(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 672 920**

(51) Int. CI.:

G06Q 20/00 (2012.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.01.2011 PCT/AU2011/000055**

(87) Fecha y número de publicación internacional: **28.07.2011 WO11088508**

(96) Fecha de presentación y número de la solicitud europea: **19.01.2011 E 11734250 (1)**

(97) Fecha y número de publicación de la concesión europea: **14.03.2018 EP 2526514**

(54) Título: **Procedimiento, dispositivo y sistema para asegurar datos de pago para la transmisión a través de redes de comunicación abiertas**

(30) Prioridad:

19.01.2010 AU 2010900195

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.06.2018

(73) Titular/es:

BLUECHAIN PTY LTD (100.0%)
392 Ringwood-Warrandyte Road
Warrandyte VIC 3113, AU

(72) Inventor/es:

GLENDENNING, CRAIG

(74) Agente/Representante:

PONS ARIÑO, Ángel

Descripción

Procedimiento, dispositivo y sistema para asegurar datos de pago para la transmisión a través de redes de comunicación abiertas

Referencia cruzada a solicitudes relacionadas

La presente solicitud reivindica la prioridad deAU2010900195.

Campo técnico

Esta invención se refiere a un procedimiento, dispositivo y sistema para asegurar datos de pago para la transmisión a través de redes de comunicaciones abiertas.

Técnica anterior

La Figura 1 ilustra esquemáticamente una red típica de cuatro partes que muestra las instituciones que participan en una transacción a través de una red abierta. La red incluye a los emisores de tarjetas y los compradores comerciales, además de los titulares de tarjetas (clientes) y los comerciantes. El emisor de la tarjeta distribuye tarjetas a los consumidores, las factura y les cobra el pago. El comprador comercial recluta comerciantes para aceptar tarjetas y proporciona el servicio front-end de enrutamiento de la transacción a las instalaciones de procesamiento de la red. El comprador es responsable de entregar la transacción al emisor de la tarjeta correspondiente para que se facture al cliente y el comerciante reciba los fondos para la compra.

El proceso de transacción generalmente tiene dos partes principales. La primera es la autorización, y la segunda es la compensación y la liquidación. La autorización es el proceso de obtener permiso del banco que emitió la tarjeta para aceptar la transacción y los detalles de la tarjeta para el pago. La autorización comienza cuando un consumidor presenta su tarjeta al comerciante para una compra (1). Tradicionalmente, la seguridad de la transacción se produce para la autorización que ocurre en el punto de venta, aunque las transacciones más recientes se realizan en situaciones de "tarjeta no presente" (por ejemplo, en línea). En los últimos años, se han extendido cada vez más las tecnologías de chip y sin contacto. Con particular referencia a la industria de pagos, las transacciones de contacto y sin contacto tienen ventajas sobre las tecnologías tradicionales de banda magnética, ya que las tecnologías basadas en chip tienen la capacidad de almacenar y procesar datos de forma más segura.

En situaciones de contacto y sin contacto, los comerciantes generalmente obtienen electrónicamente la información de la transacción, ya sea haciendo que el consumidor deslice o inserte la tarjeta a través de un terminal en el punto de venta o acercándola a un terminal o lector. Habiendo obtenido la información de la tarjeta, el terminal del comerciante compila una solicitud de autorización que contiene la información de la tarjeta, la cantidad de la transacción y el número de identificación del comerciante y envía la solicitud de autorización al comprador (2). El comprador lee la información y envía la solicitud de autorización al banco emisor específico a través de una red de tarjetas de compensación (3). El banco emisor realiza una serie de comprobaciones de fraude y verifica que los fondos disponibles o la línea de crédito del titular de la tarjeta son suficientes para cubrir la compra antes de devolver una respuesta (4), ya sea otorgando o denegando la autorización. El comprador comercial recibe la respuesta y la retransmite al comerciante (5).

Los bancos, comerciantes y consumidores comerciales exigen que las transacciones a través de Internet y otras redes abiertas sean más seguras. Mientras que las transacciones actuales de contacto y sin contacto ofrecen mayor seguridad que la tecnología de banda magnética tradicional, no abordan el suficiente nivel de seguridad requerido para asegurar una transacción a través de Internet u otras redes abiertas.

Los sistemas actuales son propensos a los "ataques man-in-the-middle" (de intermediarios) que comprometen la autenticidad de una transacción. Los ataques Man-in-the-middle se aprovechan de la dificultad de verificar tanto la autenticidad de una transacción como la autenticidad del comerciante que la inicia. Dichos ataques actúan para interceptar la comunicación entre dos dispositivos. En este tipo de ataque, el software malicioso incrustado en una computadora funciona de tal manera que parece ser el comerciante para el dispositivo del cliente, mientras que también parece ser el dispositivo del cliente para el comerciante. Dicho software puede operarse para cambiar los detalles de la parte receptora o el valor de la transacción.

El documento US-7024395-B1 divulga un procedimiento en el que un cliente que realiza una transacción de tarjeta de crédito inserta su tarjeta inteligente en un lector de tarjetas adjunto al sistema del comerciante. El lector de

tarjetas activa la tarjeta del cliente y pasa cierta información del comerciante. El sistema del comerciante solicita después un "resumen de facturación" de la tarjeta del cliente. El resumen de facturación se devuelve al lector de tarjetas del comerciante que lo reenvía (y la información de la transacción que incluye información del cliente y del comerciante) al emisor de la tarjeta de crédito correspondiente, que mantiene la cuenta de la tarjeta de crédito del cliente. En una realización, la información del cliente y la información del comerciante están encriptadas. Al recibir el resumen de facturación, si fuera necesario la información de la transacción se desencripta y el emisor de la tarjeta de crédito busca la clave maestra del cliente utilizando el número de cuenta del cliente. Después, el emisor de la tarjeta de crédito usa la información de la transacción para volver a calcular el resumen de facturación (un resumen de facturación de autentificación) y compara este nuevo valor con el resumen de facturación enviado por el comerciante. Si es auténtico, los valores de resumen de facturación y de resumen de facturación de autentificación son equivalentes, los fondos se transfieren y se devuelve una notificación de aceptación al comerciante. Si no es auténtico, se devuelve una notificación de denegación al comerciante. La seguridad se mejora aún más mediante la utilización de una referencia única para cada transacción en la información única del cliente utilizada para crear el resumen de facturación.

El documento US-2008/208759-A1 divulga procedimientos y sistemas para ejecutar transacciones financieras entre clientes y comerciantes. Se recibe un identificador de una cuenta financiera del cliente en un sistema comercial. También se recibe una contraseña de un solo uso del cliente en el sistema comercial, y se le ha proporcionado al cliente la contraseña de un solo uso mediante un dispositivo electrónico móvil o un instrumento de presentación sin contacto. Se genera un criptograma que incluye el identificador de la cuenta financiera encriptada usando la contraseña de un solo uso. Una solicitud de autorización se formula en el sistema comercial. La solicitud de autorización incluye la información de criptograma y transacción que describe al menos una parte de la transacción financiera. La solicitud de autorización se transmite desde el sistema comercial a un procesador de autorización para la autorización de la transacción financiera.

El documento US-2009/216680-A1 divulga un módulo de cómputo seguro (SCM) configurado para la conexión con un dispositivo host. El SCM incluye un procesador para realizar operaciones de procesamiento seguras, una interfaz host para acoplar el procesador al dispositivo host, y una memoria conectada al procesador donde el procesador aísla lógicamente al menos parte de la memoria del acceso al dispositivo host. El SCM genera una firma digital segura para una transacción financiera y habilita el contenido controlado recibido a través del dispositivo host. La distribución de archivos se realiza desde un proveedor de contenido a un comprador o desde un distribuidor a un comprador. La distribución de archivos incluye una transacción financiera que utiliza firmas digitales seguras y, posiblemente, el cifrado de mensajes. Las firmas digitales y los detalles de la transacción se comunican a las organizaciones financieras apropiadas para autentificar a las partes de la transacción y completar la transacción. El contenido controlado se transfiere al comprador desde el proveedor de contenido o el distribuidor.

Resumen de la invención

De acuerdo con un primer aspecto de la presente invención, se proporciona un procedimiento para asegurar datos de pago transmitidos a través de redes de comunicación abiertas, comprendiendo el procedimiento: la configuración selectiva de un primer dispositivo transceptor como un dispositivo comercial para una primera transacción de pago; el establecimiento de una conexión de datos entre el primer dispositivo transceptor y un segundo dispositivo transceptor configurado como un dispositivo del cliente, pudiendo cada uno del primer y segundo dispositivo transceptor configurarse selectivamente como un dispositivo comercial o un dispositivo del cliente; transmitiendo el dispositivo comercial un primer paquete de datos al dispositivo del cliente a través de la conexión de datos, comprendiendo el primer paquete de datos un identificador del comerciante estático único emitido por un comprador, datos de solicitud de transacción y un valor dinámico único; formando el dispositivo del cliente una solicitud de autentificación del comerciante y transmitiendo la solicitud de autentificación del comerciante al dispositivo comercial para solicitar al comerciante un certificado firmado de un emisor que contiene el identificador del comerciante estático único y la clave pública del comerciante, y una firma del valor dinámico único usando la clave privada del comerciante; recibiendo el dispositivo del cliente del dispositivo comercial un segundo paquete de datos que comprende el certificado firmado del emisor y una firma del valor dinámico único usando la clave privada del comerciante; autentificando el dispositivo del cliente la legitimidad del dispositivo comercial verificando el certificado firmado del emisor utilizando la clave pública de una autoridad de certificación y, una vez verificado, autentificando el valor dinámico único firmado contra el único valor dinámico recibido en el primer paquete de datos utilizando la clave pública del comerciante; transmitiendo el dispositivo del cliente el identificador del comerciante estático único recibido y un criptograma al dispositivo comercial solo si el valor dinámico único firmado se autentifica frente al valor dinámico único recibido en el primer paquete de datos usando la clave pública comercial, habiéndose generado el criptograma usando un clave secreta única para el dispositivo del cliente, un valor de contador, el identificador del comerciante estático único recibido y los datos de solicitud de transacción; comprobando el dispositivo comercial si

el identificador del comerciante estático único recibido del dispositivo del cliente coincide con el identificador de vendedor estático único emitido por el comprador y, si es así, formando una solicitud de autorización que comprende el criptograma recibido, el identificador del comerciante estático único y los datos de solicitud de transacción y envío dicha solicitud de autorización a al menos uno de un emisor y un adquirente para facilitar la autorización y el procesamiento de dichos datos de solicitud de transacción; recibiendo el dispositivo comercial una respuesta del emisor indicando si la transacción ha tenido éxito; y notificando el dispositivo comercial al dispositivo del cliente si la transacción ha tenido éxito; donde el comprador retiene de forma segura una copia del identificador del comerciante estático único para verificar que un comerciante afiliado con el dispositivo del comerciante sea un comerciante válido.

