(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 552 048**

(51) Int. CI.:

G07F 7/10 (2006.01)
G06Q 20/20 (2012.01)
G07F 7/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.03.2012 E 12716222 (0)**

(97) Fecha y número de publicación de la concesión europea: **05.08.2015 EP 2622585**

(54) Título: **Comprobación de PIN en una red "Hub and Spoke"**

(30) Prioridad:

07.02.2012 US 201261595867 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.11.2015

(73) Titular/es:

IZETTLE MERCHANT SERVICES AB (100.0%)
Kungsgatan 9
111 43 Stockholm, SE

(72) Inventor/es:

NILSSON, MAGNUS

(74) Agente/Representante:

MILTENYI, Peter

DESCRIPCIÓN

Comprobación de PIN en una red “Hub and Spoke”

Campo técnico

La invención se refiere en general al campo de las transacciones con tarjetas de pago electrónico seguro, y más particularmente, a un método y un sistema para pagos con tarjeta de débito y crédito seguros usando dispositivos de comunicación móvil tales como teléfonos móviles.

Antecedentes

Cada día, en todo el mundo, se realizan un número increíble de pagos con tarjeta de débito y crédito, y el número de pagos aumenta de manera continua.

EMV es la especificación para el sistema de pago más importante para las tarjetas de débito y crédito en el mercado y se desarrolló conjuntamente por las empresas Europay International, Mastercard International y Visa International, de ahí la abreviatura EMV. Para poder desarrollar un sistema de pago con tarjeta de débito y crédito que pueda usar tarjetas aprobadas por EMV convencionales, es esencial que el sistema de pago cumpla con la especificación EMV.

La mayor parte de pagos con tarjeta de débito y crédito siguen realizándose en tiendas que usan terminales de punto de venta (POS, *point-of-sale*) aprobados por EMV de gran tamaño y estacionarios. Sin embargo, en los últimos años ha aumentado rápidamente el interés, por parte del público y de las empresas, por poder realizar pagos con dispositivos de mano portátiles tales como teléfonos móviles. Sin embargo, el teléfono móvil no se considera un dispositivo seguro y no cumpliría con los requisitos para llevar a cabo un pago EMV. El principal problema de seguridad es la entrada del número de identificación personal (PIN) en el teléfono móvil que podría verse interceptada por un tercero usando por ejemplo software malicioso. Por tanto, es altamente deseable encontrar una manera de poder realizar pagos con tarjeta de débito y crédito seguros aprobados por EMV usando los teléfonos móviles habituales.

Sumario de la invención

Considerando la descripción anterior, entonces, un aspecto de la presente invención es proporcionar una manera de realizar pagos con tarjeta de débito y crédito seguros aprobados por EMV que permitan mitigar, aliviar o eliminar una o más de las deficiencias identificadas anteriormente en la técnica y las desventajas de manera individual o en cualquier combinación.

Un primer aspecto de la presente invención se refiere a un método según la reivindicación 1 para llevar a cabo pagos electrónicos con tarjeta de crédito a un adquiriente de pago usando un dispositivo del comerciante, que comprende un lector de tarjetas y un teléfono móvil, un dispositivo móvil del comprador, un servidor de pago y un servidor de banco.

En el método para llevar a cabo pagos electrónicos con tarjeta de crédito, la etapa de introducir el código PIN en dicha aplicación de entrada de PIN segura también puede comprender introducir información de seguridad de comprador y cifrar dicha información de seguridad de comprador e incluirla en dicho bloque de código PIN.

En el método para llevar a cabo pagos electrónicos con tarjeta de crédito, la etapa de recibir dicho bloque de código PIN en dicho servidor de pago también puede comprender descifrar dicha información de seguridad de comprador en dicho servidor de pago, y verificar dicha información de seguridad de comprador comparándola con dicha información de identificación de comprador.

