo para contener datos que se manipulan por un dispositivo de lectura de tarjetas para ejecutar una operación predefinida, tal como cargar un cargo de un saldo preestablecido almacenado en la memoria. Las tarjetas inteligentes, a diferencia de las tarjetas de banda magnética (tales como las tarjetas de crédito estándar), pueden implementar una variedad de funciones y contener una variedad de tipos de información en la tarjeta. Por lo tanto, en algunas aplicaciones pueden no requerir acceso a una base de datos remota con el fin de autenticar a un consumidor o crear un registro en el momento de una transacción. Un chip inteligente es un dispositivo semiconductor que es capaz de ejecutar la mayoría, si no todas, las funciones de una tarjeta inteligente, pero puede estar embebido en otro dispositivo.

Las tarjetas o chips inteligentes vienen en dos variedades generales; el tipo de contacto y el tipo sin contacto. Una tarjeta o chip inteligente de tipo de contacto es aquél que incluye un elemento físico (por ejemplo, una banda magnética, un elemento de contacto, etc.) que permite el acceso a los datos y a las capacidades funcionales de la tarjeta, normalmente a través de algún tipo de terminal o lector de tarjetas. Por el contrario, una tarjeta o 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 la necesidad de contacto físico directo. De este modo, tales dispositivos pueden "desplazarse" eficazmente (es decir, están habilitados para leerse por o de otro modo intercambiar datos con otro dispositivo) pasándolos cerca de un lector de tarjetas o terminal. Las tarjetas o chips sin contacto normalmente se comunican con un lector de dispositivos o terminal usando la tecnología RF (radiofrecuencia), en el que la proximidad al lector o terminal permite la transferencia de datos entre la tarjeta o chip y el lector o terminal. Las tarjetas sin contacto han descubierto usos en la banca y otras aplicaciones, donde tienen la ventaja de no requerir la retirada de la cartera o el bolsillo de un usuario con el fin de participar en una transacción. Una tarjeta o chip sin contacto puede estar embebido en, o incorporado de otro modo, en un dispositivo móvil tal como un teléfono móvil o un asistente digital personal (PDA). Además, debido al creciente interés en tales tarjetas, se han desarrollado normas que rigen 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 se envían 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 accederse o procesarse por otros elementos del sistema de procesamiento de transacciones (por ejemplo, el adquirente del comerciante o un procesador de pagos que forma parte de una red de procesamiento de pagos). Obsérvese que en algunos casos, puede obtenerse la autorización para la transacción sin necesidad de conectarse con el emisor; esto puede permitirse por unos parámetros de gestión de riesgo configurados por el emisor que se han establecido en la aplicación de pago o en el dispositivo de pago de consumidor. Si se autoriza la transacción propuesta, entonces el consumidor puede proporcionar otra información al comerciante como parte de completar la transacción. El emisor o procesador de datos también puede enviar datos de nuevo al consumidor. Tales datos pueden incluir una actualización de los registros de las transacciones para las que se ha usado el dispositivo de pago o un saldo actual de una cuenta asociada con el dispositivo.

Un emisor o procesador de pagos también pueden desear configurar (o re-configurar) una función, una operación o un ajuste de una aplicación de pago que está instalada en un dispositivo de pago, tal como un dispositivo móvil que incluye un elemento sin contacto. Una acción de este tipo puede incluir restablecer un contador para habilitar o deshabilitar una función, configurar una función o la capacidad de la aplicación de pago o el dispositivo de pago, o iniciar la ejecución de una secuencia de comandos o aplicación que opera en la aplicación de pago, el dispositivo de pago o los datos de transacción, por ejemplo.

Un problema para cualquier sistema o proceso de transacción de pagos es la facilidad de uso por un consumidor, ya que esto conduce a un aumento de la adopción por el consumidor y el uso del sistema, generando de este modo más ingresos para los comerciantes y las entidades involucradas en la autorización y el procesamiento de transacciones de pago. Un consumidor normalmente desea que una transacción se ejecute con una cantidad

mínima de retraso y con una carga mínima para el consumidor. Además, si se requiere para una transacción, un consumidor desea poder localizar y activar una aplicación de pago en un dispositivo de pago con relativamente poco esfuerzo con el fin de iniciar la transacción. La preocupación por minimizar la carga para un consumidor es al menos en parte el resultado de reconocer que un consumidor normalmente no quiere ser molestado por dificultades en intentar activar una aplicación de pago o por tener que esperar un tiempo adicional mientras el sistema de procesamiento de transacciones realiza el procesamiento de los datos u otras funciones. Por lo tanto, con el fin de satisfacer los deseos y las expectativas de los consumidores, la mayoría de los sistemas de procesamiento de transacciones de pago están diseñados para requerir una mínima interacción por parte de los consumidores.

5  
10  
15  
20

Por ejemplo, en el caso de una transacción que usa un elemento sin contacto, se espera normalmente que un lector de dispositivos o terminal de punto de venta entre en comunicación con el elemento sin contacto durante solo un corto período de tiempo; por ejemplo, el tiempo suficiente para que se reconozca por el lector y para proporcionar los datos necesarios para iniciar o realizar una parte de la transacción. Sin embargo, esto significa que el dispositivo de pago de consumidor y el lector de dispositivos o terminal de punto de venta pueden no estar en comunicación durante un tiempo suficiente para que un emisor o procesador de pagos procese los datos de transacción y proporcione los datos procesados al lector de dispositivos para transferir al dispositivo consumidor. También puede significar que el dispositivo de pago y el lector de dispositivos o terminal no están en comunicación cuando el emisor o procesador de pagos desea ejecutar una actualización para hacer que se ejecute un comando o función en el dispositivo de pago, tal como para restablecer un contador, configurar una función de la aplicación de pago o del dispositivo de pago, etc.

25

Otro problema para un sistema o proceso de transacción de pagos en el que se proporcionan los datos o un comando o instrucción de configuración por un emisor o procesador de pago implica garantizar que los datos recibidos, comandos o instrucciones proceden de una parte autorizada, y que el dispositivo de pago asocia correctamente la información recibida con la transacción o la aplicación a la que se aplica la información.

30  
35

Lo que se desea es un sistema, aparato y método para permitir que un emisor o procesador de pagos proporcione un dispositivo de pago de consumidor que contiene un elemento sin contacto con los datos de transacción o para iniciar un proceso de actualización, sin necesidad de que un consumidor mantenga la comunicación entre el dispositivo de pago y un lector de dispositivos o terminal durante un período de tiempo prolongado. También se desea disponer de un sistema, aparato y método para permitir el lanzamiento automático de una aplicación de pago cuando se presenta un dispositivo de pago a un lector de dispositivos o terminal de punto de venta, donde esto puede incluir una determinación de si se requiere una interacción de consumidor antes de que pueda completarse una transacción. Las realizaciones de la invención abordan estos problemas y otros problemas individual y colectivamente.

### Sumario breve

40  
45  
50

Las realizaciones de la presente invención están dirigidas a un sistema, aparato, y método para usar un elemento sin contacto (tal como un chip inteligente sin contacto) como parte de una transacción de pago. Específicamente, las realizaciones de la presente invención están dirigidas a facilitar la transferencia de datos de transacciones o registros de transacciones a una memoria que es parte del dispositivo de pago. Las realizaciones de la presente invención también pueden usarse para proporcionar un comando o instrucción (a veces denominado "secuencia de comandos") al lector de dispositivos para su ejecución por el lector, o al dispositivo de pago para su ejecución por una aplicación de pago instalada en el dispositivo. Un comando o instrucción de este tipo puede usarse para restablecer o configurar una función de la aplicación de pago o del dispositivo de pago. El sistema, el aparato y el procedimiento de la invención pueden implementarse usando un chip inteligente sin contacto y un elemento de transferencia de datos inalámbrico (por ejemplo, un elemento que tiene una capacidad de comunicaciones de campo cercano (NFC) o una tecnología de comunicaciones de corto alcance similar, etc.) embebido dentro de un dispositivo inalámbrico móvil. El dispositivo móvil puede ser un teléfono móvil, PDA, reproductor de MP3 o similar.

55  
60  
65

Para garantizar que los datos, comandos o instrucciones recibidos por el dispositivo de pago proceden de una fuente autenticada y que la información recibida puede asociarse con los datos de transacción apropiados almacenados en el dispositivo de pago, las realizaciones de la presente invención pueden incluir el uso de un criptograma u otra forma de control de seguridad o datos de identificación. Por ejemplo, con el fin de garantizar que los datos proporcionados durante un proceso de actualización del emisor proceden de un emisor auténtico y que los datos recibidos están asociados correctamente a la transacción correcta, el dispositivo de pago puede generar un criptograma y proporcionar ese criptograma a un emisor como parte de una transacción. El emisor puede generar un segundo criptograma (basado o en el criptograma inicial del dispositivo de pago o mediante un proceso independiente) y proporcionar el segundo criptograma al dispositivo de pago como parte de cualquier dato, comando o instrucción enviado al dispositivo de pago como parte de un proceso de actualización del emisor. A continuación, el dispositivo de pago puede usar el criptograma recibido del emisor (junto con el criptograma inicial enviado al emisor, si es necesario) para confirmar la autenticidad del emisor y para asociar correctamente los datos recibidos con el registro de transacciones al que se aplica, donde se almacena el registro en el dispositivo de pago. El criptograma(s) puede generarse por cualquier método adecuado y puede almacenarse en una memoria en el dispositivo de pago y si se desea, borrarse después de la finalización de una transacción.

Las realizaciones de la invención permiten que un emisor o procesador de pagos proporcione datos de transacción y/o registros de transacciones a un dispositivo de pago que incluye un elemento sin contacto de una manera que minimiza el impacto sobre un consumidor. Esto se logra introduciendo una operación de dos pulsaciones, o una combinación de una operación de pre-pulsación y de dos pulsaciones en el proceso de transacción. La operación de pre-pulsación o de dos pulsaciones puede incluir un consumidor que presenta un dispositivo de pago a un lector de dispositivos o terminal de punto de venta una o más veces para activar una aplicación de pago o para permitir la transferencia de datos o un comando al dispositivo de pago o antes, durante o después de una transacción. Algunas o todas las presentaciones del dispositivo de pago que forman parte de la implementación de una operación de pre-pulsación o de dos pulsaciones pueden ser adicionales a o incluir una presentación que se usa normalmente para iniciar o ejecutar una transacción de pago (donde la presentación puede funcionar para transferir la identificación u otros datos de autenticación al lector de dispositivos o terminal).

En una realización, la presente invención está dirigida a un método de realizar una transacción de pago, donde el método incluye detectar la presencia de un dispositivo de pago usando una tecnología de comunicaciones de campo cercano de un lector de dispositivos o terminal, recibir datos de identificación de una cuenta de pago o un consumidor asociados con el dispositivo de pago, determinar que se requiere una interacción con el dispositivo de pago o un consumidor antes de ejecutar la transacción de pago, determinar que se ha ejecutado la interacción, detectar la presentación del dispositivo de pago usando la tecnología de comunicaciones de campo cercano del lector de dispositivos o terminal, y ejecutar la transacción de pago.

En otra realización, la presente invención está dirigida a un lector de dispositivos de terminal de punto de venta, donde el lector de dispositivos o terminal de punto de venta incluye un procesador, una memoria, y un conjunto de instrucciones almacenadas en la memoria, que cuando se ejecutan por el procesador implementan un método para detectar la presencia de un dispositivo de pago que usa una tecnología de comunicaciones de campo cercano, recibe los datos que identifican una cuenta de pago o un consumidor asociados con el dispositivo de pago, en respuesta a recibir los datos, determina que se requiere una interacción con el dispositivo de pago o un consumidor antes de ejecutar una transacción de pago, determina que se ha ejecutado la interacción, detecta la presentación del dispositivo de pago usando la tecnología de comunicaciones de campo cercano del lector de dispositivos o terminal y realiza la transacción de pago.