La red abierta puede ser una red móvil o de Protocolo de Internet (IP).

Garantizar que el dispositivo comercial transmita el identificador de comerciante único al dispositivo transceptor del cliente, para su inclusión en el criptograma, vincula al comerciante y al consumidor a la transacción y minimiza el número de intercambios implicados en la autorización de una transacción. Esto se debe principalmente a que el comprador ya no está obligado a verificar la autenticidad del comerciante, solo que es un comerciante válido. Ventajosamente, se reduce sustancialmente la oportunidad para el fraude de terceros.

La etapa de establecimiento de una conexión de datos entre el primer y segundo dispositivo transceptor puede comprender establecer una conexión sin contacto o una conexión de contacto. La conexión sin contacto puede utilizar NFC, Bluetooth, WiFi, SMS, otra tecnología sin contacto similar o una combinación de los mismos. La conexión de contacto puede utilizar conectividad eléctrica como es bien conocido por los expertos en la técnica.

El procedimiento puede comprender además el mantenimiento de un contador incorporado en el dispositivo transceptor del cliente.

Se pueden incluir otros datos relevantes en el criptograma, que incluyen, entre otros, datos asociados con la capacidad técnica de un dispositivo transceptor.

El procedimiento puede comprender además la recepción de una solicitud de selección de cuenta del usuario del dispositivo transceptor del cliente. La solicitud de selección de cuenta se puede recibir a través de una interfaz de usuario de cualquiera de los dispositivos. En una realización en la que la solicitud de selección de cuenta se recibe a través de una interfaz de usuario del dispositivo transceptor del cliente, el procedimiento puede comprender además la transmisión de la selección de cuenta seleccionada por el usuario al dispositivo comercial a través de la conexión de datos. En una realización en la que la solicitud de selección de cuenta se recibe a través de una interfaz de usuario del dispositivo comercial, el procedimiento puede comprender además el almacenamiento de datos representativos de la cuenta seleccionada por el usuario en la memoria del dispositivo comercial. El procedimiento puede comprender además la transmisión de datos representativos de la cuenta seleccionada por el usuario a través de la conexión de datos al dispositivo transceptor del cliente.

Opcionalmente, el procedimiento puede comprender además la recuperación de una determinada cuenta predeterminada. La determinada cuenta predeterminada puede almacenarse en la memoria en el dispositivo transceptor del cliente.

El procedimiento puede comprender además la recuperación de los datos de solicitud de transacción, comprendiendo dichos datos de solicitud de transacción un importe para la transacción y al menos uno de un código de moneda, un sello de tiempo, datos representativos de la cuenta seleccionada por el usuario y un identificador de cliente como por ejemplo un PIN o biométrico y un valor de identificador de comerciante.

El paso del dispositivo comercial que transmite un primer paquete de datos al dispositivo transceptor del cliente a través de la conexión de datos puede ir precedido por el dispositivo transceptor del cliente que solicita el identificador comercial único y los datos de solicitud de transacción.

El paso de autentificar la legitimidad del dispositivo comercial permite que el dispositivo transceptor del consumidor se asegure de que se está comunicando con un dispositivo comercial auténtico (uno que ha sido emitido por un emisor aprobado dentro de un esquema definido). Además garantiza que el número de identificación único proporcionado como parte de la solicitud de transacción sea el mismo que el firmado por el emisor en el certificado de módulo seguro firmado.

De acuerdo con un segundo aspecto de la presente invención, se proporciona un procedimiento para operar un

primer dispositivo transceptor configurado selectivamente como un dispositivo comercial para asegurar datos de pago para una primera transacción de pago transmitida a través de una red de comunicación abierta, comprendiendo el procedimiento: el establecimiento de una conexión de datos con un segundo dispositivo transceptor configurado como un dispositivo del cliente, pudiendo cada uno del primer y segundo dispositivo transceptor configurarse selectivamente como un dispositivo comercial o un dispositivo del cliente; transmitiendo un primer paquete de datos al dispositivo del cliente a través de la conexión de datos, comprendiendo el primer paquete de datos un identificador del comerciante estático único emitido por un comprador, datos de solicitud de transacción y un valor dinámico único; recibiendo del dispositivo del cliente una solicitud de autentificación del comerciante que solicita un certificado firmado de un emisor que contiene el identificador único del comerciante estático y la clave pública del comerciante y una firma del valor dinámico único utilizando la clave privada del comerciante; y transmitiendo al dispositivo del cliente un segundo paquete de datos que comprende el certificado firmado del emisor y una firma del valor dinámico único usando la clave privada del comerciante; donde si el dispositivo del cliente autentifica la legitimidad del dispositivo comercial verificando el certificado firmado del emisor utilizando la clave pública de una autoridad de certificación y, una vez verificado, autentifica el valor dinámico único firmado contra el único valor dinámico recibido en el primer paquete de datos utilizando la clave pública del comerciante; el procedimiento comprende además: la recepción del dispositivo del cliente el identificador del comerciante estático único y un criptograma, habiéndose generado el criptograma usando una clave secreta exclusiva para el dispositivo del cliente, un valor de contador, el identificador del comerciante estático único y los datos de solicitud de transacción; comprobando si el identificador del comerciante estático único recibido del dispositivo del cliente coincide con el identificador del vendedor estático único emitido por el comprador y, si es así, formando una solicitud de autorización que comprende el criptograma recibido, el identificador del comerciante estático único y los datos de solicitud de transacción y envío dicha solicitud de autorización a al menos uno de un emisor y un adquirente para facilitar la autorización y el procesamiento de dichos datos de solicitud de transacción; recibiendo una respuesta del emisor que indique si la transacción tuvo éxito; y notificando al dispositivo del cliente si la transacción ha tenido éxito; en el que el comprador retiene de forma segura una copia del identificador del comerciante estático único para verificar que un comerciante afiliado al comerciante sea un comerciante válido.

De acuerdo con un tercer aspecto de la presente invención, se proporciona un procedimiento para operar un segundo dispositivo transceptor configurado selectivamente como un dispositivo del comprador para asegurar datos de pago para una primera transacción de pago transmitida a través de una red de comunicación abierta, comprendiendo el procedimiento: el establecimiento de una conexión de datos con un primer dispositivo transceptor configurado como un dispositivo comprador, pudiendo cada uno del primer y segundo dispositivo transceptor configurarse selectivamente como un dispositivo comercial o un dispositivo del cliente; recibiendo del dispositivo comercial un primer paquete de datos sobre la conexión de datos, comprendiendo el primer paquete de datos un identificador del comerciante estático único emitido por un comprador, datos de solicitud de transacción y un valor dinámico único; formando una solicitud de autentificación del comerciante y transmitiendo la solicitud de autentificación del comerciante al dispositivo comercial para solicitar al comerciante un certificado firmado de un emisor que contiene el identificador del comerciante estático único y la clave pública del comerciante, y una firma del valor dinámico único usando la clave privada del comerciante; recibiendo del dispositivo comercial un segundo paquete de datos que comprende el certificado firmado del emisor y una firma del valor dinámico único usando la clave privada del comerciante; autentificando la legitimidad del dispositivo comercial verificando el certificado firmado del emisor utilizando la clave pública de una autoridad de certificación y, una vez verificado, autentificando el valor dinámico único firmado contra el único valor dinámico recibido en el primer paquete de datos utilizando la clave pública del comerciante; transmitiendo el identificador del comerciante estático único recibido y un criptograma al dispositivo comercial solo si el valor dinámico único firmado se autentifica frente al valor dinámico único recibido en el primer paquete de datos usando la clave pública comercial, habiéndose generado el criptograma usando un clave secreta única para el dispositivo del cliente, un valor de contador, el identificador del comerciante estático único recibido y los datos de solicitud de transacción; y recibiendo del dispositivo comercial una notificación que indique si la transacción ha tenido éxito; donde el criptograma permite que el dispositivo comercial una vez recibido compruebe si el identificador del comerciante estático único recibido del dispositivo del cliente coincide con el identificador del comerciante estático único emitido por el comprador, y si es así, formar una solicitud de autorización que comprende el criptograma recibido, el identificador del comerciante estático único y los datos de solicitud de transacción y enviar dicha solicitud de autorización a al menos uno de un emisor y un comprador para facilitar la autorización y el procesamiento de dichos datos de solicitud de transacción; y donde el comprador retiene de forma segura una copia del identificador del comerciante estático único para verificar que un comerciante afiliado al comerciante sea un comerciante válido.