En el método para llevar a cabo pagos electrónicos con tarjeta de crédito, dicha información de identificación de comprador puede ser cualquiera de: el número de teléfono móvil del comprador, una dirección de correo electrónico, una dirección postal, un número de seguridad social, una firma, un código de un solo uso, un número de identificación previamente registrado, una fotografía e información biométrica.

En el método para llevar a cabo pagos electrónicos con tarjeta de crédito, dicha etapa de lanzar una aplicación de entrada de PIN segura en dicho dispositivo móvil del comprador puede implicar lanzar una interfaz web cifrada que se cifra de manera única para cada evento de entrada de PIN, o un navegador web dedicado que puede descifrar el componente web de entrada de PIN y garantizar una entrada segura del código PIN.

En el método para llevar a cabo pagos electrónicos con tarjeta de crédito, dicha transmisión entre dicho dispositivo del comerciante y dicho servidor de pago, entre dicho servidor de pago y dicho dispositivo móvil del comprador, y entre dicho servidor de pago y dicho servidor de banco puede cifrarse usando comunicación de capa de conexión segura (*secure socket layer*) convencional.

En el método para llevar a cabo pagos electrónicos con tarjeta de crédito, dicho mensaje de recepción puede almacenarse en el servidor de pago, y es accesible por el comprador y/o el comerciante usando un navegador web, el dispositivo del comerciante o el dispositivo móvil del comprador.

Un segundo aspecto de la presente invención se refiere a un sistema para llevar cabo pagos electrónicos con tarjeta de crédito que comprende un dispositivo del comerciante, que comprende un lector de tarjetas y un teléfono móvil, un servidor de pago, un teléfono móvil del comprador y un servidor de banco, en el que dicho dispositivo del comerciante, servidor de pago, dispositivo del comprador y servidor de banco tienen medios transceptores y medios procesadores para llevar a cabo las etapas indicadas en el primer aspecto anteriormente.

Breve descripción de los dibujos

A partir de la siguiente descripción detallada de algunas realizaciones de la invención, en la que se describirán en más detalle algunas realizaciones de la invención con referencia a los dibujos adjuntos, resultarán evidentes objetos, características y ventajas adicionales de la presente invención. En los dibujos:

la figura 1 muestra un teléfono móvil para llevar a cabo pagos EMV autorizados con PIN, según una realización de la presente invención; y

la figura 2 muestra un diagrama de bloques de un sistema para llevar a cabo pagos EMV autorizados con PIN usando un teléfono móvil convencional, según una realización de la presente invención; y

la figura 3a muestra un diagrama de flujo que describe las etapas en un método para llevar a cabo pagos EMV autorizados con PIN usando un teléfono móvil convencional, según una realización de la presente invención; y

la figura 3b muestra un diagrama de flujo que es una continuación del diagrama de flujo en la figura 3a, según una realización de la presente invención; y

la figura 3c muestra un diagrama de flujo que es una continuación del diagrama de flujo en la figura 3a, según una realización de la presente invención.

Descripción detallada

A continuación en el presente documento, con referencia a los dibujos adjuntos en los que se muestran realizaciones de la invención, se describirán en más detalle realizaciones de la presente invención. Sin embargo, esta invención puede implementarse de muchas maneras diferentes y no se interpretará como limitada a las realizaciones expuestas en el presente documento. Más bien, estas realizaciones se proporcionan de modo que esta divulgación será completa y detallada, y transmitirá completamente el alcance de la invención a los expertos en la técnica. Los números de referencia similares se refieren a elementos similares en todo el documento.

Las realizaciones de la presente invención se explicarán con ejemplos usando un dispositivo de comunicación móvil tal como un teléfono móvil. Sin embargo, se apreciará que la invención como tal es igualmente aplicable a dispositivos electrónicos que tienen soporte de comunicación por radio inalámbrica y/o por cable. Ejemplos de tales dispositivos pueden ser, por ejemplo, cualquier tipo de teléfono móvil, ordenadores de mano portátiles (tales como los convencionales, ultraportátiles, *netbooks* y microordenadores portátiles), asistentes digitales portátiles, ordenadores tipo tableta, dispositivos de juego, accesorios de teléfonos móviles, etc. Sin embargo, por motivos de claridad y simplicidad, las realizaciones indicadas en esta memoria descriptiva se muestran como ejemplos con, y con respecto a, sólo teléfonos móviles.