En otra realización más, la presente invención está dirigida a un método de realizar una transacción de pago, donde el método incluye detectar la presencia de un dispositivo de pago usando una tecnología de comunicaciones de campo cercano de un lector de dispositivos o terminal, y en respuesta a detectar la presencia del dispositivo de pago, activar una aplicación de pago instalada en el dispositivo de pago.

En otra realización más, la presente invención está dirigida a un lector de dispositivos o terminal de punto de venta, donde el lector de dispositivos o terminal de punto de venta incluye un procesador, una memoria, y un conjunto de instrucciones almacenadas en la memoria, que cuando se ejecutan por el procesador implementan un método para detectar la presencia de un dispositivo de pago usando una tecnología de comunicaciones de campo cercano de un lector de dispositivos o terminal, y en respuesta a la detección de la presencia del dispositivo de pago, se activa una aplicación de pago instalada en el dispositivo de pago.

Otros objetos y ventajas de la presente invención serán evidentes para un experto en la materia tras la revisión de la descripción detallada de la presente invención y las figuras incluidas.

**Breve descripción de los dibujos**

La figura 1 es un diagrama de bloques que ilustra un sistema de procesamiento de transacciones que puede usarse con algunas realizaciones de la presente invención;

La figura 2 es un diagrama de bloques funcional que ilustra los componentes primarios de un sistema para iniciar o facilitar una transacción de pago usando un elemento sin contacto contenido dentro de un dispositivo móvil y una operación de pre-pulsación y/o de dos pulsaciones, de acuerdo con algunas realizaciones del presente invención;

La figura 3 es un diagrama de bloques funcional que ilustra los componentes primarios de un dispositivo móvil, tal como un teléfono móvil que puede usarse como parte del sistema y método de la invención;

La figura 4 es un diagrama de flujo que ilustra una realización del método o proceso inventivo para ejecutar una transacción de pago que usa un elemento sin contacto contenido dentro de un dispositivo móvil implementando una operación de pre-pulsación y/o de dos pulsaciones;

La figura 5 es un diagrama de flujo que ilustra un proceso para determinar si se requiere una interacción con un dispositivo de pago de consumidor antes de que el dispositivo se use para realizar una transacción de pago, de acuerdo con algunas realizaciones de la presente invención; y

La figura 6 es un diagrama de bloques de un aparato informático a modo de ejemplo que puede usarse para implementar una realización del método o proceso inventivo para ejecutar una transacción de pago con un dispositivo de pago sin contacto usando una operación de pre-pulsación y/o de dos pulsaciones.

5 **Descripción detallada**

10 Las realizaciones de la presente invención están dirigidas a un sistema, aparato y método para procesar las transacciones de pago que se realizan usando un dispositivo de pago móvil que incluye un elemento sin contacto, tal como un chip de circuito integrado. Las realizaciones de la invención permiten una o más de entre las operaciones de activación de una aplicación de pago, de transferencia de datos de transacción, de actualización de registros de cuentas, de establecimiento o restablecimiento de un contador o registro de aplicación de pago, o de transferencia o procesamiento de una secuencia de comandos, un comando, o una instrucción, ejecutándose estas funciones con un impacto mínimo en un consumidor. Esto se logra introduciendo una operación de pre-pulsación y/o de dos pulsaciones antes de o como parte del flujo de transacción. El resultado es acelerar el proceso de transacción de pagos para un consumidor que usa un dispositivo de pago sin contacto, al tiempo que facilita la capacidad de un emisor o procesador de pagos para actualizar los registros de transacciones o habilitar, deshabilitar o configurar de otra forma una aplicación de pago o el dispositivo consumidor.

20 Además, para garantizar que los datos, comandos o instrucciones recibidos por el dispositivo de pago proceden de una fuente autenticada y que la información recibida puede asociarse con los datos de transacción apropiados almacenados en el dispositivo de pago, las realizaciones de la presente invención pueden incluir el uso de un criptograma u otra forma de control de seguridad o datos de identificación. Por ejemplo, el dispositivo de pago puede generar un criptograma y proporcionar ese criptograma a un emisor como parte de una transacción. El emisor puede generar un segundo criptograma (basado o en el criptograma inicial procedente del dispositivo de pago o por un proceso independiente) y proporcionar el segundo criptograma al dispositivo de pago como parte de cualquier dato, comando o instrucción enviado al dispositivo de pago durante un proceso de actualización de emisor. A continuación, el dispositivo de pago puede usar el criptograma recibido del emisor (junto con el criptograma inicial enviado al emisor, si es necesario) para confirmar la autenticidad del emisor y para asociar correctamente los datos recibidos con el registro de transacciones al que se aplica, donde ese registro se almacena en el dispositivo de pago. El criptograma(s) puede generarse mediante cualquier método adecuado y puede almacenarse en una memoria en el dispositivo de pago y, si se desea, borrarse después de la finalización de una transacción para la que se generó el criptograma.

35 La presente invención se implementa normalmente en el contexto de una transacción de pago; por lo tanto antes de describir una o más realizaciones de la invención con mayor detalle, se presentará una breve exposición de las entidades implicadas en el procesamiento y autorización de una transacción de pago y sus funciones en el proceso de autorización.

40 La figura 1 es un diagrama de bloques que ilustra un sistema de procesamiento de transacciones que puede usarse con algunas realizaciones de la presente invención. Normalmente, se autoriza una transacción de pago electrónico si el consumidor que realiza la transacción está autenticado correctamente (es decir, se verifica su identidad y su uso válido de una cuenta de pago) y si el consumidor tiene suficientes fondos o crédito para realizar la transacción. Por el contrario, si no hay suficientes fondos o crédito en la cuenta del consumidor, o si el dispositivo de pago del consumidor está en una lista negativa (se indica, por ejemplo, que posiblemente se ha robado), entonces no puede autorizarse una transacción de pago electrónico. En la siguiente descripción, un "adquiriente" es normalmente una entidad de negocios (por ejemplo, un banco comercial) que tiene una relación comercial con un comerciante específico. Un "emisor" es normalmente una entidad de negocios (por ejemplo, un banco) que emite un dispositivo de pago (tal como una tarjeta de crédito o de débito) a un consumidor. Algunas entidades pueden ejecutar tanto las funciones de emisor como de adquiriente.

55 La figura 1 ilustra los elementos funcionales primarios que normalmente están implicados en el procesamiento de una transacción de pago y en el proceso de autorización para una transacción de este tipo. Como se muestra en la figura 1, en una transacción de pago típica, un consumidor que desea comprar un bien o servicio de un comerciante usa un dispositivo de pago de consumidor portátil 20 para proporcionar los datos de transacción de pagos que pueden usarse como parte de un proceso de autenticación o de autorización de transacción de consumidor. El dispositivo de pago de consumidor portátil 20 puede ser una tarjeta de débito, una tarjeta de crédito, una tarjeta inteligente, un dispositivo móvil que contenga un chip sin contacto u otra forma adecuada de dispositivo.

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

el historial de transacciones del consumidor con el comerciante. El sistema de procesamiento de transacciones comerciales 26 se comunica normalmente con el adquirente 30 (que gestiona las cuentas del comerciante) como parte del proceso de autenticación o autorización general. El sistema de procesamiento de transacciones comerciales 26 y/o el adquirente 30 proporcionan datos a la red de procesamiento de pagos 34 que, entre otras funciones, participa en los procesos de liberación y liquidación que forman parte del proceso de transacción general. La comunicación y la transferencia de datos entre el sistema de procesamiento de transacciones comerciales 26 y la red de procesamiento de pagos 34 son normalmente por medio de un intermediario, tal como el adquirente 30. Como parte del proceso de autorización de transacción o autenticación de consumidor, la red de procesamiento de pagos 34 puede acceder a la base de datos de cuentas 36, que normalmente contiene información con respecto al historial de pagos de cuentas del consumidor, el historial de devolución de cargo o de transacción, la solvencia crediticia, etc. La red de procesamiento de pagos 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 para el consumidor y gestiona la cuenta del consumidor. Los datos de cuenta de cliente o consumidor se almacenan normalmente en la base de datos de clientes/consumidores 40 a la que el emisor 38 puede acceder como parte de los procesos de autenticación, autorización o gestión de cuentas. Obsérvese que en lugar de, o además de estar almacenados en la base de datos de cuentas 36, los datos de cuenta de consumidor pueden incluirse o de otro modo formar parte de la base de datos cliente/consumidor 40.

En las operaciones normales, se crea un mensaje de solicitud de autorización durante una compra del consumidor de un bien o servicio en un punto de venta (POS) usando un dispositivo de pago de consumidor portátil. En algunas realizaciones, el dispositivo de pago de consumidor portátil puede ser un teléfono inalámbrico o un asistente digital personal que incorpora una tarjeta o chip sin contacto. La tarjeta o chip sin contacto puede comunicarse con el terminal de punto de venta usando una capacidad de comunicaciones de campo cercano (NFC). El mensaje de solicitud de autorización se envía normalmente desde el lector de dispositivos/terminal POS 22 a través del sistema de procesamiento de datos 26 del comerciante al adquirente 30, a una red de procesamiento de pagos 34 y a continuación a un emisor 38. Un "mensaje de solicitud de autorización" puede incluir una solicitud de autorización para realizar una transacción de pago electrónico y los datos pertinentes para determinar si debería concederse la solicitud. Por ejemplo, puede incluir uno o más de un número de cuenta de pago de titular de cuenta, código de moneda, importe de venta, sello de transacción comercial, ciudad del aceptante, estado/país del aceptante, etc. Un mensaje de solicitud de autorización puede protegerse usando un método de cifrado seguro. Por ejemplo, SSL de 128 bits o equivalente) con el fin de evitar el acceso no autorizado a los datos de cuentas o transacciones.

Después de que el emisor reciba el mensaje de solicitud de autorización, el emisor determina si la transacción debería autorizarse y envía un mensaje de respuesta de autorización de vuelta a la red de procesamiento de pagos para indicar si se autoriza o no la transacción actual. A continuación, el sistema de procesamiento de pagos reenvía el mensaje de respuesta de autorización al adquirente. A continuación, el adquirente envía el mensaje de respuesta al comerciante. De este modo, se informa al comerciante de si el emisor ha autorizado la transacción y, por lo tanto, si puede completarse la transacción.

En un momento posterior, puede realizarse un proceso de liberación y liquidación por los elementos del sistema de procesamiento de pago/transacción representado en la figura 1. Un proceso de liberación implica el intercambio de datos financieros entre un adquirente y un emisor para facilitar la publicación de una transacción a un consumidor y reconciliar la posición de liquidación del consumidor. La liberación y liquidación pueden producirse simultáneamente o como procesos separados.

La red de procesamiento de pagos 34 puede incluir subsistemas de proceso de datos, redes, y otros medios de implementar operaciones usadas para soportar y entregar servicios de autorización, servicios de archivos de excepción, y servicios de liberación y liquidación de transacciones de pago. Una red de procesamiento de pagos a modo de ejemplo puede incluir VisaNet. Las redes de procesamiento de pagos como VisaNet pueden procesar transacciones con tarjetas de crédito, transacciones con tarjetas de débito y otros tipos de transacciones comerciales. VisaNet, en particular, incluye un sistema VIP (sistema de pagos integrados de Visa) que procesa solicitudes de autorización de transacciones y un sistema Base II que ejecuta servicios de liberación y liquidación de transacciones.