De acuerdo con un cuarto aspecto de la presente invención, se proporciona un primer dispositivo transceptor operable para asegurar datos de pago transmitidos a través de redes de comunicación abiertas, pudiendo configurarse el primer dispositivo transceptor selectivamente como dispositivo comercial o como dispositivo

transceptor del cliente, comprendiendo el primer dispositivo transceptor: un módulo de interfaz operable para permitir la comunicación de datos con otros dispositivos transceptores; y un procesador acoplado a una memoria, pudiendo funcionar la memoria para almacenar el código de control del procesador; donde cuando el primer transceptor se configura selectivamente como un dispositivo comercial, el código de control del procesador es operable para controlar selectivamente el procesador y el módulo de interfaz, cuando se ejecuta para: establecer una conexión de datos con un segundo dispositivo transceptor configurado como dispositivo del cliente; recuperar de la memoria un identificador del comerciante estático único, habiendo sido el identificador del comerciante estático único emitido por un comprador; transmitir un primer paquete de datos al dispositivo del cliente a través de la conexión de datos, comprendiendo el primer paquete de datos el identificador del comerciante estático único, los datos de solicitud de transacción y un valor dinámico único; recibir del dispositivo del cliente una solicitud de autentificación del comerciante que solicita un certificado firmado de un emisor que contiene el identificador del comerciante estático único y la clave pública del comerciante y una firma del valor dinámico único utilizando la clave privada del comerciante; y transmitir al dispositivo del cliente un segundo paquete de datos que comprende el certificado firmado del emisor y una firma del valor dinámico único usando la clave privada del comerciante; donde si el dispositivo del cliente autentifica la legitimidad del dispositivo comercial verificando el certificado firmado del emisor usando la clave pública de la autoridad de certificación y, una vez verificado, autentifica el valor dinámico único firmado contra el valor dinámico único recibido en el primer paquete de datos usando la clave pública del comerciante, el código de control del procesador es operable para controlar selectivamente el procesador y el módulo de interfaz, cuando se ejecuta para: recibir del dispositivo del cliente el identificador del comerciante estático único y un criptograma, habiéndose generado el criptograma usando una clave secreta exclusiva para el dispositivo del cliente, un valor de contador, el identificador del comerciante estático único y los datos de solicitud de transacción; comprobar si el identificador del comerciante estático único recibido del dispositivo del cliente coincide con el identificador del vendedor estático único emitido por el comprador y, si es así, formar una solicitud de autorización que comprende el criptograma recibido, el identificador del comerciante estático único y los datos de solicitud de transacción y enviar dicha solicitud de autorización a al menos uno de un emisor y un adquirente para facilitar la autorización y el procesamiento de dichos datos de solicitud de transacción; recibir una respuesta del emisor que indique si la transacción ha tenido éxito y notificar a un usuario del dispositivo del cliente; y notificar al dispositivo del cliente si la transacción ha tenido éxito; donde el comprador retiene de forma segura una copia del identificador del comerciante estático único para verificar que un comerciante afiliado con un comerciante sea un comerciante válido; o donde cuando el primer dispositivo transceptor se configura selectivamente como dispositivo del cliente, el código de control del procesador es operable para controlar selectivamente el procesador y el módulo de interfaz, cuando se ejecuta para establecer una conexión de datos con un segundo dispositivo transceptor configurado como dispositivo comercial; recibir del dispositivo comercial un primer paquete de datos sobre la conexión de datos, comprendiendo el primer paquete de datos un identificador del comerciante estático único emitido por un comprador, datos de solicitud de transacción y un valor dinámico único; formar una solicitud de autentificación del comerciante y transmitir la solicitud de autentificación del comerciante al dispositivo comercial para solicitar al comerciante un certificado firmado de un emisor que contiene el identificador del comerciante estático único y la clave pública del comerciante, y una firma del valor dinámico único usando la clave privada del comerciante; recibir del dispositivo comercial un segundo paquete de datos que comprende el certificado firmado del emisor y una firma del valor dinámico único usando la clave privada del comerciante; autentificar la legitimidad del dispositivo comercial verificando el certificado firmado del emisor utilizando la clave pública de una autoridad de certificación y, una vez verificado, autentificando el valor dinámico único firmado contra el único valor dinámico recibido en el primer paquete de datos utilizando la clave pública del comerciante; recuperar de la memoria un valor de contador y una clave privada del dispositivo del cliente almacenado; transmitiendo el identificador del comerciante estático único recibido y un criptograma al dispositivo comercial solo si el valor dinámico único firmado se autentifica frente al valor dinámico único recibido en el primer paquete de datos usando la clave pública del comercial, habiéndose generado el criptograma usando un clave secreta única recuperada para el dispositivo del cliente, un valor de contador recuperado, el identificador del comerciante estático único recibido y los datos de solicitud de transacción; y recibir del dispositivo comercial una notificación que indique si la transacción ha tenido éxito; donde el criptograma permite que el dispositivo comercial una vez recibido compruebe si el identificador del comerciante estático único recibido del dispositivo del cliente coincide con el identificador del comerciante estático único emitido por el comprador, y si es así, formar una solicitud de autorización que comprende el criptograma recibido, el identificador del comerciante estático único y los datos de solicitud de transacción y enviar dicha solicitud de autorización a al menos uno de un emisor y un comprador para facilitar la autorización y el procesamiento de dichos datos de solicitud de transacción; y donde el comprador retiene de forma segura una copia del identificador del comerciante estático único para verificar que un comerciante afiliado al comerciante sea un comerciante válido.

El primer dispositivo transceptor se puede incorporar a un dispositivo de comunicación móvil, como por ejemplo un teléfono móvil, un teléfono celular o un iPhone. Opcionalmente, el primer dispositivo transceptor puede estar separado de, pero en comunicación con, un dispositivo de comunicación móvil. Opcionalmente, el primer dispositivo

transceptor puede incorporarse en un dispositivo de punto de venta (POS) o separarse de, pero en comunicación con un POS. En otras disposiciones más, el dispositivo transceptor puede integrarse en un dispositivo informático personal (como por ejemplo una computadora portátil, PDA, buscapersonas) o un dispositivo que está separado de, pero en comunicación con, un dispositivo informático personal.

El módulo de interfaz puede tener la forma de un módulo de interfaz de contacto, un módulo de interfaz sin contacto o un módulo de interfaz de contacto dual y sin contacto. En una realización que utiliza un módulo de interfaz sin contacto, el módulo de interfaz preferiblemente incorpora los mecanismos necesarios para permitir la transferencia de datos entre dos dispositivos (como por ejemplo ISO 7816, NFC, Bluetooth, Wi-Fi, SMS, etc.). Por ejemplo, uno de dichos módulos de interfaz sin contacto puede comprender un transpondedor y una antena.

Los datos de solicitud de transacción pueden comprender un importe para la transacción, y al menos uno (o más) de un código de moneda, un sello de tiempo y un identificador de cliente como por ejemplo un PIN o biométrico y cualquier otro dato relevante.

Breve descripción de los dibujos

La técnica anterior se ha descrito con referencia a la Figura 1, que ilustra una red típica de cuatro partes que participa en una transacción de pago a través de una red abierta.

Se describirá ahora un ejemplo de la invención con referencia a los dibujos adjuntos, en los que:

La Figura 2 es un diagrama de bloques que ilustra esquemáticamente los componentes de un dispositivo transceptor para asegurar transacciones a través de redes abiertas;
La Figura 3 es un diagrama de bloques que ilustra esquemáticamente los componentes de un sistema para asegurar transacciones a través de redes abiertas;
La Figura 4 es un diagrama de flujo de los pasos involucrados en asegurar transacciones a través de redes abiertas; y
La Figura 5 es un diagrama de flujo de un paso específico que se muestra en la Figura 4.

Mejor modo de la invención

La Figura 2 ilustra componentes de un dispositivo transceptor 10 para asegurar transacciones a través de redes abiertas. Debe apreciarse que el término red abierta, o red de comunicación abierta, se define ampliamente como cualquier red inalámbrica, generalmente no segura, como por ejemplo la red de Protocolo de Internet (IP). Por ejemplo, la infraestructura de red abierta puede comprender las redes comúnmente denominadas red troncal de Internet y cada una de una red de área local (LAN) y una red de área extensa (WAN). Cada una de las redes LAN y WAN está conectada a Internet mediante un enrutador o servidor de traducción de direcciones de red (NAT) y cada una de ellas es capaz de transferir tramas IP.

El dispositivo transceptor 10 es cualquier dispositivo que está configurado para comunicarse con otro dispositivo transceptor. En este ejemplo, el dispositivo transceptor 10 es un dispositivo que se incorpora a un dispositivo de comunicación móvil en forma de un teléfono móvil.

Como se ilustra, el transceptor 10 comprende un módulo de interfaz en forma de un módulo de interfaz de contacto o sin contacto (CIM) 12. En este ejemplo, el CIM 12 es un módulo de interfaz sin contacto. El CIM 12 puede ser cualquier mecanismo para transferir datos entre dos dispositivos (como por ejemplo ISO 7816, Near Field Communication (NFC), Bluetooth, SMS, etc.) y en esta aplicación se utiliza NFC. NFC es un estándar de conectividad inalámbrica de corto alcance (Ecma-340, ISO/IEC 18092) que utiliza inducción de campo magnético para permitir la comunicación entre el dispositivo 10 y un dispositivo vecino cuando se introducen a unos pocos centímetros el uno del otro. El estándar especifica una forma para que los dispositivos respectivos establezcan una red de igual a igual (P2P) para intercambiar datos. Una vez que se configura la red P2P, se puede utilizar otra tecnología como por ejemplo Bluetooth para permitir una comunicación de mayor alcance.