La presente invención se refiere a pagos con tarjeta de débito y crédito aprobados por EMV usando un teléfono móvil convencional. A continuación en el presente documento el término tarjeta de crédito se referirá a tarjetas de crédito, tarjetas de débito, otro tipo de tarjetas electrónicas que pueden usarse y/o funcionan como tarjeta de débito o crédito. El término tarjeta de crédito también puede incluir un software que actúa como tarjeta de débito o crédito, o un servicio informático que actúa como tarjeta de débito o crédito. La figura 1 muestra un teléfono móvil 100 típico con medios de entrada 101, que pueden tener la forma de botones físicos o botones virtuales visualizados en una pantalla 102. El teléfono móvil puede tener además medios procesadores (no mostrados), para ejecutar aplicaciones seguras, y medios de comunicación (no mostrados) para conectarse a otros dispositivos de comunicación móvil y/o Internet, o bien por cable o bien de manera inalámbrica.

Anteriormente se ha mostrado que puede hacerse que los pagos con tarjeta de crédito sean seguros y aprobados por EMV usando un dispositivo de lector de tarjetas especializado que puede unirse a un teléfono móvil de la manera presentada en la solicitud de patente internacional con el número de solicitud PCT/EP2010/066186 de la empresa iZettle. Sin embargo, no ha sido posible llevar a cabo un pago EMV autorizado por PIN desde un teléfono móvil no conectado a un dispositivo de lector de tarjetas de pago puesto que el dispositivo de entrada de PIN, en este caso el teléfono móvil, se ha considerado poco seguro. El principal problema de seguridad es la etapa de introducir un código PIN (o alguna otra información de identificación sensible tal como una firma o información biométrica) usando el teclado del teléfono móvil. Es un hecho muy conocido que los programas de software malicioso pueden infectar el teléfono móvil y de manera secreta registrar la información de identificación sensible introducida, tal como un código PIN introducido con el teclado del teléfono móvil, y después transmitirla a un tercero con intenciones delictivas.

En general, un pago EMV con el lector de tarjetas de pago y un teléfono móvil se aprueba generalmente fuera de

línea, con el chip de tarjeta EMV (insertado en el lector de tarjetas de pago) como referencia de código PIN, para adquirir velocidad. También es posible autorizar el pago EMV en línea, con el banco como referencia de PIN, en el que el código PIN se transfiere directamente al servidor de banco en un bloque de datos cifrado. El pago también puede llevarse a cabo y verificarse mediante la firma por escrito del usuario.

Sin embargo, los requisitos de seguridad (protección frente a intentos de manipular indebidamente el dispositivo para obtener acceso al código PIN) impiden que los teléfonos móviles modernos actúen como dispositivo de entrada de PIN seguro para la entrada de códigos PIN. Por tanto, hasta ahora no ha sido posible realizar pagos EMV autorizados con PIN seguros a menos que tanto el dispositivo de lector de tarjetas como el dispositivo de entrada de PIN sean dispositivos seguros. Sin embargo, la presente invención dada a conocer a continuación presenta un método y un sistema que permiten que un teléfono móvil convencional lleve a cabo un pago EMV autorizado por PIN seguro en combinación con el método de pago muy conocido dado a conocer en la solicitud de patente internacional con el número de solicitud PCT/EP2010/066186.

La figura 2 presenta un sistema de pago seguro 200 según una realización de la presente invención en el que puede usarse un teléfono móvil (dispositivo móvil 203) para llevar a cabo un pago con tarjeta de débito o crédito EMV autorizado con PIN seguro. Para entender mejor la presente invención, y las realizaciones de la misma, a continuación se presenta un ejemplo de cómo puede realizarse un pago con tarjeta de crédito en el sistema de pago seguro 200 novedoso.