La red de procesamiento de pagos 34 puede incluir un ordenador servidor. Un ordenador servidor es normalmente un ordenador potente o un grupo de ordenadores. Por ejemplo, el ordenador servidor puede ser un mainframe grande, un clúster de minicomputadoras o un grupo de servidores que funcionan como una unidad. En un ejemplo, el ordenador servidor puede ser un servidor de base de datos acoplado a un servidor web. La red de procesamiento de pagos 34 puede usar cualquier combinación adecuada de redes cableadas o inalámbricas, incluida Internet, para permitir la comunicación y la transferencia de datos entre elementos de red. Entre otras funciones, la red de procesamiento de pagos 34 puede ser responsable de garantizar que un consumidor esté autorizado para realizar una transacción (a través de un proceso de autenticación), confirmar la identidad de una parte en una transacción (por ejemplo, mediante la recepción de un número de identificación personal) confirmar un saldo o una línea de crédito suficiente para permitir una compra, o reconciliar el importe de una compra con la cuenta del consumidor (a través de la introducción de un registro del importe de la transacción, la fecha, etc.).

El dispositivo de pago de consumidor 20 puede tomar una de las muchas formas adecuadas. Como se ha mencionado, el dispositivo de consumidor portátil puede ser un dispositivo móvil que incorpora un elemento sin contacto tal como un chip para almacenar datos de pagos (por ejemplo, un número BIN, un número de cuenta, etc.) y un elemento de transferencia de datos de comunicaciones de campo cercano tal como una antena, un diodo emisor de luz, un láser, etc. El dispositivo portátil de consumidor también puede incluir un dispositivo del tamaño de un llavero (tal como el Speedpass™ comercialmente disponible en Exxon-Mobil Corp.), etc. El dispositivo que contiene la tarjeta o chip sin contacto, u otro elemento de almacenamiento de datos puede ser un teléfono móvil, un asistente digital personal (PDA), un buscapersonas, un transpondedor o similares. El dispositivo de consumidor portátil también puede incorporar la capacidad de ejecutar funciones de débito (por ejemplo, una tarjeta de débito), funciones de crédito (por ejemplo, una tarjeta de crédito) o funciones de valor almacenadas (por ejemplo, un valor almacenado o una tarjeta teléfono de prepago).

En las realizaciones de la invención que incluyen un elemento sin contacto (por ejemplo, un chip sin contacto y un elemento de transferencia de datos de comunicaciones de campo cercano) embebido dentro de un teléfono móvil inalámbrico o dispositivo similar, el elemento sin contacto pueden comunicarse con el lector de dispositivos del comerciante o terminal de punto de venta usando un método de comunicación de corto alcance, tal como una capacidad de comunicaciones de campo cercano (NFC). Ejemplos de tales tecnologías de NFC o tecnologías de comunicaciones de corto alcance similares incluyen los métodos de comunicaciones norma ISO 14443, RFID, Bluetooth™ e infra-rojos.

La figura 2 es un diagrama de bloques funcional que ilustra los componentes primarios de un sistema para iniciar o facilitar una transacción de pago usando un elemento sin contacto contenido dentro de un dispositivo móvil y una operación de pre-pulsación o de dos pulsaciones, de acuerdo con algunas realizaciones de la presente invención. Como se muestra en la figura 2, el sistema 100 incluye un dispositivo móvil 102 que tiene capacidades de comunicaciones inalámbricas 122. El dispositivo móvil 102 puede ser un teléfono móvil inalámbrico, PDA, ordenador portátil, buscapersonas, etc. En una realización típica, el dispositivo móvil 102 es un teléfono móvil, aunque como se ha indicado, la implementación de la presente invención no se limita a esta realización en la medida que el dispositivo móvil que funciona como un dispositivo de pago puede adoptar cualquier forma adecuada conveniente para su uso por un consumidor. Naturalmente, si el dispositivo móvil no es un teléfono móvil o forma similar de dispositivo de comunicaciones inalámbricas, entonces el dispositivo móvil puede no ser capaz de una comunicación usando una red inalámbrica o móvil. En el caso de un teléfono móvil como el dispositivo móvil 102, el dispositivo incluye una circuitería de dispositivo móvil (teléfono móvil) 104 que permite ciertas de las funciones de telefonía. Entre otras funciones, la circuitería de dispositivo móvil 104 permite que el dispositivo móvil 102 se comunique de manera inalámbrica con sistema móvil (es decir, un operador inalámbrico) 120 a través de la red móvil 122.

El dispositivo móvil 102 incluye además un elemento sin contacto 106, implementado normalmente en la forma de un chip semiconductor. El elemento sin contacto 106 puede incluir un elemento de almacenamiento de datos seguro 110, aunque el elemento de almacenamiento de datos seguro 110 también puede implementarse como un elemento separado del elemento sin contacto 106. El elemento sin contacto 106 incluye un elemento (por ejemplo, transmisión de datos) de transferencia de datos de comunicaciones de campo cercano (NFC) 105, tal como una antena o transductor. Como se describirá, la capacidad de comunicaciones de campo cercano permite que un lector de dispositivos o terminal de punto de venta intercambie datos con (o ejecutar operaciones en) un elemento sin contacto 106 como parte de, o en preparación para, una transacción de pago. En algunas realizaciones, el elemento sin contacto 106 puede estar embebido dentro de e integrado con los elementos del dispositivo móvil 102. En tal caso, los datos o las instrucciones de control pueden transmitirse opcionalmente a través de la red móvil 122 y pueden intercambiarse con, o aplicarse a, el elemento sin contacto 106 por medio de la interfaz de elemento sin contacto 108. En esa situación, la interfaz de elemento sin contacto 108 funciona para permitir el intercambio de datos y/o instrucciones de control entre la circuitería de dispositivo móvil 104 (y por tanto de la red celular) y el elemento sin contacto 106. Por lo tanto, el elemento sin contacto 106 puede incluir la capacidad de almacenamiento de datos en la forma de una memoria o almacenamiento de datos seguro 110 que pueda accederse a través de una capacidad o interfaz de comunicaciones de campo cercano 108 para permitir, por ejemplo, la implementación de las funciones de lectura, escritura y borrado de datos.

El almacenamiento de datos seguro 110 puede usarse por el dispositivo móvil 102 para almacenar parámetros de funcionamiento u otros datos utilizados en la operación del dispositivo. El almacenamiento de datos seguro 110 puede usarse también para almacenar otros datos para el que se desea una mayor seguridad, por ejemplo, datos de transacción, datos de cuenta personal, datos de identificación, datos de autenticación, datos de control de acceso para una función de aplicación o dispositivo, etc. Como se ha mencionado, el almacenamiento de datos seguro 110 puede implementarse en la forma de un chip que está separado y aparte del elemento sin contacto 106, o como alternativa, puede ser una sección de memoria en un chip que forma parte del elemento sin contacto 106. Obsérvese también que el almacenamiento de datos seguro y/o el elemento sin contacto contenido dentro del dispositivo móvil puede ser un elemento removible o puede estar integrado dentro del dispositivo móvil. Ejemplos de elementos removibles 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 entre software, firmware o hardware. Las aplicaciones 109 se usan para implementar diversas funciones deseadas por un consumidor, donde tales funciones pueden incluir, pero no se limitan a, las operaciones de transacción de comercio electrónico, las operaciones de transacción de pagos, etc. Normalmente, las aplicaciones 109 representan procesos u operaciones que se dedican a una función específica que proporciona un valor añadido para el consumidor y que no son parte del funcionamiento convencional del dispositivo (es decir, no son parte de permitir que las funciones de telefonía convencionales, por ejemplo). Como se muestra en la figura, las aplicaciones 109 pueden intercambiar datos con el almacenamiento de datos seguro 110 (a través de la interfaz de elemento sin contacto 108), y también pueden ser capaces de intercambiar datos con la circuitería de dispositivo móvil 104. Una aplicación típica 109 para los fines de la presente invención es una aplicación de pago que permite a un consumidor hacer un pago de una transacción, cuando la transacción se realiza- total o parcialmente usando el dispositivo móvil. En un ejemplo de este tipo, el almacenamiento de datos seguro 110 puede contener datos de autenticación, datos de identificación de consumidor, datos de registro de transacción, datos de saldo de cuenta, etc. Las aplicaciones 109 normalmente se almacenan como un conjunto de instrucciones ejecutables en la memoria 107, que también puede incluir el almacenamiento de datos 113. Un procesador accede a la memoria 107 para cargar y descargar las instrucciones y los datos según sea necesario para ejecutar las instrucciones para realizar las funciones de las aplicaciones.

El elemento sin contacto 106 es capaz de transferir y recibir datos usando el elemento de transferencia de datos 105 que implementa una capacidad de comunicaciones de campo cercano 112, normalmente de acuerdo con un protocolo estandarizado o un mecanismo de transferencia de datos (identificado como ISO 14443/NFC en la figura). La capacidad de comunicaciones de campo cercano 112 es una capacidad de comunicaciones de corto alcance, tales como RFID, Bluetooth™, infrarrojos, u otra capacidad de transferencia de datos que puede usarse para intercambiar datos entre el dispositivo móvil 102 y un lector de dispositivos o terminal de punto de venta 130, que normalmente se localiza en el negocio del comerciante. Por lo tanto, en algunas realizaciones, el dispositivo móvil 102 es capaz de comunicar y transferir instrucciones de datos y/o de control a través tanto de la red móvil 122 como de la capacidad de comunicaciones de campo cercano 112, aunque como se ha observado, no se requieren comunicaciones y transferencia de datos por medio de la red móvil con el fin de implementar algunas realizaciones de la presente invención.

El sistema 100 incluye además un adquiriente 132 que está en comunicación con el comerciante o con el lector de dispositivos o terminal de punto de venta del comerciante 130. El adquiriente 132 está en comunicación con la red de procesamiento de pagos 134 y como se ha descrito, puede intercambiar datos con la red de procesamiento de pagos 134 como parte del proceso de autorización de transacción. La red de procesamiento de pagos 134 también está en comunicación con el emisor 136. Como se ha descrito, el emisor 136 puede intercambiar datos con la red de procesamiento de pagos 134, como parte de un proceso de reconciliación de autenticación, autorización de transacción, o transacción.

El sistema 100 también puede incluir una pasarela móvil 138, que es capaz de acoplar la red o sistema móvil (inalámbrica) con una segunda red (normalmente una red cableada, tal como Internet) y que permite la transferencia de datos entre las redes. La pasarela móvil 138 puede realizar operaciones de procesamiento de datos según sea necesario para permitir la transferencia eficaz de datos entre los dos tipos de redes, incluyendo, pero no limitado a, reformatear datos u otro procesamiento para tener en cuenta las diferencias en los protocolos de red. La pasarela móvil 138 también puede ejecutar las operaciones de procesamiento de datos para permitir la transferencia de datos más eficaz entre las redes y los dispositivos acoplados a cada tipo de red, tal como para fines de mejorar la capacidad de un consumidor para utilizar los datos recibidos en un dispositivo móvil. Como se muestra en la figura, en algunas realizaciones, la pasarela móvil 138 está acoplada a la red de procesamiento de pagos 134, que está acoplada al adquiriente 130. Téngase en cuenta que son posibles otras realizaciones, tales como cuando la pasarela móvil 138 está acoplada al emisor 136, así como cuando el adquiriente 130 está acoplado al emisor 136. Del mismo modo, el emisor 136 puede incluir la capacidad de funcionar como una pasarela móvil 138.