Junto con el CIM hay una unidad de procesamiento central 14 que controla el funcionamiento del dispositivo 10 y la memoria 16. El módulo de transacción 18 se implementa como una aplicación de software, programas de ordenador, etc., utilizando cualquier lenguaje informático adecuado (C, C ++, Java, Perl, PHP, etc.). El software se almacena como una serie de instrucciones o comandos escritos en la memoria 16 de modo que cuando el procesador 14 lee la memoria, se realizan las funciones descritas aquí.

Además de la parte programable de la memoria 16, la memoria puede incluir diferentes tipos de memoria, como memoria volátil y no volátil y memoria de solo lectura.

La Figura 3 ilustra un sistema 20 en el que se puede usar una realización de la invención para asegurar transacciones a través de redes abiertas. Los números similares se refieren a componentes similares. El sistema 20 comprende un primer dispositivo transceptor 10 que en este ejemplo está configurado como un "dispositivo comercial" y un segundo dispositivo transceptor 22 que en este ejemplo está configurado como un "dispositivo cliente". En este ejemplo, el dispositivo comercial 10 y el dispositivo cliente 22 son dispositivos con capacidad NFC habilitados para móviles y cada uno está configurado para comunicarse con el otro a través de sus respectivas interfaces sin contacto 12. Cada dispositivo 10, 22 está equipado con los componentes descritos con respecto a la Figura 2.

La unidad de memoria 16 del dispositivo transceptor comercial 10 almacena de forma segura el identificador comercial exclusivo que identifica al comerciante a quien se le debe abonar el importe de la transacción. El identificador de comerciante está incrustado en la memoria del dispositivo 10 durante el proceso de emisión, y el comprador retiene de forma segura una copia. La unidad de memoria 16 del dispositivo transceptor 22 del cliente almacena de forma segura el número de cuenta principal ("PAN") del usuario, el número de identificación personal del usuario ("PIN"), un contador de transacción de la aplicación (ATC) y una clave secreta. La clave secreta está incorporada en la memoria del dispositivo 22 durante el proceso de emisión, y el emisor 30 conserva de forma segura una copia.

El dispositivo comercial 10 se comunica con un comprador 28 y/o un emisor 30 a través de una red 26. El dispositivo se puede unir a la red de cualquier manera adecuada conocida en la técnica. La red 26 puede incluir cualquier tipo de sistema de entrega que incluye, pero no se limita a, una red de área local, red de área amplia, red telefónica y/o cualquier red de comunicaciones por cable configurada para transferir datos.

La Figura 4 ilustra los pasos de un procedimiento 40 para asegurar transacciones a través de redes abiertas. El procedimiento puede implementarse mediante el sistema ilustrado en la Figura 3. El procedimiento comprende los pasos generales del procesamiento de transacción preliminar - paso 42, procesamiento de descubrimiento - paso 44, paso de selección de aplicación - 46, procesamiento de la aplicación - paso 48, y autorización de transacción - paso 50.

La etapa de procesamiento de transacción preliminar 42 implica al dispositivo comercial 10, que recopila los datos variables (que incluye la cantidad de transacción y el código de moneda) y los datos de transacción estáticos que es necesario enviar al dispositivo 22 de cliente. Además, el CIM 12 está habilitado para las comunicaciones con el dispositivo del cliente 22.

El procesamiento de descubrimiento en la etapa 44 sigue el procesamiento de transacción preliminar en la etapa 42. Una vez que el dispositivo 22 del cliente se encuentra dentro del alcance del dispositivo comercial 10, la comunicación se establece a través de los respectivos CIM 12 del dispositivo. El dispositivo comercial 10 energiza su CIM 12 y establece una conexión con el dispositivo cliente 22 a través de su CIM 12. Si el dispositivo comercial 10 detecta múltiples dispositivos sin contacto dentro de su campo de alcance, entonces el dispositivo comercial 10 puede indicar esta condición al titular del dispositivo cliente 22 y solicitar que solo se presente un único dispositivo para la transacción.

Una vez que se establece la comunicación entre los dispositivos respectivos, el dispositivo comercial 10 compila y transmite un mensaje de selección de la aplicación al dispositivo 22 del cliente.

La etapa 46 de selección de la aplicación sigue a la etapa 44 de procesamiento de descubrimiento e implica formar una respuesta al mensaje de selección de la aplicación. La etapa de selección de la aplicación (que se muestra con más detalle con referencia a la Figura 5) implica el descubrimiento de la aplicación 62, la selección de la aplicación real 64 y la presentación del PIN 66.

La selección de aplicación 60 puede emplear una de dos metodologías. Si el dispositivo del cliente 22 es un dispositivo inteligente que puede construir una lista de cuentas, entonces el dispositivo del cliente procede a construir una lista de cuentas disponibles y el dispositivo del cliente muestra la lista de cuentas en la pantalla del dispositivo para la selección del cliente (etapa 62). En respuesta, el usuario del dispositivo 22 de cliente selecciona una etapa de cuenta 64, posiblemente mediante la entrada a través de un teclado numérico en el cuerpo del dispositivo 22. Se debe tener en cuenta que el teclado puede ser un teclado físico o un teclado virtual. El usuario, en respuesta a la selección de una cuenta, introduce después una etapa de PIN 66, posiblemente en el mismo teclado

numérico en el cuerpo del dispositivo 22, cuyo valor se compara después con un valor de referencia almacenado en la memoria.

El dispositivo del cliente 22 responde entonces al mensaje de selección de la aplicación y transmite la información de la cuenta seleccionada al dispositivo comercial 10. Además, el dispositivo del cliente 22 envía una solicitud al dispositivo comercial 10 para obtener la información específica requerida para completar la transacción segura.

Si el dispositivo del cliente 22 no tiene la inteligencia requerida, entonces en respuesta a la recepción del mensaje de selección de la aplicación, el dispositivo del cliente 22 construye una lista de cuentas disponibles y transmite la lista de cuentas disponibles al dispositivo comercial 10. El dispositivo comercial 10 compara después las cuentas enumeradas recibidas desde el dispositivo cliente 22 contra las que soporta el dispositivo comercial 10. La lista de cuentas que el dispositivo comercial 10 soporta se presenta luego al usuario del dispositivo cliente 22 en la pantalla del dispositivo comercial, etapa 62. En respuesta, el usuario selecciona una cuenta a la que se debita el valor de la transacción, posiblemente a través de un teclado en una pantalla de usuario en el cuerpo del dispositivo comercial 10, etapa 64. El usuario, en respuesta a la selección de una cuenta, introduce un PIN 66. Los datos indicativos de la cuenta seleccionada se almacenan posteriormente en la memoria en el dispositivo comercial 10. Además, los datos indicativos de la cuenta seleccionada y el PIN presentado se transmiten desde el dispositivo comercial 10 al dispositivo cliente 22. El dispositivo del cliente verifica después los datos introducidos PIN contra un valor de referencia almacenado en la memoria del dispositivo del cliente. Como en la primera metodología, en respuesta a la solicitud de selección de cuenta, el dispositivo del cliente 22 envía una solicitud al dispositivo comercial 10 para obtener la información específica requerida para completar la transacción segura.

Independientemente de la metodología empleada, la información específica recopilada posteriormente incluirá varios detalles sobre las capacidades del dispositivo comercial 10 junto con los datos específicos requeridos para procesar la transacción.

La etapa 48 de procesamiento de la aplicación sigue la etapa 46 de selección de la aplicación e implica la compilación de un mensaje de comando. En respuesta a la solicitud del dispositivo transceptor del cliente 22 de información específica requerida para completar la transacción segura, el dispositivo comercial 10 compila un mensaje de comando que se transmite después al dispositivo transceptor del cliente 22.

El mensaje de comando comprende una cantidad de elementos de datos o campos. Un primer campo se rellena con un valor único que identifica al comerciante. Este valor será conocido por las organizaciones compradoras. Un segundo campo se rellena con datos representativos de un importe para la transacción. Un tercer campo se rellena con datos representativos del código de moneda de la transacción. Un cuarto campo se rellena con datos representativos de la cuenta seleccionada del cliente desde la que se debe cargar el importe de la transacción. Se pueden rellenar campos adicionales con datos asociados con un número único que se proporciona para asegurar aún más la transacción, datos representativos de la cuenta seleccionada por el usuario y un PIN que se pudo haber capturado en el momento de la selección de la cuenta, ya sea en el dispositivo del cliente 22 o el dispositivo comercial 10.

El dispositivo comercial 10 realiza una serie de procesos de gestión de riesgos para garantizar que no se hayan excedido los intentos de verificación de PIN y para proteger contra ataques de man-in-the-middle y rasgados de transacción. Los rasgados de transacción describen la situación en la que un dispositivo transceptor se retira del campo de acoplamiento con otro dispositivo transceptor antes de que la transacción se haya completado. La aplicación del módulo de transacción debe garantizar que siempre se sepa dónde está el proceso si los dos dispositivos restablecieran una ruta de comunicación de datos para completar la transacción. En efecto, o bien los dispositivos respectivos suponen que la transacción no se ha completado y todos los valores se restablecen a los valores anteriores al comienzo de la transacción, o los dispositivos respectivos asumen que la transacción se ha completado con respecto al otro dispositivo y cada dispositivo almacena datos asociado con cualquier cambio en el punto de rasgado de la memoria. En el caso posterior, dichos datos se envían al Emisor, quien es responsable de resolver cualquier discrepancia.

Después de la finalización del proceso de gestión de riesgos, el procesador 14 del dispositivo del cliente 22 construye la respuesta segura apropiada al mensaje de comando y transmite la respuesta segura al dispositivo transceptor comercial 10.