Cuando el comprador se ha decidido a comprar un producto o a pagar un servicio, entra en contacto con un comerciante para completar el pago del producto o servicio. Por tanto en este caso el adquiriente de pago es el comerciante o la empresa del comerciante que recibirá el pago por el producto o servicio. Se ejecuta una aplicación de pago, y de este modo se iniciará 301 una transacción de pago electrónico con tarjeta de crédito 300 (véase método de pago con tarjeta de crédito en la figura 3), en el teléfono móvil 203 (el dispositivo del comerciante 202, 203), o bien antes de que se traspase del comerciante al comprador o bien cuando el comerciante introduzca el lector de tarjetas 202 en el dispositivo 203 (y por tanto forme un dispositivo del comerciante 202, 203).

El comerciante o el comprador introduce información de venta 301, que por ejemplo puede ser información sobre el producto y la cantidad de la compra (precio), en dicho dispositivo del comerciante. La información de venta también puede incluir información sobre la empresa que vende el producto o servicio, tal como información que se encuentra habitualmente en recibos, información de GPS que ubica la tienda o la posición geográfica del vendedor, la cuenta del vendedor en el servidor de pago 205, la cuenta del vendedor en el banco 207 o cualquier otra información que pueda usarse para identificar al vendedor y/o el lugar de venta. La información de venta también puede leerse usando un lector de código de barras, lector de infrarrojos o un lector de comunicación de campo cercano (NFC, *near field communication*), integrado en el teléfono móvil 203, directamente desde el producto (por ejemplo la etiqueta del producto) o de un catálogo que enumera los productos y sus precios. En otra variante, parte o toda la información de venta puede descargarse o autogenerarse desde uno o varios servidores conectados al dispositivo del comerciante 202, 203.

El comprador inserta su tarjeta de crédito EMV 201 en el lector de tarjetas de pago 303 (el dispositivo del comerciante 202, 203) y de este modo inicia una transacción de pago con tarjeta de crédito segura 300. El comerciante le pasa su teléfono móvil 203 con un lector de tarjetas de pago 202 unido al mismo (a continuación en el presente documento denominado dispositivo del comerciante 202, 203) al comprador. Al comprador se le pide que introduzca información de identificación de comprador 304 que por ejemplo podría ser información de contacto tal como su número de teléfono móvil o dirección de correo electrónico en la aplicación de pago, si el comprador no introdujo su número de teléfono o dirección de correo electrónico anteriormente. El número de teléfono y/o la dirección de correo electrónico se almacenan en el servidor de pago 205 y se asocian con la tarjeta de débito o crédito EMV 201. Si el número de teléfono o la dirección de correo electrónico se introdujo anteriormente (es decir, si anteriormente se realizó un pago en la tienda), el usuario, en una variante, puede no tener que introducir la misma información de nuevo, a menos que use una tarjeta de pago EMV diferente. El lector de tarjetas de pago 202 lee la información de tarjeta EMV cifrada 201.

El método para completar el pago será una verificación del PIN fuera de línea si la tarjeta de pago EMV 201 soporta la verificación del PIN fuera de línea 315, 316. En caso de que la tarjeta de pago EMV 201 no soporte la verificación del PIN fuera de línea, el método para completar el pago será la verificación del PIN en línea con el banco 207. Si por alguna razón no es posible una verificación del PIN fuera de línea o en línea, el método de verificación puede ser introducir una firma.

La información de identificación de comprador que debe introducir el comprador mediante la aplicación de pago que se ejecuta en el dispositivo del comerciante 202, también puede ser cualquiera de: el número de teléfono móvil del comprador, una dirección de correo electrónico, una dirección postal, un número de seguridad social, un código de un solo uso, una firma, un número de identificación previamente registrado, una fotografía (realizada por la cámara en el teléfono móvil 203), información biométrica (leída o escaneada mediante el teléfono móvil 203 o algún adaptador conectado al teléfono móvil 203) o cualquier otra información que haga posible identificar al comprador en cuestión.