El sistema de la invención 100 proporciona una forma eficaz para que un consumidor realice una transacción de pago usando un elemento sin contacto. Como se describirá, usando la capacidad de comunicaciones de campo cercano (o una tecnología de transferencia de datos de corto alcance similar) y un proceso de pre-pulsación, un proceso de dos pulsaciones, o una combinación de los dos procesos, un consumidor puede realizar una transacción de pago sin contacto de una manera que tenga un impacto mínimo e imponga una carga mínima en el consumidor. Las realizaciones de la presente invención facilitan el uso de un elemento sin contacto para las transacciones de pago de una manera que es conveniente para el consumidor mientras que se mantiene la capacidad de un emisor o procesador de pagos para actualizar o restablecer los contadores o registros de la aplicación de pago, o para realizar otra operación en el dispositivo de pago, la aplicación de pago, o los datos almacenados en el dispositivo. Tales datos pueden incluir los datos de gestión de autenticación y de cuenta, tales como los registros de transacciones o saldos de cuentas. Por ejemplo, un almacén de datos seguro (por ejemplo, el almacenamiento de datos seguro 110 o una región de memoria de seguridad similar que es parte del elemento sin contacto o de otro elemento del dispositivo móvil) puede contener registros de transacciones y un total acumulado del saldo disponible para una cuenta del consumidor. En el caso del elemento sin contacto que se usa con una tarjeta o cuenta de prepago, el saldo reflejaría la cantidad restante de dinero disponible para un consumidor. En el caso del elemento sin contacto que se usa con una cuenta de crédito o débito, el saldo reflejaría un límite de crédito restante o la

cantidad disponible en la cuenta de débito.

Las realizaciones de la presente invención proporcionan un mecanismo para ejecutar eficazmente una transacción de pago que usa un elemento sin contacto introduciendo una operación de pre-pulsación y/o de dos pulsaciones como un preludio a (en el caso de un pre-pulsación), como se parte de, o después de, la transacción de pago. En algunas realizaciones, un dispositivo de pago puede presentarse a un lector de dispositivos o terminal de punto de venta (POS) antes de la iniciación de una transacción, durante una transacción, o después de una transacción, con el dispositivo que se presentan en una o más de estas situaciones. Entre otros usos, la presentación del dispositivo de pago puede usarse para lanzar una aplicación de pago, permitir una transacción, proporcionar los datos de transacción al dispositivo, o para restablecer o configurar una función u operación de la aplicación de pago o del dispositivo de pago. Obsérvese que en el contexto de la presente invención, presentar el dispositivo a un lector de dispositivos o terminal POS será denominado como una “pulsación”, donde una pulsación incluye cualquier acción por un consumidor que permite la comunicación entre el dispositivo de pago del consumidor y un lector de dispositivos o terminal POS usando un mecanismo de comunicaciones de corto alcance o campo cercano (incluyendo agitar el dispositivo de consumidor cerca de un lector de dispositivos o terminal, colocar el dispositivo de consumidor contra un lector de dispositivos o terminal, etc.).

Como parte de facilitar una transacción de pago usando un elemento sin contacto, puede usarse una operación de pre-pulsación para activar una aplicación de pago, establecer o restablecer un contador o registro que es parte de una aplicación de pago, solicitar que una interacción de consumidor (u otra forma de interacción) a ejecutar antes de realizar la transacción de pago, o configurar o reconfigurar una aplicación de pago o una función de dispositivo de pago que se requiere con el fin de usar una aplicación de pago. Obsérvese que en el contexto de la presente invención, una pre-pulsación se refiere a un proceso donde un consumidor presenta su dispositivo de pago a un lector de dispositivos o terminal POS, y en lugar de iniciar una transacción de pago, la “pulsación” funciona para iniciar un proceso para preparar el dispositivo de pago para la transacción (tal como, activando una aplicación de pago), realizar funciones de mantenimiento de datos, solicitar una acción de consumidor, o una operación similar. En el contexto de la invención, un proceso de dos pulsaciones puede usarse donde se usa una primera pulsación para realizar una transacción de pago (por ejemplo transfiriendo los datos de identidad o de autenticación del consumidor al lector de dispositivos o terminal POS), seguido de una segunda pulsación en un momento posterior para permitir que los datos proporcionados por un emisor o procesador de pagos se transfieran a la aplicación de pago o al dispositivo de pago (como puede ocurrir como parte de una operación de actualización de emisor). Además, un proceso de pre-pulsación o dos pulsaciones puede usarse para permitir la ejecución de una secuencia de comandos proporcionada por un emisor o procesador de pagos, cuando la secuencia de comandos provoca la ejecución de una función u operación deseada por la aplicación de pago, o la aplicación de una función u operación deseada por un lector de dispositivos para el dispositivo de pago. En algunas realizaciones, puede usarse una pre-pulsación inicial usada en combinación con una presentación única de pulsación posterior del dispositivo de pago, o dos presentaciones del dispositivo para habilitar una aplicación de pago o un dispositivo de pago a configurarse correctamente para su uso en una transacción y para permitir la ejecución de una transacción (o parte de la misma) después de la finalización de la operación de configuración.

Los procesos o métodos de la invención pueden desearse (y en algunos casos de uso pueden ser necesarios) cuando se usa un elemento sin contacto para una transacción de pago. Esto es debido a que el procesamiento de la transacción de pago típico para transacciones que usan un elemento sin contacto no se basan en el elemento que es capaz de la comunicación con un lector de dispositivos o terminal POS durante más de un breve período de tiempo. Esto se hace para minimizar el impacto en un consumidor y para reducir cualquier inconveniente que podría crear un desincentivo al consumidor para participar en las transacciones usando el dispositivo. Sin embargo, ciertas operaciones o funciones que pueden desearse por un emisor o procesador de pagos como parte de la iniciación o el procesamiento de una transacción de pago son difíciles o no realistas de implementar a menos que un consumidor presente su dispositivo de pago durante un período de tiempo más largo. Las realizaciones de la presente invención proporcionan una forma de implementar estas operaciones o funciones sin tener un impacto negativo en la experiencia del consumidor, y por lo tanto sin crear un desincentivo a un consumidor que utilice el dispositivo de pago sin contacto.

En las realizaciones de la presente invención, el dispositivo de pago móvil puede ser cualquier dispositivo que incluye un elemento sin contacto capaz de la comunicación y la transferencia de datos usando un sistema de comunicación de campo cercano. Como se ha señalado, un ejemplo es un teléfono inalámbrico móvil equipado con una capacidad de NFC u otra tecnología de comunicaciones de corto alcance. La figura 3 es un diagrama de bloques funcional que ilustra los componentes primarios de un dispositivo de consumidor portátil (por ejemplo, el elemento 102 de la figura 2), tal como un teléfono móvil que puede usarse como parte del sistema y el método de la invención. Como se ilustra en la figura 3, el dispositivo móvil 302 puede incluir una circuitería que se usa para permitir cierta telefonía y otras funciones de dispositivo. Los elementos funcionales son responsables de permitir que esas funciones puedan 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 (o a otra región o elemento de memoria adecuado) para recuperar las instrucciones o los datos usados en la ejecución de las instrucciones. Los elementos de entrada/salida de datos 308 pueden usarse para permitir a un usuario introducir datos (por ejemplo, a través de un micrófono o un teclado) o recibir datos de salida (por ejemplo, a través de un altavoz). La pantalla 306 puede usarse también para los datos de salida a un usuario. El elemento de

comunicaciones 310 puede usarse para permitir la transferencia de datos entre el dispositivo 302 y una red inalámbrica (por ejemplo, a través de la antena 318) para ayudar a permitir las funciones de telefonía y de transferencia de datos. Como se ha descrito haciendo referencia a la figura 2, el dispositivo 302 puede incluir también una interfaz de 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 comunicaciones de campo cercano u otro elemento de transferencia de datos de comunicaciones de corto alcance. El elemento sin contacto puede implementar una capacidad de comunicaciones de campo cercano o de otras comunicaciones de corto alcance que permiten la comunicación y la transferencia de datos entre el dispositivo 302 y un lector de dispositivos o terminal POS que es parte de un sistema de procesamiento de transacción de pagos.

El almacenamiento de datos 312 puede ser una memoria que almacena datos, y puede estar en cualquier forma adecuada incluyendo un chip de memoria, etc. La memoria puede usarse para almacenar datos tales como la identificación de usuario o la información de autenticación, la información de cuenta de usuario, datos de transacción, etc. La información financiera almacenada puede incluir información tal como información de cuenta bancaria, número de identificación bancaria (BIN), la información del número de cuenta de tarjeta de crédito o de débito, la información de saldo de cuenta, la fecha de caducidad, la información del consumidor tal como nombre, la fecha de nacimiento, etc. Obsérvese que tales datos pueden, en su lugar o también, almacenarse en un elemento de almacenamiento de datos seguro, tal como el almacenamiento de datos seguro 110 de la figura 2 o en una memoria segura similar que es parte de elemento sin contacto 316. Como se ha descrito, el almacenamiento de datos 312 puede contener también instrucciones que cuando se ejecutan por el procesador 304 implementan operaciones o procesos que son parte del funcionamiento del dispositivo o de las aplicaciones instaladas en el dispositivo.

La figura 4 es un diagrama de flujo que ilustra una realización 400 del método o proceso de la invención para ejecutar una transacción de pago usando un elemento sin contacto contenido dentro de un dispositivo móvil implementando una operación de pre-pulsación y/o de dos pulsaciones. Las etapas o fases del proceso ilustradas en la figura pueden implementarse como una rutina o proceso independiente, o como parte de una rutina o proceso más grande. Obsérvese que cada etapa o fase del proceso representada puede implementarse como un aparato que incluye un procesador que ejecuta un conjunto de instrucciones, un método, o un sistema, entre otras realizaciones.

Como se muestra en la figura, en la fase 402 un consumidor presenta su dispositivo de pago móvil a un lector de dispositivos o terminal de punto de venta (POS). El dispositivo móvil funciona como un dispositivo de pago e incluye un elemento sin contacto, tal como un chip sin contacto. Normalmente, el consumidor presenta su dispositivo móvil al lector de dispositivos o terminal POS como parte de la provisión de datos para iniciar o participar en una transacción de pago. Sin embargo, de acuerdo con las realizaciones de la presente invención, la presentación del dispositivo de pago (es decir, una "pulsación") puede servir también para otras funciones.

En una realización, la presentación del dispositivo de pago puede usarse para activar o "lanzar" una aplicación de pago instalada en el dispositivo de pago móvil (etapa 404). Esto puede lograrse haciendo que la comunicación entre el lector de dispositivos o terminal POS y el dispositivo de pago dispare la activación de la aplicación de pago. Tal disparo o activación puede producirse como el resultado de los datos transferidos del lector de dispositivos o terminal POS o de un comando para el dispositivo de pago (tal como ejecutando el equivalente de una clave de activación o una tecla programada), ya sea o automáticamente o en respuesta, por ejemplo, a un consumidor que selecciona un icono de aplicación de pago en una pantalla de lector de dispositivos o terminal POS. Obsérvese que la activación de la aplicación de pago en esta fase es opcional, y puede implementarse en una fase diferente en el proceso.

Además, en función de la operación del proceso representado en la figura 4, la activación de la aplicación de pago puede o no puede ser necesaria con el fin de poder implementar una o más de las otras fases del proceso global. Por ejemplo, en algunas realizaciones, puede necesitar activarse la aplicación de pago con el fin de que ciertas de las fases posteriores a implementarse, o para los datos de autenticación del consumidor se transfieran al lector de dispositivos o terminal POS. Del mismo modo, en algunas realizaciones, los datos de autenticación de consumidor pueden ser capaces de transferirse sin la activación de la aplicación de pago, o la necesidad de una interacción con el dispositivo de pago o el consumidor y pueden ser capaces de detectarse en la ausencia de una solicitud de pago activada.