La respuesta segura se basa en un criptograma calculado utilizando una clave única para el dispositivo del cliente 22 junto con el identificador único del comerciante y toda la información requerida para procesar la transacción. Al igual que con el mensaje de comando, la respuesta de autorización comprende una serie de campos de datos, los

primeros tres de los cuales están rellenos con datos previamente recibidos del dispositivo comercial, que son el identificador único del comerciante, el importe de la transacción y el código de moneda. Además, otros campos de la respuesta de autorización segura al mensaje de comando se rellenan con la pista de datos 2 de la aplicación de emisor o PAN del dispositivo del Cliente que corresponde a la cuenta seleccionada por el usuario, un contador de transacciones de aplicaciones (ATC) e información de verificación del PIN indicativa de respuestas correcta/incorrecta. El dispositivo de cliente 22 gestiona un valor de contador denominado Contador de transacciones de aplicaciones (ATC). El ATC está incluido en el cálculo del criptograma y se incrementa con cada transacción, como una defensa contra los ataques de repetición.

La respuesta segura se transmite al dispositivo comercial 10. Incluido con la respuesta segura puede estar el valor único que identifica al comerciante. Una vez que se recibe la respuesta, el comerciante verifica la respuesta y si la respuesta incluye un valor que identifica al comerciante, entonces el dispositivo comercial 10 verifica que ese valor recibido corresponde al valor de identificación único que identifica al comerciante almacenado de forma segura en la memoria del dispositivo comercial. Con la condición de que el valor recibido que identifica al comerciante y el valor único que identifica al comerciante sea uno y el mismo, la respuesta segura estará lista para ser enviada al comprador/emisor.

El dispositivo transceptor del cliente 22 puede ahora retirarse del campo de alcance del dispositivo transceptor comercial 10.

La etapa de autorización 50 sigue a la etapa de procesamiento de la aplicación 48. El dispositivo transceptor comercial 10 envía la respuesta segura al comprador y después al emisor para su verificación. Al recibir una transacción, el emisor puede volver a calcular el criptograma utilizando su copia de la clave del dispositivo del cliente. En base a una respuesta recibida posteriormente del emisor, el dispositivo transceptor comercial 10 notifica al usuario del dispositivo transceptor del cliente 22 si la transacción ha tenido éxito.

Suponiendo que los datos recalculados del criptograma estén intactos, el emisor cargará a la cuenta seleccionada por el usuario el valor de la transacción. El comprador/emisor tiene la seguridad de la identidad del comerciante y la identidad del cliente, ya que el dispositivo del cliente 22 devuelve al dispositivo comercial 10 la información que recibió previamente, así como otra información obtenida de su sistema para procesar la transacción. Si estuviera presente un man in the middle, el dispositivo comercial será alertado posteriormente.

La metodología de acuerdo con la invención puede, además, autentificar la legitimidad del comerciante. Esto se puede lograr mediante la firma asimétrica de un valor dinámico único.

Cuando se emiten los dispositivos transceptores 10, 22, se cargan con la clave pública del emisor 30, en un certificado firmado por la clave privada de una o más autoridades de certificación (CA). Además, los dispositivos transceptores 10, 22 se cargan con la clave pública para la una o más autoridades de certificación para verificar la clave pública del emisor 30 incrustada en el certificado.

Además, el módulo de seguridad 24 de cada dispositivo transceptor 10, 22 tiene su propio par de claves públicas/privadas cargadas. La clave pública de cada módulo de seguridad respectivo 24 se mantiene en un valor de identificación único de certificado que se firma con la clave privada del emisor 30.

El dispositivo transceptor del cliente 22 solicita desde el dispositivo transceptor comercial 10 el certificado firmado del Emisor 30 que contiene el número de identificación único. Además, solicita que el dispositivo transceptor comercial 10 firme un valor dinámico único utilizando la clave privada del módulo de seguridad 24.

El dispositivo transceptor del cliente 22 verifica el certificado del emisor firmado por CA utilizando la clave pública CA y una vez autentificado, el dispositivo transceptor del cliente 22 autentifica el certificado del módulo seguro firmado por el Emisor utilizando la clave pública del Emisor y luego autentifica el valor dinámico único firmado utilizando el clave pública cargada en el certificado firmado del emisor del comerciante.

Como debería ser evidente para los expertos en la materia, las realizaciones de la invención son ventajosamente mucho más simples en su implementación que las técnicas conocidas, por ejemplo, aquellas que utilizan EMV (Europay, Mastercard y VISA). EMV no contempla vincular al comerciante y al consumidor a una sola transacción, en contraste EMV simplemente identifica que se usa una tarjeta válida en una transacción. Posteriormente, las realizaciones de la invención no se basan en que el dispositivo comercial necesite asegurar una transacción particular, ni se basan en la condición de que se haya establecido una relación preexistente entre el comerciante, el consumidor y el emisor.

Los expertos en la materia apreciarán que se pueden realizar numerosas variaciones y/o modificaciones a la invención como se muestra en las formas de realización específicas sin alejarse del alcance de la invención como se reivindica. Además, las realizaciones de la invención son adecuadas no solo para un mercado nacional sino también para esquemas de pago dentro de un contexto internacional. Las presentes formas de realización tienen, por lo tanto, que ser consideradas en conjunto como ilustrativas y no restrictivas.

REIVINDICACIONES

1. Un procedimiento para asegurar datos de pago transmitidos a través de redes de comunicación abiertas, comprendiendo el procedimiento:

la configuración selectiva de un primer dispositivo transceptor (10) como un dispositivo comercial (10) para una primera transacción de pago;

el establecimiento (44) de una conexión de datos entre el primer dispositivo transceptor y un segundo dispositivo transceptor configurado como un dispositivo del cliente (22), pudiendo cada uno del primer y segundo dispositivo transceptor configurarse selectivamente como un dispositivo comercial (10) o un dispositivo del cliente (22);

transmitiendo (48) el dispositivo comercial (10) un primer paquete de datos al dispositivo del cliente (22) a través de la conexión de datos, comprendiendo el primer paquete de datos un identificador del comerciante estático único emitido por un comprador, datos de solicitud de transacción y un valor dinámico único;

formando el dispositivo del cliente (22) una solicitud de autentificación del comerciante y transmitiendo la solicitud de autentificación del comerciante al dispositivo comercial (10) para solicitar al dispositivo comercial (10) un certificado firmado de un emisor (30) que contiene el identificador del comerciante estático único y la clave pública del comerciante, y una firma del valor dinámico único usando la clave privada del comerciante;

recibiendo el dispositivo del cliente (22) del dispositivo comercial (10) un segundo paquete de datos que comprende el certificado firmado del emisor y una firma del valor dinámico único usando la clave privada del comerciante;

autentificando el dispositivo del cliente (22) la legitimidad del dispositivo comercial (10) verificando el certificado firmado del emisor utilizando la clave pública de una autoridad de certificación y, una vez verificado, autentificando el valor dinámico único firmado contra el único valor dinámico recibido en el primer paquete de datos utilizando la clave pública del comerciante;

transmitiendo (48) el dispositivo del cliente (22) el identificador del comerciante estático único recibido y un criptograma al dispositivo comercial (22) solo si el valor dinámico único firmado se autentifica frente al valor dinámico único recibido en el primer paquete de datos usando la clave pública comercial, habiéndose generado el criptograma usando un clave secreta única para el dispositivo del cliente, un valor de contador, el identificador del comerciante estático único recibido y los datos de solicitud de transacción;

comprobando el dispositivo comercial (10) si el identificador del comerciante estático único recibido del dispositivo del cliente (22) coincide con el identificador del comerciante estático único emitido por el comprador y, si es así, formando una solicitud de autorización que comprende el criptograma recibido, el identificador del comerciante estático único y los datos de solicitud de transacción y envío (50) dicha solicitud de autorización a al menos uno de un emisor (30) y un comprador (28) para facilitar la autorización y el procesamiento de dichos datos de solicitud de transacción;

recibiendo el dispositivo comercial (10) una respuesta del emisor que indica si la transacción ha tenido éxito; y

notificando el dispositivo comercial (10) al dispositivo del cliente (22) si la transacción ha tenido éxito;

donde el comprador (28) conserva de forma segura una copia del identificador del comerciante estático único para verificar que un comerciante afiliado al dispositivo comercial (10) sea un comerciante válido.

2. Un procedimiento de acuerdo con la reivindicación 1 donde el establecimiento (44) de una conexión de datos entre el primer y segundo dispositivo transceptor (10) comprende el establecimiento de una conexión sin contacto o una conexión de contacto.

3. Un procedimiento de acuerdo con la reivindicación 2, donde el establecimiento (44) de una conexión de datos entre el primer y el segundo dispositivo transceptor (10) comprende el establecimiento de una conexión sin contacto y dicha conexión sin contacto utiliza al menos una de las tecnologías NFC, Bluetooth y WiFi.

4. Un procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además el mantenimiento de un contador incorporado en el dispositivo del cliente (22).

5. Un procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además la recepción de una solicitud de selección de la cuenta del usuario del dispositivo del cliente (22).

6. Un procedimiento de acuerdo con la reivindicación 5 donde la solicitud de selección de la cuenta se recibe a través de una interfaz de usuario del dispositivo del cliente (22), comprendiendo el procedimiento preferentemente la transmisión de la selección de la cuenta seleccionada por el usuario al dispositivo comercial (10) a través de la conexión de datos y almacenamiento de datos representativos de la cuenta seleccionada por el usuario en una memoria del dispositivo comercial (10).

7. Procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 4, donde se recibe una solicitud de selección de cuenta a través de una interfaz de usuario del dispositivo comercial (10), comprendiendo además el procedimiento la recuperación de una determinada cuenta predeterminada de una memoria (16) del dispositivo del cliente (22).