En una primera realización el comprador verificará el pago usando su código PIN asociado con la tarjeta EMV 201 con la que está pagando, y por tanto el comprador, en la aplicación de pago, también recibirá un enlace a página web de entrada de PIN en el dispositivo móvil del comprador 208. Esta etapa es la misma tanto en el caso de aplicar una verificación del PIN en línea como fuera de línea. Como el comprador verificará el pago usando su código PIN asociado con la tarjeta EMV 201 se genera una petición de entrada de PIN mediante la aplicación de pago.

Cuando el comprador ha completado la tarea de introducir información de identificación de comprador 305, se transmite un mensaje de compra cifrado desde el dispositivo del comerciante 202, 203, de manera inalámbrica (o por cable) por Internet 204, a un servidor de pago 205. El mensaje de compra cifrado puede contener parte o toda la información cifrada siguiente:

- la información de identificación de comprador,
- la petición de entrada de PIN,
- la información de venta y
- la información de tarjeta de crédito cifrada

leída por el lector de tarjetas 202 desde la tarjeta EMV del comprador 201. En una variante sólo se cifran la información de identificación de comprador y la información de tarjeta de crédito y la petición de entrada de PIN y la información de venta se transmiten como texto sin formato al servidor de pago 205. La transmisión por Internet 204 puede cifrarse o no usando la técnica de capa de conexión segura convencional.

El servidor de pago 205 recibe el mensaje de compra cifrado 306 procedente del dispositivo del comerciante 202, 203 y descifra el contenido del mensaje de compra y almacena temporalmente la información de tarjeta de crédito cifrada y la información de venta.

En una variante de la realización de la presente invención el servidor de pago 205 puede verificar entonces que la información relativa a la cuenta del comerciante o bien en el servidor de pago 205 o bien en el servidor de banco 207 es legítima y no está en una lista negra por algún motivo. La verificación puede o bien realizarse con el servidor de banco 207 directamente o bien puede comprobarse con un registro en el servidor de pago 205 que puede actualizarse regularmente con el registro del servidor de banco 207.

La información de identificación de comprador (y/o la información de tarjeta de crédito) se usa para determinar información de contacto del comprador 307 registrada en el servidor de pago 205. La información de contacto del comprador puede ser por ejemplo una dirección de correo electrónico, un número de teléfono móvil, identificación de red social (tal como la identificación de *Facebook* o *LinkedIn*) o cualquier otra información que puede usarse para ponerse en contacto con el comprador. En este ejemplo la información de identificación de comprador registrada previamente recibida es un número de teléfono móvil del teléfono móvil del comprador. En una variante la información de contacto del comprador se suministra en dicha información de identificación de comprador y no se almacena en dicho servidor de pago.

El servidor de pago 205 puede transmitir entonces una petición de código PIN 308 al dispositivo móvil del comprador 208 usando la información de contacto del comprador (por ejemplo el número de teléfono móvil). La transmisión de la petición de código PIN al dispositivo móvil del comprador 208 puede realizarse por Internet 204. La conexión a Internet puede ser por la red del teléfono móvil, Wi-Fi, o puede conectarse a una conexión de Internet de línea fija. La transmisión por Internet 204 puede estar o no cifrada usando la técnica de capa de conexión segura convencional.

En una variante, el servidor de pago 205 también puede verificar que la petición de entrada de PIN es legítima por ejemplo comparando las posiciones geográficas del dispositivo del comerciante y el teléfono móvil del comprador 208. Este enfoque requiere que tanto el dispositivo del comerciante 202, 203 como el dispositivo móvil 208 transmitan su ubicación al servidor de pago 205 para su comparación. El comprador puede por ejemplo iniciar el pago transmitiendo las coordenadas del dispositivo móvil 208 al servidor de pago 205, y las coordenadas del comerciante pueden o bien haberse registrado previamente en el servidor de pago 205 (una tienda habitualmente no cambia su ubicación tan a menudo) o bien estar incluidas en el mensaje de compra cifrado transmitido desde el dispositivo del comerciante 202, 203, de manera inalámbrica (o por cable) por Internet 204, al servidor de pago 205.