Siguiendo con la descripción de la figura 4, en la fase 406 se determina si se requiere la interacción (por ejemplo, una entrada o acción de consumidor) antes de realizar o completar la transacción de pago. Por ejemplo, basándose en la identificación del consumidor, la cuenta de pago del consumidor, etc., puede determinarse si se requiere la interacción con el dispositivo de pago del consumidor o el consumidor antes de proceder con una transacción de pago. En algunas realizaciones, esta determinación puede realizarse de acuerdo con el procedimiento representado en la figura 5, o por un proceso similar. Si no se requiere la interacción con el dispositivo de pago para proceder con una transacción de pago, entonces la transacción de pago puede realizarse; obsérvese que en algunas realizaciones, se le puede pedir al usuario presentar el dispositivo de pago con el fin de permitir la ejecución de la transacción de pago, cuando la primera presentación del dispositivo de pago (en la fase 402) sirve para activar la

5 aplicación de pago (como se muestra en la fase 408). Sin embargo, si se requiere la interacción con el dispositivo de  
 pago o el consumidor antes de proceder con una transacción de pago, entonces se implementa esta interacción,  
 seguida por la presentación del dispositivo de pago al lector de dispositivos o terminal de punto de venta para  
 permitir la ejecución de la transacción (fase 408). La interacción necesaria puede implicar que el consumidor  
 proporcione ciertos datos (como un código de acceso u otros datos de autenticación, o responder a una pregunta de  
 seguridad), o la ejecución de una operación en el dispositivo de pago. Por lo tanto, si se requiere, la interacción se  
 ejecuta y el dispositivo móvil se vuelve a presentar al lector de dispositivos o terminal de punto de venta para  
 ejecutar la transacción de pago. Como se ha mencionado, y como se describirá haciendo referencia a la figura 5, la  
 interacción puede implicar que un consumidor proporcione datos (tal como una contraseña, etc.), o el dispositivo de  
 pago o la aplicación de pago se configuren para permitir la ejecución de una transacción de pago.

15 Después de la ejecución de la transacción de pago, se procesa la transacción de pago (fase 410). Después de que  
 se procese la transacción de pago, se determina si se desea una actualización de emisor (fase 412). Una  
 actualización de emisor es un proceso deseado o necesario por un emisor en el que los datos se proporcionan por el  
 emisor (tal como una actualización o corrección a los datos de transacción, por ejemplo), o se proporciona una  
 secuencia de comandos por el emisor para su ejecución por el lector de dispositivo, la aplicación de pago instalada  
 en el dispositivo de pago, o el dispositivo de pago. Esto puede producirse después de que la transacción de pago se  
 haya completado sustancialmente, o puede producirse en una fase anterior de la transacción de pago, tal como  
 después de que se recibe una respuesta a un mensaje de solicitud de autorización (en cuyo caso el proceso de  
 actualización puede ser necesario para permitir que se complete la transacción de pago). Si la actualización de  
 emisor implica que el emisor proporcione datos, entonces los datos pueden ser con el fin de actualizar, sincronizar o  
 reconciliar un registro de cuenta almacenado en el dispositivo de pago. En tal caso, el lector de dispositivos o  
 terminal POS pueden usarse para transferir los datos al dispositivo de pago mediante la comunicación que usa las  
 comunicaciones de campo cercano u otra capacidad de comunicaciones de corto alcance. Como una alternativa, la  
 actualización puede proporcionarse directamente al dispositivo móvil, usando una red inalámbrica (tal como la red  
 móvil 122 de la figura 2). Si la actualización de emisor implica la comunicación de un comando o secuencia de  
 comandos que provoca la ejecución de una operación o por la aplicación de pago o por un dispositivo de pago,  
 entonces el comando o secuencia de comandos puede transferirse al lector de dispositivos o terminal de punto  
 de venta y ejecutarse por el lector de dispositivos o terminal POS, o puede transferirse al dispositivo de pago por el  
 lector de dispositivos o sobre una red inalámbrica al dispositivo de pago para su ejecución por el dispositivo de pago  
 o la aplicación de pago. El comando o secuencia de comandos pueden ser con el fin de, por ejemplo, establecer o  
 restablecer un contador, configurar o reconfigurar una función de la aplicación de pago o del dispositivo de pago, o  
 actualizar el software del dispositivo.

35 Si se desea una actualización de emisor usando el lector de dispositivos o terminal POS, entonces se solicita al  
 consumidor (por ejemplo, se indica) que presente su dispositivo de pago al lector de dispositivos o terminal POS  
 (esto se muestra como una opción en la fase 414, siendo la otra opción la preparación para proporcionar una  
 actualización aérea al dispositivo de pago). Si se va a proporcionar la actualización de emisor al dispositivo de pago  
 usando el lector de dispositivos o terminal POS, entonces la actualización se proporciona al lector/terminal (fase  
 40 416). Si se va a proporcionar la actualización de emisor al dispositivo de pago usando un proceso de entrega aérea,  
 entonces la actualización se proporciona a la red inalámbrica o móvil (a través, por ejemplo, de la intermediación de  
 una pasarela móvil) y se entrega mediante ese método (fase 416). En el caso de la entrega al dispositivo de pago  
 por el lector de dispositivos o terminal POS, después de presentar el dispositivo de pago al lector/terminal, se  
 establece la comunicación entre el dispositivo de pago y el lector/terminal, y el emisor proporciona los datos o la  
 secuencia de comandos puede enviarse al dispositivo de pago usando la capacidad de comunicaciones de campo  
 cercano. Los datos, comandos, instrucciones, la secuencia de comandos u otra forma de información  
 proporcionados por el emisor pueden estar acompañados por un criptograma generado por el emisor (como se  
 indica en la fase 416). El criptograma generado por el emisor puede usarse para autenticar o de otra forma  
 identificar al emisor, y/o para proporcionar un medio para asociar los datos recibidos con el registro de transacción  
 correspondiente que se almacena en el dispositivo de pago. Los datos, comandos, instrucciones, la secuencia de  
 comandos u otra forma de información proporcionados por el emisor se reciben por el dispositivo de pago y pueden  
 usarse, por ejemplo, para actualizar los datos de transacción almacenados en el dispositivo de pago o provocar la  
 ejecución de una función u operación por la aplicación de pago o el dispositivo de pago (fase 418). En el caso de  
 una función u operación que se ejecuta, la función o la operación pueden ejecutarse por el lector de dispositivos o  
 55 terminal POS, por la aplicación de pago, o por el dispositivo de pago. En este punto, el suministro de la actualización  
 de emisor normalmente se completará y el proceso terminará (fase 420). Obsérvese que si no se desea una  
 actualización de emisor (como se determina en la fase 412), entonces el control pasará al final del proceso en la  
 fase 420.

60 Como se ha observado, si se requiere la interacción con el dispositivo de pago del consumidor antes de realizar una  
 transacción de pago, entonces la interacción se ejecuta antes de ejecutar la transacción de pago. Un proceso o  
 método para determinar si se requiere una interacción se representa en la figura 5, que es un diagrama de flujo que  
 ilustra un proceso 500 para determinar si se requiere una interacción con un dispositivo de pago de consumidor  
 antes de que se use el dispositivo para realizar una transacción de pago, de acuerdo con algunas realizaciones de la  
 presente invención. Se observa que la figura 5 representa un proceso a modo de ejemplo para determinar si se  
 65 requiere la interacción con el dispositivo de pago antes de iniciar una transacción de pago, y que, otros procesos

similares pueden usarse sin alejarse de los conceptos subyacentes de la invención. Además, aunque se proporcionan ejemplos de los tipos de interacciones o interacciones de consumidor que pueden solicitarse o requerirse antes de la ejecución de una transacción de pago, debería entenderse que otros tipos de interacciones u operaciones pueden solicitarse y caer dentro de los conceptos subyacentes de la invención.

5 Como se muestra en la figura 5, la determinación de si se requiere la interacción con el dispositivo de pago del consumidor se realiza considerando si al menos uno de entre la aplicación de pago (o el dispositivo de pago), el emisor, o el lector de dispositivos (o terminal de punto de venta) ha solicitado o requerido que se presente el dispositivo de pago para ejecutar algún tipo de interacción antes de realizar una transacción de pago. El proceso representado en la figura 5 opera para determinar si uno o más de los elementos indicados (es decir, la aplicación de pago, el dispositivo de pago, el lector de dispositivo, el terminal POS, el emisor, etc.) ha solicitado o requerido la presentación del dispositivo de pago (en cuyo caso se establece un indicador que indica que se requiere la presentación del dispositivo de pago), o si ninguno de los elementos indicados ha solicitado o requerido la presentación del dispositivo de pago (en cuyo caso se establece un indicador que indica que no se requiere la presentación del dispositivo de pago, o que no se establece ningún indicador).

Por ejemplo, en la fase 502 el proceso a modo de ejemplo determina si la aplicación de pago o el dispositivo de pago ha solicitado una acción de consumidor antes de la ejecución de una transacción de pago. Una acción de este tipo podría requerirse para proporcionar datos de consumidor tal como una entrada de consumidor, permitir la configuración o reconfiguración de una aplicación, una función de dispositivo u operación; por ejemplo, permitir o denegar una función, transferir datos a un emisor o procesador de pago, etc. Si se requiere una acción de consumidor de este tipo (que normalmente se realiza mediante la presentación del dispositivo de pago a un lector de dispositivos o terminal POS), entonces el control pasa a la fase 503 donde puede establecerse un indicador o bandera para indicar que se requiere una acción de consumidor antes de la ejecución de una transacción de pago.

A continuación, el control vuelve a la fase 504, donde se determina si un emisor ha solicitado una acción de consumidor antes de la ejecución de una transacción de pago. Obsérvese que si la aplicación de pago o dispositivo de pago no ha solicitado una acción de consumidor, entonces el control pasa directamente a la fase 504. Un emisor solicita una acción de consumidor que podría solicitarse para establecer o restablecer un contador que se usa para realizar un seguimiento de las transacciones de pago, para permitir o desactivar una función del dispositivo de pago, para solicitar una acción por un comerciante como parte de una transacción, etc. Como se ha descrito haciendo referencia a la fase 502, si se solicita una acción de consumidor de este tipo, entonces el control pasa a la fase 505 donde puede establecerse un indicador o bandera para indicar que se requiere una acción de consumidor antes de la ejecución de una transacción de pago. A continuación, el control vuelve a la fase 506, donde se determina si el lector de dispositivos o terminal POS ha solicitado una acción de consumidor antes de la ejecución de una transacción de pago. Obsérvese que si un emisor no ha solicitado una acción de consumidor, entonces el control pasa directamente a la fase 506. Un lector de dispositivos o terminal POS solicita una acción de consumidor que podría solicitarse para transferir datos al dispositivo de pago, etc. Como se ha descrito haciendo referencia a las fases 502 y 504, si se solicita una acción de consumidor de este tipo, entonces el control pasa a la fase 507 donde puede establecerse un indicador o bandera para indicar que se requiere una acción de consumidor antes de la ejecución de una transacción de pago. Obsérvese que si un lector de dispositivos o terminal de punto de venta no ha solicitado una acción de consumidor, entonces el control pasa directamente a la fase 508. Después de la terminación de la determinación(es) de si se ha solicitado una acción de consumidor, el control pasa a la fase 508 donde se determina si se ha establecido el indicador.

Obsérvese que en una realización alternativa, si cualquiera de los elementos ha solicitado o requerido que se implemente una acción de consumidor antes de la ejecución de una transacción de pago, entonces el control puede enviarse directamente a la fase 510, donde se ejecuta la interacción o se solicita una acción de consumidor. Del mismo modo, si el control no ha pasado a la fase 510, entonces el control puede pasar automáticamente a la fase 408 de la figura 4, ya que esto indicaría que se requiere o no se solicita ninguna interacción de consumidor.

La función principal del proceso 500 representado en la figura 5 es para determinar si cualquiera de los elementos pertinentes de un sistema de procesamiento de transacciones ha solicitado o requerido una acción de consumidor antes de la iniciación o la realización de una transacción de pago (en cuyo caso el indicador se establece en un valor especificado), o si por el contrario, ninguno de los elementos pertinentes ha solicitado o requerido una acción de consumidor antes de la realización de una transacción de pago (en cuyo caso no se establece el indicador, o se establece a un valor diferente). Si se ha establecido el indicador, entonces se solicita o ejecuta la interacción. Si el indicador no se ha establecido (o se establece en un valor que indica que no se requiere una acción de consumidor), entonces el control pasa a la fase 408 de la figura 4.