8. Un procedimiento de acuerdo con la reivindicación 6, que comprende además la transmisión de datos representativos de la cuenta seleccionada por el usuario a través de la conexión de datos al dispositivo del cliente (22).

9. Un procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además la recuperación de los datos de solicitud de la transacción, comprendiendo dichos datos de solicitud de la transacción una cantidad para la transacción, y al menos uno de un código de moneda, un sello de tiempo, datos representativos de la cuenta seleccionada por el usuario, y un identificador de cliente como por ejemplo un PIN o biométrico y un valor identificador del comerciante estático.

10. Un procedimiento para operar un primer dispositivo transceptor (10) configurado selectivamente como un dispositivo comercial (10) para asegurar datos de pago para una primera transacción de pago transmitida a través de una red de comunicación abierta, comprendiendo el procedimiento:

el establecimiento (44) de una conexión de datos con un segundo dispositivo transceptor (10) configurado como un dispositivo del cliente (22), pudiendo cada uno del primer y segundo dispositivo transceptor configurarse selectivamente como un dispositivo comercial (10) o un dispositivo del cliente (22);

la transmisión (48) de un primer paquete de datos al dispositivo del cliente (22) a través de la conexión de datos, comprendiendo el primer paquete de datos un identificador del comerciante estático único emitido por un comprador, datos de solicitud de transacción y un valor dinámico único;

la recepción del dispositivo del cliente (22) de una solicitud de autentificación del comerciante que solicita un certificado firmado de un emisor (30) que contiene el identificador del comerciante estático único y la clave pública del comerciante y una firma del valor dinámico único utilizando la clave privada del comerciante; y

la transmisión al dispositivo del cliente (22) de un segundo paquete de datos que comprende el certificado firmado del emisor y una firma del valor dinámico único usando la clave privada del comerciante;

donde si el dispositivo del cliente (22) se autentifica la legitimidad del dispositivo comercial (10) verificando el certificado firmado del emisor utilizando la clave pública de una autoridad de certificación y, una vez verificado, se autentifica el valor dinámico único firmado contra el único valor dinámico recibido en el primer paquete de datos utilizando la clave pública del comerciante; el procedimiento comprende además:

la recepción del dispositivo del cliente (22) el identificador del comerciante estático único y un criptograma, habiéndose generado el criptograma usando una clave secreta exclusiva para el dispositivo del cliente, un valor de contador, el identificador del comerciante estático único y los datos de solicitud de transacción;

la comprobación de si el identificador del comerciante estático único recibido del dispositivo del cliente (22) coincide con el identificador del comerciante estático único emitido por el comprador y, si es así, la formación de una solicitud de autorización que comprende el criptograma recibido, el identificador del comerciante estático único y los datos de solicitud de transacción y envío (50) dicha solicitud de autorización a al menos uno de un emisor (30) y un comprador (28) para facilitar la autorización y el procesamiento de dichos datos de solicitud de transacción;

la recepción de una respuesta del emisor que indique si la transacción ha tenido éxito; y

la notificación al dispositivo del cliente (22) si la transacción ha tenido éxito;

donde el comprador (28) conserva de forma segura una copia del identificador del comerciante estático único para verificar que un comerciante afiliado al dispositivo comercial (10) sea un comerciante válido.

11. Un procedimiento para operar un segundo dispositivo transceptor (10) configurado selectivamente como un dispositivo del cliente (22) para asegurar datos de pago para una primera transacción de pago transmitida a través de una red de comunicación abierta, comprendiendo el procedimiento:

el establecimiento (44) de una conexión de datos con un primer dispositivo transceptor configurado como un dispositivo comercial (10), pudiendo cada uno del primer y segundo dispositivo transceptor configurarse selectivamente como un dispositivo comercial (10) o un dispositivo del cliente (22);

la recepción (48) del dispositivo comercial (10) de un primer paquete de datos sobre la conexión de datos, comprendiendo el primer paquete de datos un identificador del comerciante estático único emitido por un comprador, datos de solicitud de transacción y un valor dinámico único;

la formación de una solicitud de autentificación del comerciante y transmitiendo la solicitud de autentificación del comerciante al dispositivo comercial (10) para solicitar al dispositivo comercial (10), un certificado firmado de un emisor (30) que contiene el identificador del comerciante estático único y la clave pública del comerciante, y una firma del valor dinámico único usando la clave privada del comerciante;

la recepción del dispositivo comercial (10) de un segundo paquete de datos que comprende el certificado firmado del emisor y una firma del valor dinámico único usando la clave privada del comerciante;

la autentificación de la legitimidad del dispositivo comercial (10) verificando el certificado firmado del emisor utilizando la clave pública de una autoridad de certificación y, una vez verificado, autentificando el valor dinámico único firmado contra el único valor dinámico recibido en el primer paquete de datos utilizando la clave pública del comerciante;

la transmisión (48) del identificador del comerciante estático único y un criptograma al dispositivo comercial (22) solo si el valor dinámico único firmado se autentifica frente al valor dinámico único recibido en el primer paquete de datos usando la clave pública comercial, habiéndose generado el criptograma usando un clave secreta única para el dispositivo del cliente, un valor de contador, el identificador del comerciante estático único recibido y los datos de solicitud de transacción; y

la recepción del dispositivo comercial (10) de una notificación que indique si la transacción ha tenido éxito;

donde el criptograma permite que el dispositivo comercial (10) una vez recibido compruebe si el identificador del comerciante estático único recibido del dispositivo del cliente (22) coincide con el identificador del comerciante estático único emitido por el comprador, y si es así, formar una solicitud de autorización que comprende el criptograma recibido, el identificador del comerciante estático único y los datos de solicitud de transacción y enviar (50) dicha solicitud de autorización a al menos uno de un emisor (30) y un comprador (28) para facilitar la autorización y el procesamiento de dichos datos de solicitud de transacción; y

donde el comprador (28) conserva de forma segura una copia del identificador del comerciante estático único para verificar que un comerciante afiliado al dispositivo comercial (10) sea un comerciante válido.

12. Un primer dispositivo transceptor operable para asegurar los datos de pago transmitidos a través de redes de comunicación abiertas, siendo el primer dispositivo transceptor configurable selectivamente como un dispositivo comercial (10) o un dispositivo transceptor del cliente (22), comprendiendo el primer dispositivo transceptor (10):

un módulo de interfaz (12) operable para permitir la comunicación de datos con otros dispositivos transceptores (10); y

un procesador (14) acoplado a una memoria (16), siendo la memoria (16) operable para almacenar el código de control del procesador;

donde cuando el primer transceptor se configura selectivamente como un dispositivo comercial (10), el código de

control del procesador es operable para controlar selectivamente el procesador (14) y el módulo de interfaz (12), cuando se ejecuta para:

establecer (44) una conexión de datos con un segundo dispositivo transceptor configurado como dispositivo del cliente (22);

recuperar de la memoria (16) un identificador del comerciante estático único, habiendo sido el identificador del comerciante estático único emitido por un comprador (28);

transmitir (48) un primer paquete de datos al dispositivo del cliente (22) a través de la conexión de datos, comprendiendo el primer paquete de datos el identificador del comerciante estático único, los datos de solicitud de transacción y un valor dinámico único;

recibir del dispositivo del cliente (22) una solicitud de autentificación del comerciante que solicita un certificado firmado de un emisor (30) que contiene el identificador del comerciante estático único y la clave pública del comerciante y una firma del valor dinámico único utilizando la clave privada del comerciante; y

transmitir al dispositivo del cliente (22) un segundo paquete de datos que comprende el certificado firmado del emisor y una firma del valor dinámico único usando la clave privada del comerciante;

donde si el dispositivo del cliente (22) autentifica la legitimidad del dispositivo comercial (10) verificando el certificado firmado del emisor usando la clave pública de la autoridad de certificación y, una vez verificado, autentifica el valor dinámico único firmado contra el valor dinámico único recibido en el primer paquete de datos usando la clave pública del comerciante, el código de control del procesador es operable para controlar selectivamente el procesador (14) y el módulo de interfaz (12), cuando se ejecuta para:

recibir (48) del dispositivo del cliente (22) el identificador del comerciante estático único y un criptograma, habiéndose generado el criptograma usando una clave secreta exclusiva para el dispositivo del cliente, un valor de contador, el identificador de comerciante estático único y los datos de solicitud de transacción;

comprobar si el identificador del comerciante estático único recibido del dispositivo del cliente (22) coincide con el identificador del comerciante estático único emitido por el comprador y, si es así, formar una solicitud de autorización que comprende el criptograma recibido, el identificador del comerciante estático único y los datos de solicitud de transacción y envío (50) dicha solicitud de autorización a al menos uno de un emisor (30) y un comprador (28) para facilitar la autorización y el procesamiento de dichos datos de solicitud de transacción;

recibir una respuesta del emisor que indique si la transacción ha tenido éxito y notificar a un usuario del dispositivo del cliente (22); y

notificar al dispositivo del cliente (22) si la transacción ha tenido éxito;

donde el comprador (28) conserva de forma segura una copia del identificador del comerciante estático único para verificar que un comerciante afiliado a un dispositivo comercial (10) sea un comerciante válido; o

donde cuando el primer transceptor se configura selectivamente como un dispositivo comercial (22), el código de control del procesador es operable para controlar selectivamente el procesador (14) y el módulo de interfaz (12), cuando se ejecuta para:

establecer (44) una conexión de datos con un segundo dispositivo transceptor configurado como dispositivo comercial (10);