Si se determina que es necesaria una acción de consumidor (tal como una interacción con el dispositivo de pago del consumidor o una entrada del consumidor) antes de ejecutar una transacción de pago, entonces puede informarse al consumidor de esto y solicitar la ejecución de la acción. Obsérvese que la acción de consumidor puede tomar la forma del consumidor proporcionando datos solicitados (tales como los datos de autenticación o de seguridad, o una respuesta a un desafío) usando un mecanismo de entrada de datos del dispositivo de pago, etc. En algunos casos, puede solicitarse al consumidor o se le sugiere presentar su dispositivo de pago a un lector de dispositivos o terminal

POS. En una situación de este tipo, el consumidor presenta su dispositivo de pago al lector/terminal, normalmente permitiendo la comunicación entre el dispositivo de pago y el lector de dispositivos o terminal POS (por ejemplo, agitando, deslizando, pulsando, o ejecutando una acción similar con el dispositivo de pago). A continuación, puede ejecutarse una acción u operación en el dispositivo de pago, donde la acción u operación puede incluir uno o más de

5 entre establecer o restablecer un contador o indicador, permitir o denegar una función u operación de la aplicación de pago o del dispositivo de pago, ejecutar una etapa de procesamiento de datos en los datos almacenados en el dispositivo, acceder a los datos especificados almacenados en el dispositivo y proporcionar esos datos a un emisor, un comerciante, o procesador de pagos, etc. Obsérvese que en algunos casos, la presentación del dispositivo de

10 pago en respuesta a una solicitud para que el consumidor realice una acción puede servir como una “pulsación” que provoca la ejecución de una transacción de pago.

Algunos de los procesos, métodos, u operaciones descritos con respecto a las figuras 4 y 5 pueden implementarse en su totalidad o en parte por un aparato de procesamiento de datos residente en un lector de dispositivos o terminal POS (tal como el elemento 130 de la figura 2), un servidor que se comunica con el lector de dispositivos o terminal

15 POS a través de una red de comunicaciones (como parte de la red de procesamiento de pagos 134 de la figura 2), o por otro dispositivo adecuado. Los procesos, métodos, u operaciones pueden implementarse como un conjunto de instrucciones que se ejecutan por un procesador, siendo el procesador un elemento del aparato o servidor de procesamiento de datos.

Lo siguiente es un ejemplo de un caso de uso típico o escenario en el que pueden usarse las realizaciones del sistema, aparato y métodos de la invención. Se observa que el caso de uso es solamente a modo de ejemplo, ya que son posibles otros casos de uso o escenarios y serán evidentes para los expertos en la materia. En este ejemplo, un consumidor desea usar un dispositivo de pago móvil para hacer el pago de un bien o servicio en una

20 localización del comerciante. El dispositivo de pago móvil puede ser un teléfono móvil que contiene, por ejemplo un elemento sin contacto. El consumidor presenta su dispositivo móvil a un lector de dispositivos en la localización del comerciante, donde el lector de dispositivos usa un mecanismo de comunicaciones de campo cercano o de comunicaciones de corto alcance para acceder a los datos almacenados en el elemento sin contacto. Después de la presentación del dispositivo, puede activarse una aplicación de pago instalada en el dispositivo. A continuación, se determina si se requiere una interacción de consumidor antes de ejecutar una transacción de pago. Esta

25 determinación puede basarse en los datos leídos del dispositivo de pago. Si se requiere la interacción de consumidor puede determinarse por cualquier medio adecuado, tal como acceder a una base de datos que almacena un registro de todas las cuentas para las que se requiere una actualización u otra acción, o accediendo a una base de datos que almacena un registro de cuenta para la cuenta de pago asociada con el dispositivo de pago, donde ese registro incluye una indicación de que se requiere una interacción de consumidor.

30

Si se requiere una interacción de consumidor, entonces se ejecuta la interacción. A continuación, el consumidor presenta de nuevo el dispositivo de pago al lector de dispositivos o terminal de punto de venta. Si es necesario, el lector de dispositivos puede “leer” los datos de cuenta de consumidor y/o los datos de identificación de consumidor del dispositivo móvil para permitir la ejecución de la transacción de pago.

35

Obsérvese que en este escenario, la primera presentación del dispositivo de pago funciona como una “pre-pulsación”, ya que debe ejecutarse una función (por ejemplo, la activación de la aplicación de pago, la configuración del dispositivo de pago o la aplicación de pago) antes de permitir que se inicie una transacción. Esto se sigue por determinar si se requiere una interacción de consumidor (tal como la entrada de un código de acceso para confirmar la identidad del usuario). En algunos casos, determinar que se requiere una acción de consumidor puede implicar una re-presentación del dispositivo de pago para permitir una función u operación a ejecutar. Después de la ejecución de la función requerida o la ejecución de la acción de consumidor, la transacción de pago puede ejecutarse de acuerdo con sus procedimientos habituales, usando los datos que se proporcionaron anteriormente o al mismo tiempo para autenticar al consumidor y ejecutar un proceso de autorización. Si es necesario, el consumidor puede necesitar volver a presentar su dispositivo de pago al lector de dispositivos o terminal POS para provocar la ejecución de la transacción de pago. Después de la finalización de la transacción de pago, el consumidor puede solicitar que se vuelva a presentar su dispositivo de pago móvil para permitir una actualización de emisor o una operación similar a ejecutar. Como una alternativa, la actualización de emisor puede proporcionarse sobre otro canal de comunicaciones, tal como una red inalámbrica o móvil. La actualización puede usarse para transferir datos de transacciones actualizadas, establecer o restablecer un contador, permitir o denegar una función del dispositivo de pago, etc. Por lo tanto, en este ejemplo, se usan en combinación una pre-pulsación, seguida de una “primera” pulsación y una “segunda” pulsación para activar una aplicación de pago, determinar que una función u operación necesita ejecutarse en el dispositivo de pago o en la aplicación de pago (o que se requiere una acción de consumidor), para ejecutar esa función u operación, para ejecutar la transacción, y para proporcionar una actualización de los datos de transacción. Obsérvese que pueden usarse la pre-pulsación y una pulsación para ejecutar la transacción de pago con o sin otra presentación del dispositivo de pago (tal como para permitir una actualización de emisor) en la implementación de las realizaciones de la invención.

40

45

50

55

60

La figura 6 es un diagrama de bloques de un aparato informático a modo de ejemplo que puede usarse para implementar una realización del método o proceso de la invención para ejecutar una transacción de pago con un dispositivo de pago sin contacto usando una operación de pre-pulsación y/o de dos pulsaciones. Los elementos del

65

- aparato informático ilustrados en la figura 6, pueden usarse para implementar en todo o en parte los procesos, métodos, u operaciones de la invención, y pueden ser parte de un servidor u otro aparato informático (por ejemplo, una pasarela móvil, un servidor de gestión de emisor, etc.). Los subsistemas mostrados en la figura 6 están interconectados a través de un bus de sistema 600. Se muestran unos subsistemas adicionales tales como una impresora 610, un teclado 620, un disco fijo 630 (u otra memoria que comprende un medio legible por ordenador), un monitor 640, que está acoplado al adaptador de pantalla 650, y otros. Unos dispositivos periféricos y de entrada/salida (E/S), que se acoplan al controlador de E/S 660, pueden conectarse al sistema informático mediante cualquier número de medios conocidos en la técnica, tal como un puerto serie 670. Por ejemplo, el puerto serie 670 o la interfaz externa 680 pueden usarse para conectar el aparato informático a una red de área amplia tal como Internet, un dispositivo de entrada de ratón, o un escáner. La interconexión a través del bus del sistema permite que el procesador central 690 se comuniquen con cada subsistema y controle la ejecución de las instrucciones de la memoria de sistema 695 o del disco fijo 630, así como el intercambio de información entre los subsistemas. La memoria de sistema 695 y/o el disco fijo 630 pueden contener un medio legible por ordenador.
- 15 De acuerdo con las realizaciones de la presente invención, se han descrito un sistema, aparatos y métodos para permitir el uso de un dispositivo de pago móvil que incluye un elemento sin contacto en la ejecución de una transacción de pago. El elemento sin contacto está embebido dentro de un dispositivo móvil que es capaz de la comunicación y la transferencia de datos usando una capacidad de comunicaciones de campo cercano. Pueden usarse una o más "pulsaciones" o presentaciones del dispositivo móvil a un lector de dispositivos o terminal de punto de venta para permitir que un consumidor lance una aplicación de pago contenida en el dispositivo de pago, inicie una transacción de pago, configure o reconfigure una función u operación del dispositivo de pago, transfiera registros de transacciones al dispositivo de pago, etc.
- 20 Debería entenderse que la presente invención como se ha descrito anteriormente puede implementarse en la forma de lógica de control usando un software informático de una manera modular o integrada. Basándose en la divulgación y las enseñanzas proporcionadas en el presente documento, un experto en la materia sabrá y apreciará otras formas y/o métodos para implementar la presente invención usando un hardware y una combinación de hardware y software.
- 25 Cualquiera de los componentes de software o funciones descritas en esta solicitud, pueden implementarse como un código de software a ejecutar por un procesador usando cualquier lenguaje informático adecuado, tal como, por ejemplo, Java, C++ o Perl usando, por ejemplo, técnicas convencionales u orientadas a objetos. El código de software puede almacenarse como una serie de instrucciones o comandos en un medio legible por ordenador, tal como una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), un medio magnético, tal como una unidad de disco duro o un disquete, o un medio óptico, tal como un CD-ROM. Cualquier medio legible por ordenador de este tipo puede residir en o dentro de un único aparato informático, y puede estar presente en o dentro de diferentes aparatos informáticos dentro de un sistema o red.
- 30 Mientras que ciertas realizaciones a modo de ejemplo se han descrito en detalle y se muestran en los dibujos adjuntos, debería entenderse que tales realizaciones son simplemente ilustrativas y no pretenden ser restrictivas de la amplia invención, y que esta invención no debe limitarse a las disposiciones y construcciones específicas mostradas y descritas, ya que diversas otras modificaciones pueden ocurrírseles a los expertos en la materia.
- 35 Como se usa en el presente documento, el uso de "un", "una" o "el", "la" pretende significar "al menos uno", a menos que se indique específicamente lo contrario.
- 40
- 45

**REIVINDICACIONES**

1. Un método de proporcionar datos de transacción a un dispositivo de pago que incluye un elemento sin contacto, que comprende:
- 5 recibir, por un ordenador servidor desde una red de procesamiento de pago, un mensaje de solicitud de autorización que incluye una solicitud de autorización para realizar una transacción de pago electrónico usando el dispositivo de pago;
- 10 determinar, por el ordenador servidor, si la transacción de pago electrónico debería autorizarse basándose en datos incluidos en el mensaje de solicitud de autorización;
- enviar, por el ordenador servidor, un mensaje de respuesta de autorización a la red de procesamiento de pago para indicar si la transacción de pago electrónico se autoriza;
- 15 tras completar la transacción de pago electrónico, determinar que una actualización del emisor para el dispositivo de pago se requiere;
- en el que el método comprende además uno de:
- (i) proporcionar, por el ordenador servidor, una secuencia de comandos a un dispositivo lector en comunicación con el dispositivo de pago usando el elemento sin contacto del dispositivo de pago, en el que el elemento sin contacto es capaz de una comunicación y una transferencia de datos usando una tecnología de comunicaciones inalámbricas que comprende una tecnología de transferencia de datos de corto alcance, en el que la secuencia de comandos, cuando se ejecuta por el lector de dispositivos del dispositivo de pago, realiza la actualización del emisor en el dispositivo de pago, y
- 20 (ii) proporcionar, por el ordenador servidor, en caso de que el dispositivo de pago sea un teléfono móvil, la actualización del emisor sobre el aire mediante una red celular.
- 25 2. El método de la reivindicación 1, que comprende además:
- recibir, desde el dispositivo de pago, datos de autenticación proporcionados por el usuario al dispositivo de pago.
- 30 3. El método del aspecto (i) de la reivindicación 1, en el que el método comprende además:
- generar un criptograma para autenticar u de otra manera identificar al emisor, o para asociar la actualización del emisor con un registro de transacción apropiado que se almacena en el dispositivo de pago; enviar el criptograma al lector de dispositivo junto con la actualización del emisor.
- 35 4. El método del aspecto (ii) de la reivindicación 1, que comprende además:
- recibir, por el ordenador servidor, un primer criptograma desde el dispositivo de pago;
- 40 generar, por el ordenador servidor, un segundo criptograma basado en el primer criptograma, en el que el segundo criptograma confirma una autenticidad del emisor; y
- proporcionar, por el ordenador servidor, el segundo criptograma al dispositivo de pago como parte de cualquier dato, orden o instrucción enviada al dispositivo de pago en conexión con la actualización de emisor.
5. El método de la reivindicación 1, en el que determinar, por el ordenador servidor, si la transacción de pago electrónico debería autorizarse comprende además:
- 45 realizar un proceso de autenticación y autorización; y
- acceder a datos de cuenta del consumidor almacenados en una base de datos como parte del proceso de autenticación y autorización.
- 50 6. El método de la reivindicación 1, que comprende además:
- solicitar una acción de consumidor antes de ejecutar la transacción de pago electrónico.
- 55 7. El método de la reivindicación 6, en el que la acción de consumidor se solicita para proporcionar una entrada de consumidor, para establecer o reiniciar un contador que se usa para rastrear transacciones de pago, para permitir o desactivar una función del dispositivo de pago, o para solicitar una acción por un comerciante como parte de una transacción.
- 60 8. El método de la reivindicación 1, que comprende además:
- cifrar el mensaje de respuesta de autorización.
9. El método de la reivindicación 1, que comprende además:
- 65 recibir datos de consumidor que comprenden un código de acceso, una contraseña o una respuesta a una

pregunta.

- 5 10. El método de cualquier reivindicación anterior, en el que la actualización de emisor ajusta un valor de un contador, configura una función del dispositivo de pago, permite o desactiva una función del dispositivo de pago, o accede a datos almacenados en el dispositivo de pago.
11. El método de la reivindicación 1, en el que el ordenador servidor se opera por un emisor del dispositivo de pago.
- 10 12. Un ordenador servidor para uso en un método de cualquiera de las reivindicaciones anteriores.