recibir (48) del dispositivo comercial (10) un primer paquete de datos sobre la conexión de datos, comprendiendo el primer paquete de datos un identificador del comerciante estático único emitido por un comprador, datos de solicitud de transacción y un valor dinámico único;

formar una solicitud de autentificación del comerciante y transmitir la solicitud de autentificación del comerciante al dispositivo comercial (10) para solicitar al dispositivo comercial (10), un certificado firmado de un emisor (30) que contiene el identificador del comerciante estático único y la clave pública del comerciante, y una firma del valor dinámico único usando la clave privada del comerciante;

recibir del dispositivo comercial (10) un segundo paquete de datos que comprende el certificado firmado del emisor y una firma del valor dinámico único usando la clave privada del comerciante;

autentificar la legitimidad del dispositivo comercial (10) verificando el certificado firmado del emisor utilizando la clave pública de una autoridad de certificación y, una vez verificado, autentificando el valor dinámico único firmado contra el único valor dinámico recibido en el primer paquete de datos utilizando la clave pública del comerciante;

recuperar de la memoria (16) un valor de contador y una clave privada del dispositivo del cliente almacenado;

transmitir (48) del identificador del comerciante estático único y de un criptograma al dispositivo comercial (22) solo si el valor dinámico único firmado se autentifica frente al valor dinámico único recibido en el primer paquete de datos usando la clave pública del comercial, habiéndose generado el criptograma usando una clave secreta única recuperada para el dispositivo del cliente, un valor de contador recuperado, el identificador del comerciante estático único recibido y los datos de solicitud de transacción; y

recibir del dispositivo comercial (10) una notificación que indique si la transacción ha tenido éxito;

donde el criptograma permite que el dispositivo comercial (10) una vez recibido compruebe si el identificador del comerciante estático único recibido del dispositivo del cliente (22) coincide con el identificador del comerciante estático único emitido por el comprador, y si es así, formar una solicitud de autorización que comprende el criptograma recibido, el identificador del comerciante estático único y los datos de solicitud de transacción y enviar (50) dicha solicitud de autorización a al menos uno de un emisor (30) y un comprador (28) para facilitar la autorización y el procesamiento de dichos datos de solicitud de transacción; y

donde el comprador (28) conserva de forma segura una copia del identificador del comerciante estático único para verificar que un comerciante afiliado al dispositivo comercial (10) sea un comerciante válido.

13. Un primer dispositivo transceptor (10) de acuerdo con la reivindicación 12, donde el módulo de interfaz (12) tiene la forma de un módulo de interfaz de contacto, un módulo de interfaz sin contacto o un módulo de interfaz de contacto dual y sin contacto.

14. Un primer dispositivo transceptor (10) de acuerdo con la reivindicación 13, donde el módulo de interfaz (12) tiene la forma de un módulo de interfaz sin contacto que incorpora tecnología de comunicaciones de campo cercano.

15. Un primer dispositivo transceptor (10) de acuerdo con una cualquiera de las reivindicaciones 12 a 14, donde los datos de solicitud de transacción comprenden una cantidad para la transacción y al menos uno de un código de moneda, un sello de tiempo y un identificador de cliente como un PIN o biométrico.

16. Un dispositivo de comunicación móvil, dispositivo informático personal o dispositivo de punto de venta que tiene incorporado en él, un primer dispositivo transceptor (10) según una cualquiera de las reivindicaciones 12 a 15.

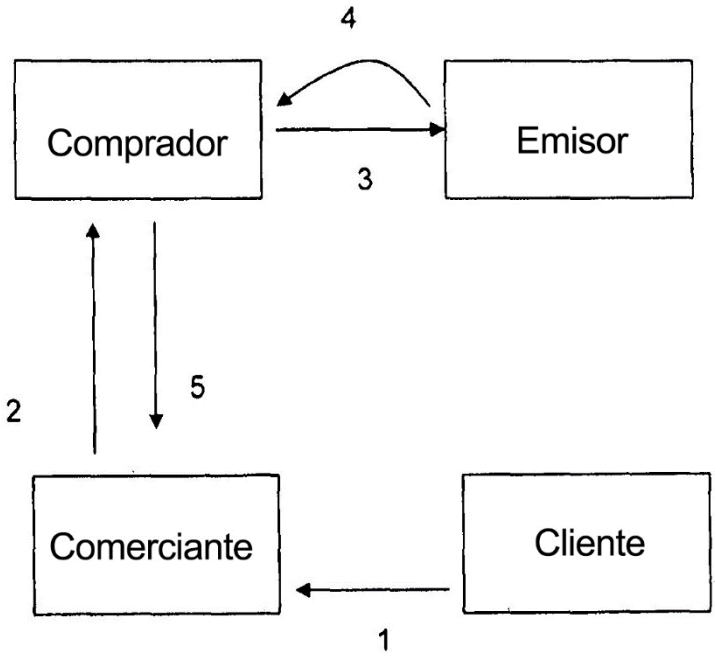

Fig. 1

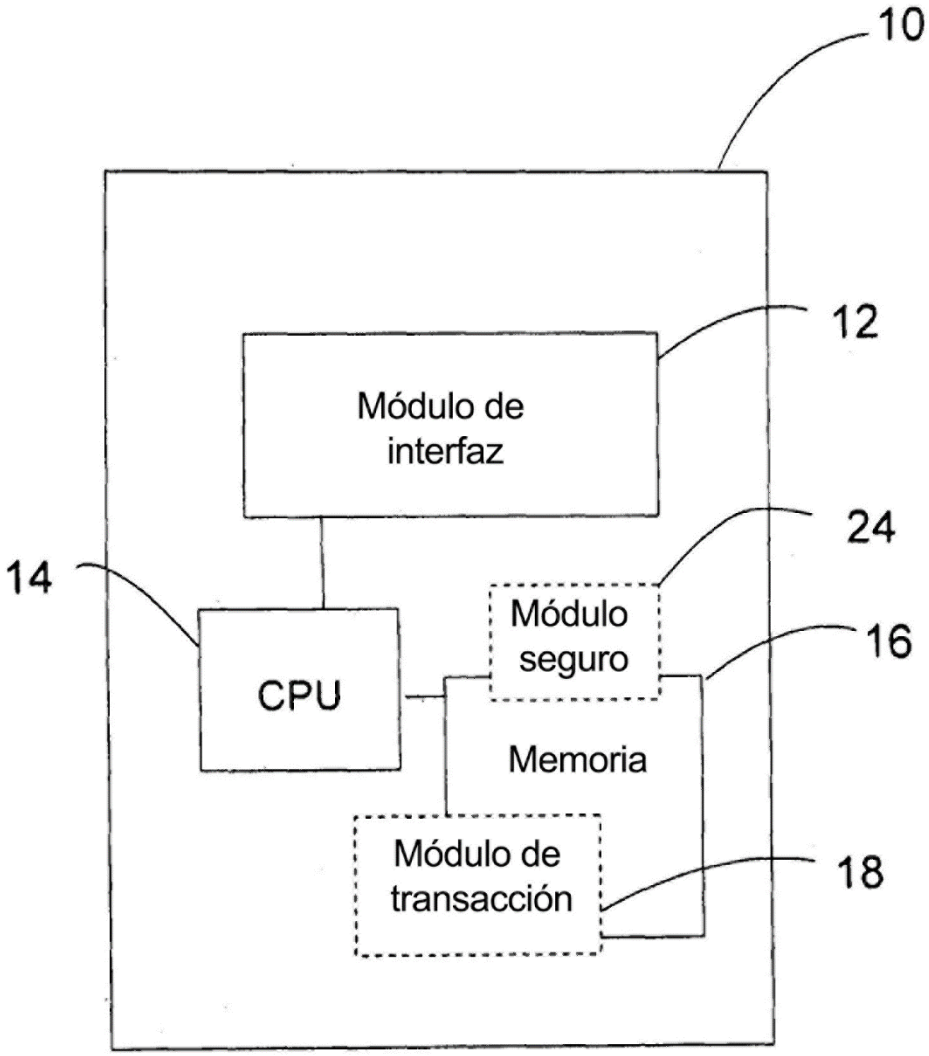
10
12
Módulo de interfaz
24
14
Módulo seguro
16
CPU
Memoria
Módulo de transacción
18