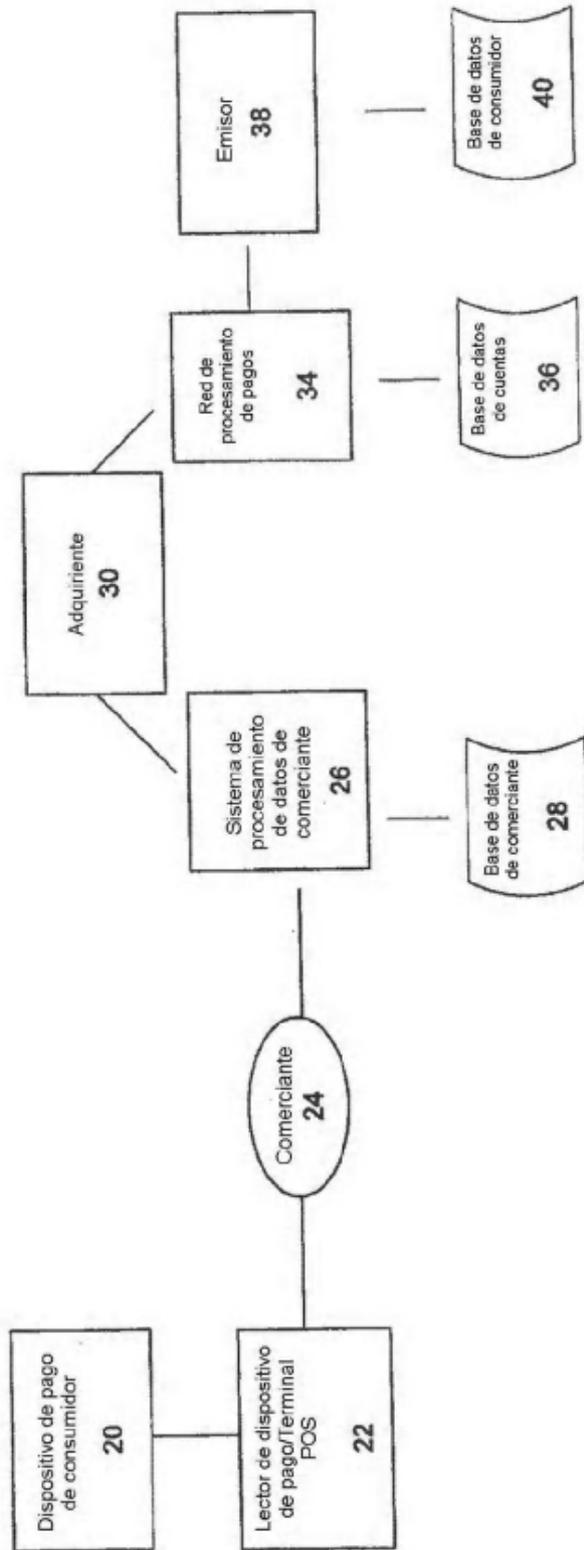


Figura 1

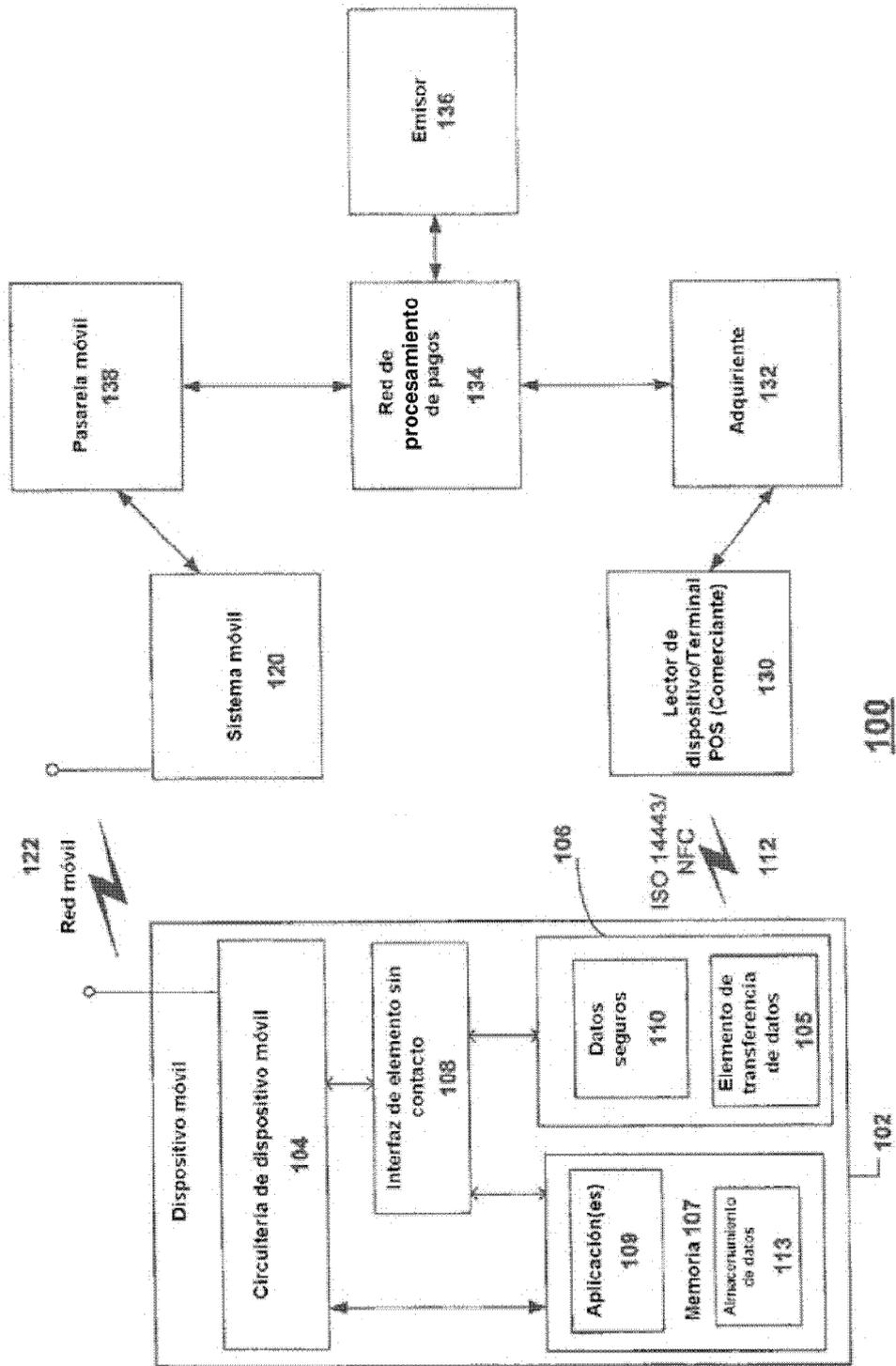


Figura 2

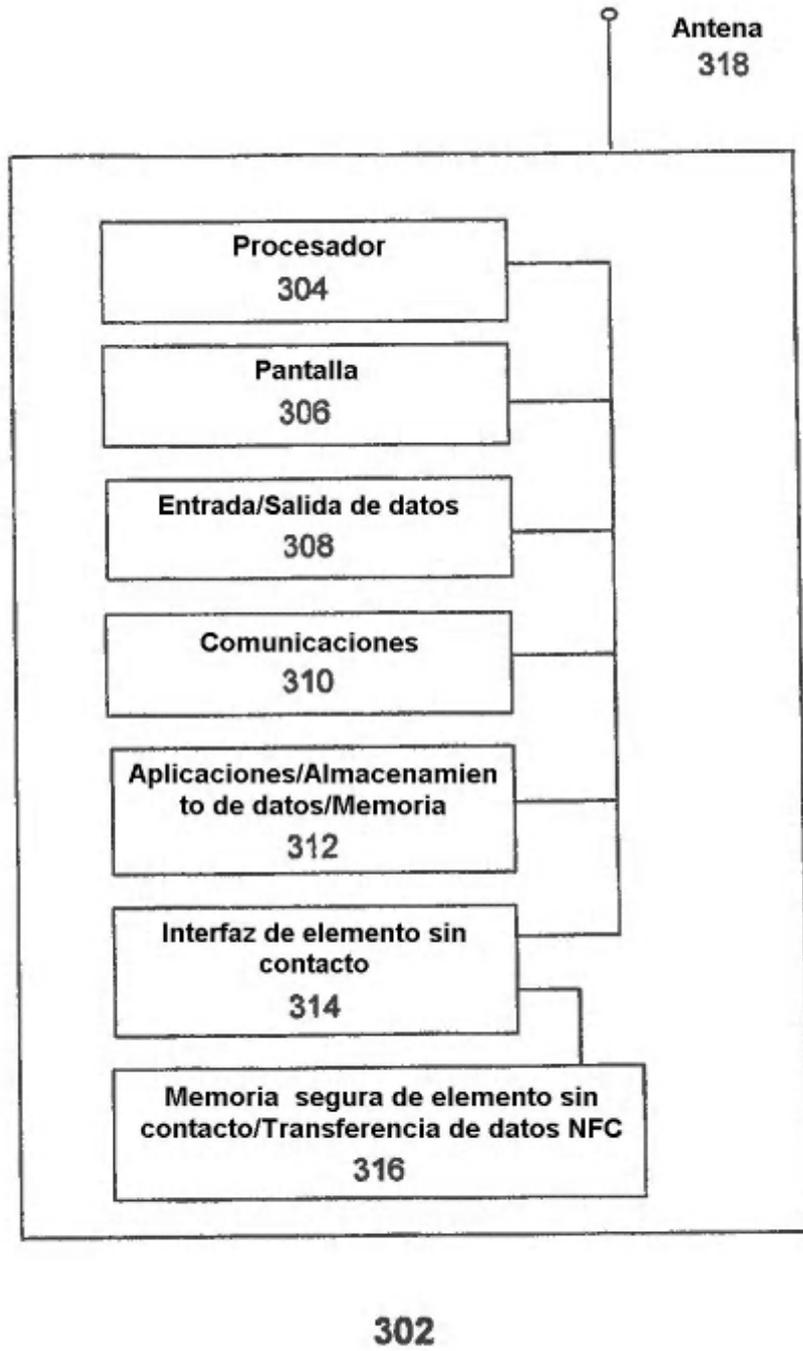


Figura 3

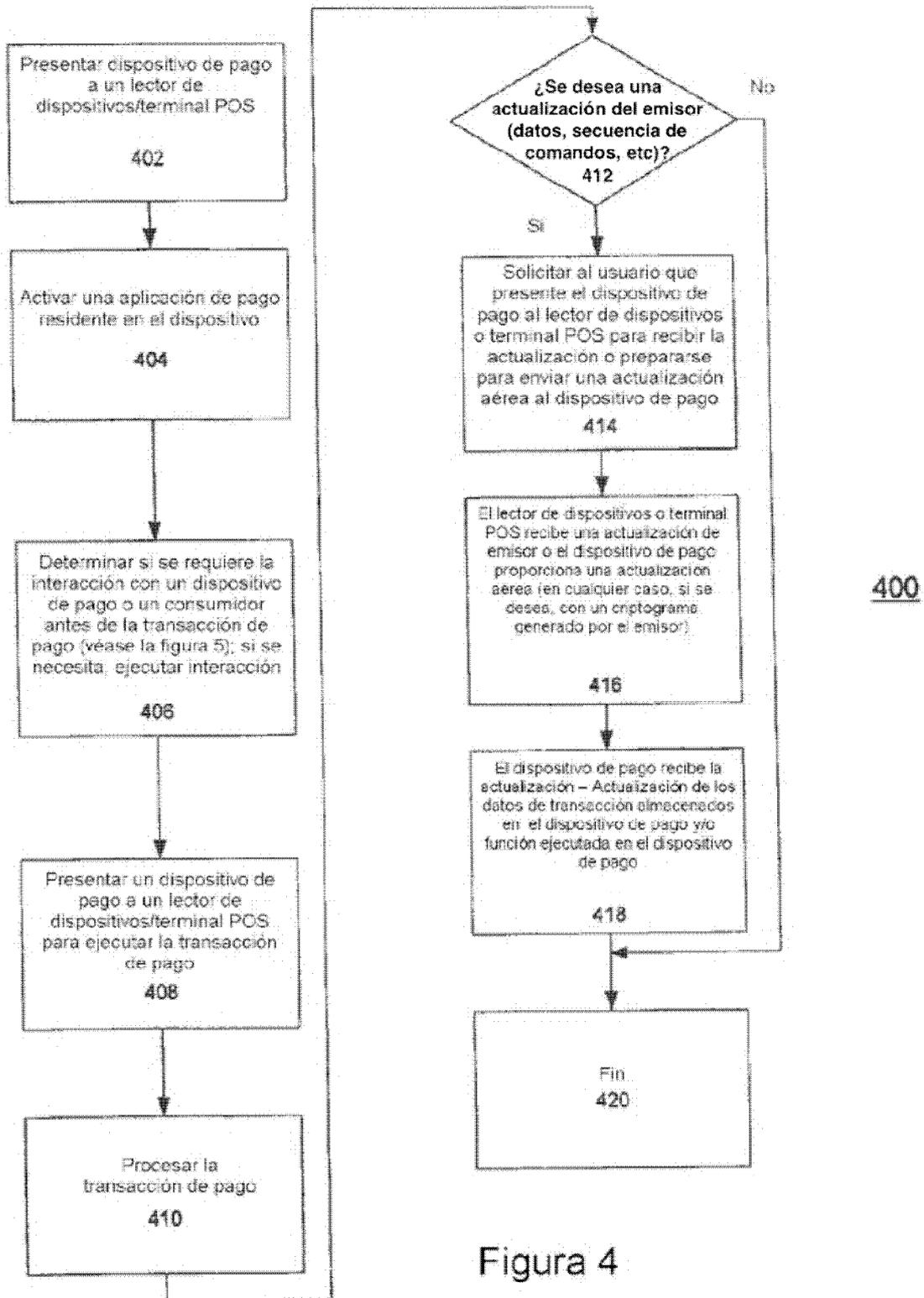
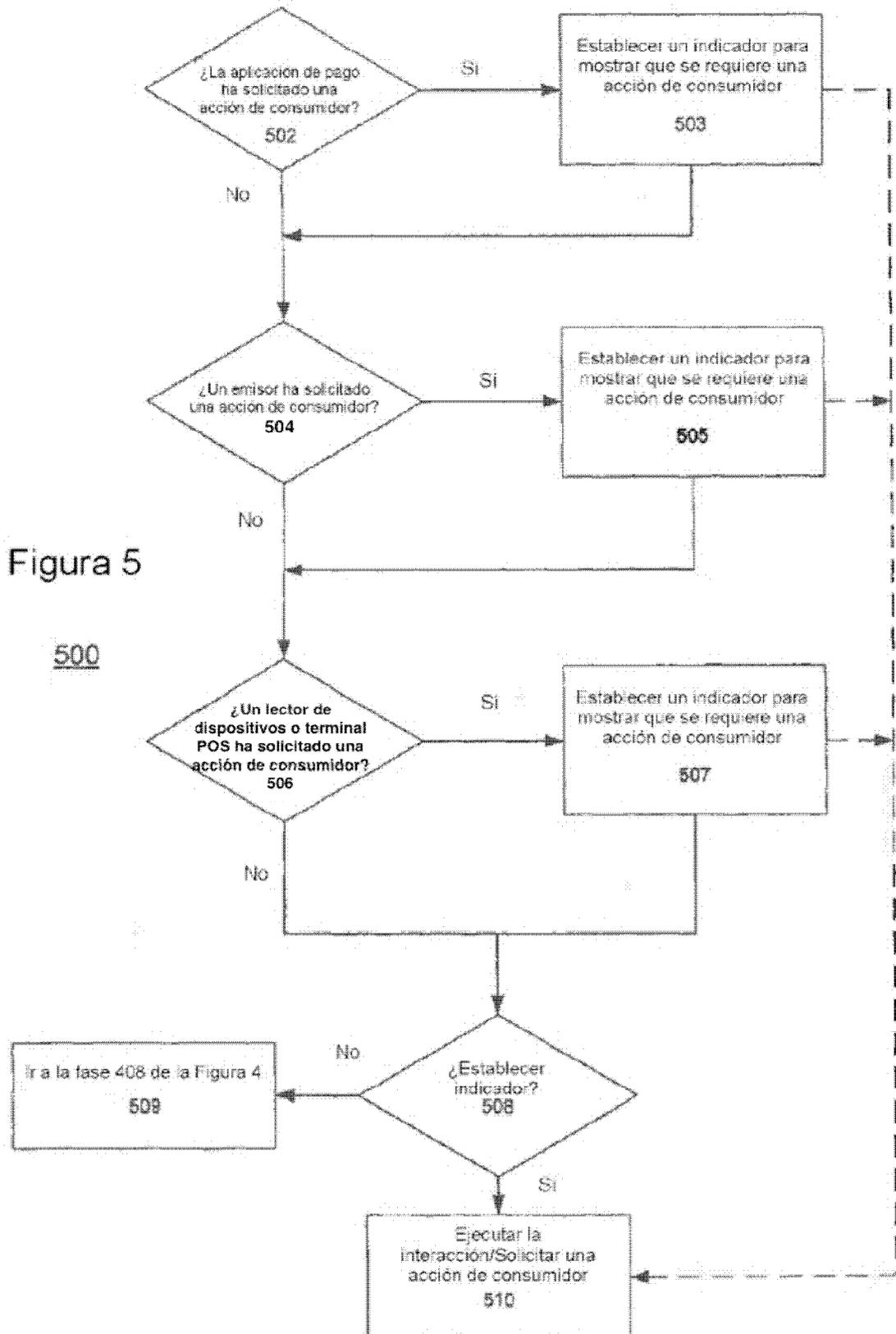


Figura 4



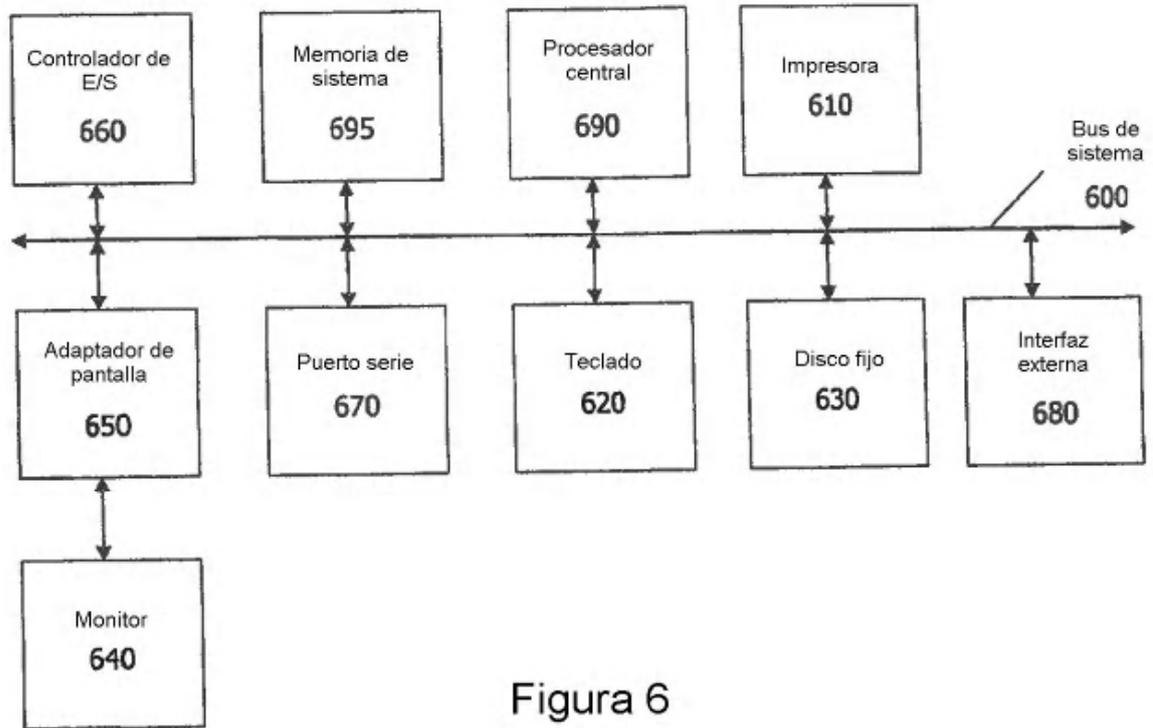


Figura 6