Fig. 2

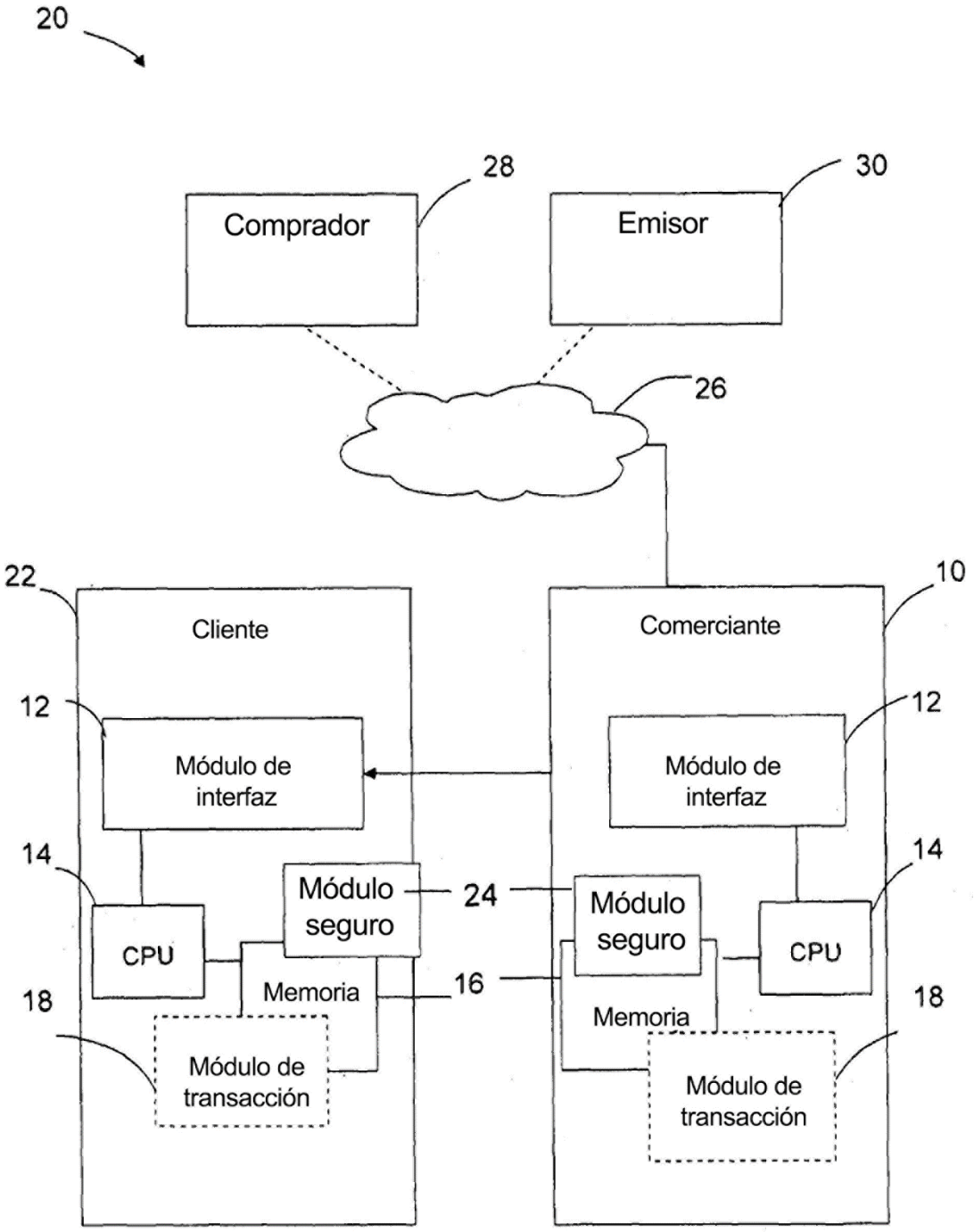
20
28
Comprador
30
Emisor
26
22
Cliente
10
Comerciante
12
Módulo de interfaz
12
Módulo de interfaz
14
Módulo seguro
24
Módulo seguro
14
CPU
Memoria
16
CPU
18
Módulo de transacción
Memoria
18
Módulo de transacción

Fig. 3

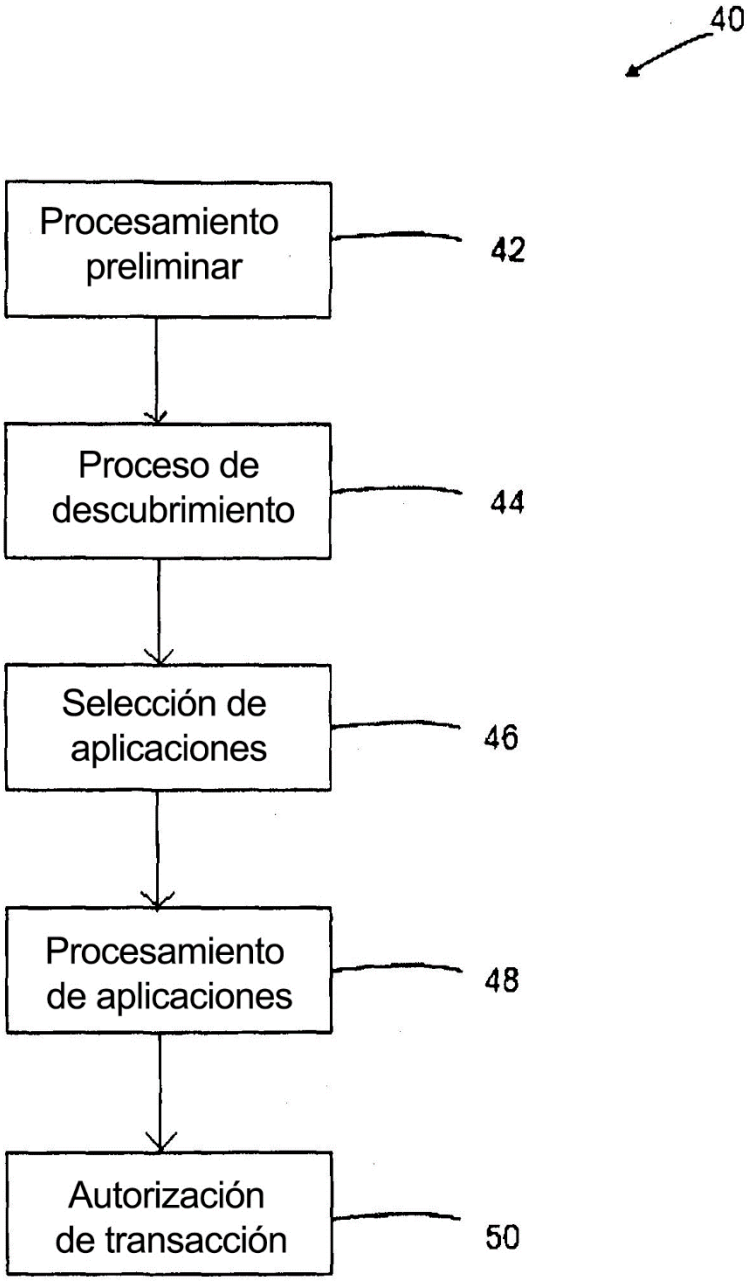
40
Procesamiento preliminar
42
Proceso de descubrimiento
44
Selección de aplicaciones
46
Procesamiento de aplicaciones
48
Autorización de transacción
50

Fig. 4

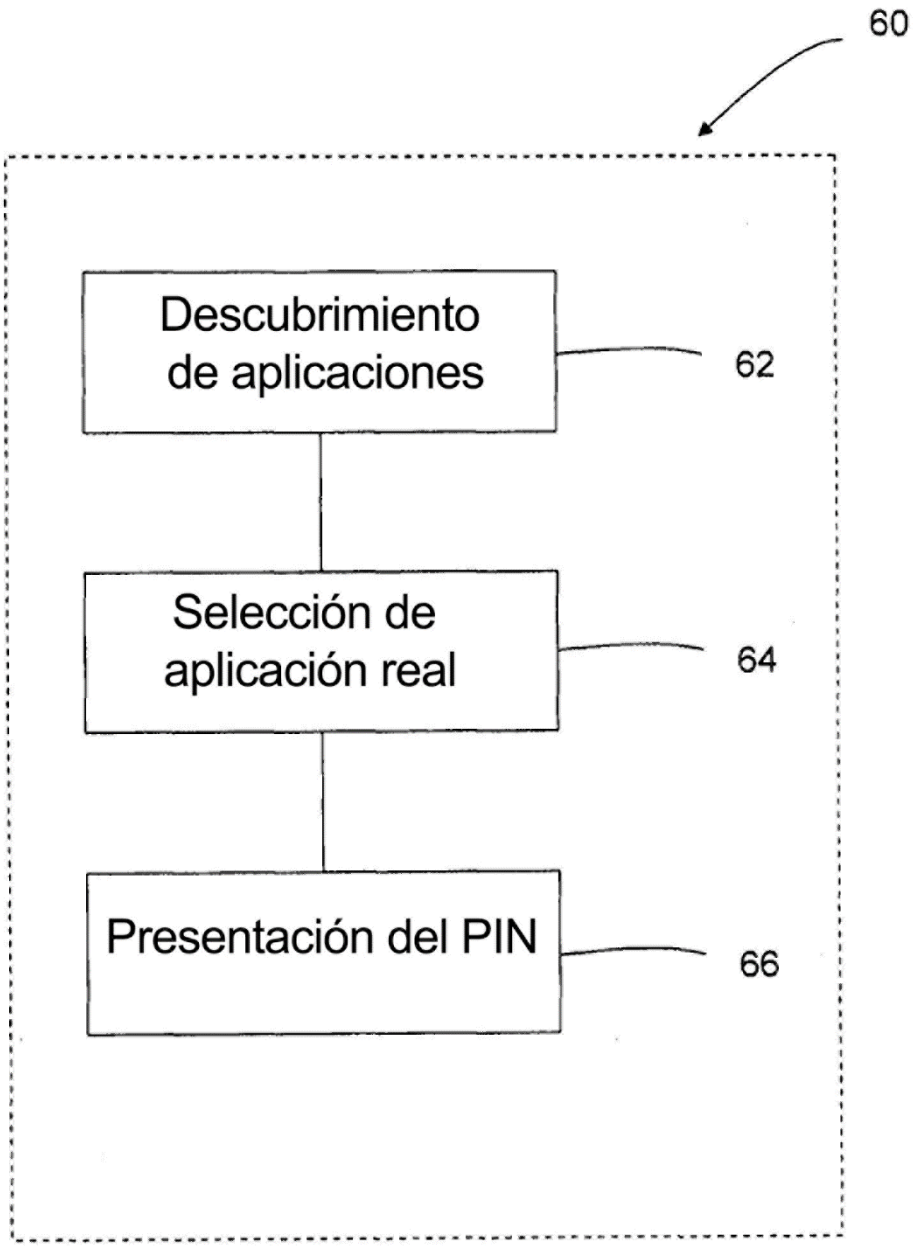
60
Descubrimiento de aplicaciones
62
Selección de aplicación real
64
Presentación del PIN
66

Fig. 5