En una variante, la petición de código PIN puede contener información (tal como información de verificación escrita) para el comprador sobre que el código PIN no debe introducirse en caso de que el comprador haya sido el que ha iniciado la transacción de pago EMV de tarjeta segura.

Cuando la petición de código PIN se recibe en el dispositivo móvil del comprador 208, 3409 se lanza una aplicación de entrada de PIN segura. La aplicación de entrada de PIN segura que se ejecuta en el dispositivo móvil del comprador 208 puede implementarse como interfaz web cifrada que se cifra de manera única para cada evento de entrada de PIN. La interfaz web puede aparecer en una aplicación segura, que establece un canal de comunicación segura y cifrada entre el dispositivo móvil 208 y el servidor de pago 205, diferente del navegador web del teléfono

móvil para minimizar el riesgo de manipulación indebida del software. La aplicación de entrada de PIN segura puede ser en este caso un navegador web dedicado adaptado para descifrar el componente web de entrada de PIN y garantizar una entrada segura del código PIN 310.

En una variante, una página web de entrada de PIN segura (a continuación en el presente documento también denominada aplicación de entrada de PIN segura) en el dispositivo móvil del comprador 208 establece una conexión segura y cifrada con el servidor de pago 205 y cifrará el código PIN de manera asimétrica, usando la clave pública de la tarjeta de pago EMV 202.

Alternativamente, una aplicación de entrada de PIN segura puede ser una aplicación compilada, lanzada en el dispositivo móvil 208 del comprador de lo contrario poco seguro, que se ejecuta en el sistema operativo del dispositivo móvil. El sistema operativo del teléfono móvil puede ser cualquiera de iOS, Android, Windows Phone, Linux u otro SO de teléfono móvil. La aplicación de entrada de PIN segura en el dispositivo móvil del comprador 208 establece una conexión segura y cifrada con el servidor de pago 205.

La aplicación de entrada de PIN segura lanzada en el dispositivo móvil del comprador 208 crea un entorno seguro en el teléfono móvil usando por ejemplo una técnica de entorno de pruebas basada en web. De este modo el comprador puede introducir de manera segura su código PIN 311 sin el riesgo de que el programa de un tercero malicioso lo intercepte. La representación real de números y/o letras en la aplicación de entrada de PIN puede crearla de manera única para el evento el servidor de pago, usando una clave segura tal como la clave pública de la tarjeta de pago EMV 201, y no se reutilizará, lo que significa que incluso si la comunicación entre la aplicación de entrada de PIN en el dispositivo móvil 208 y el servidor de pago 205 se intercepta y descifra, los números y/o letras sólo tienen sentido cuando se combinan con una clave segura en el servidor de pago 205.

El comprador también puede estar asociado o contribuir con cierta información de seguridad, tal como la ubicación geográfica actual del dispositivo móvil del comprador 208, un ID de transacción, el número IMEI del dispositivo móvil, el número MSISDN, el número de seguridad social, la firma, información biométrica y/u otra información de seguridad que puede ser única para el usuario. Si la ubicación geográfica del dispositivo del comerciante 202, 203 se almacena o conoce en el servidor de pago 205 (véase más arriba con respecto a cómo puede conseguirse), las posiciones del dispositivo del comerciante y el teléfono móvil del comprador pueden compararse para garantizar que el pago se completa en la misma ubicación o en ubicaciones previamente aprobadas.

El código PIN introducido por el comprador en la aplicación de entrada de PIN segura lanzada en el dispositivo móvil del comprador 208 se cifra en un bloque de código PIN. Si va a transmitirse más información que el código PIN al servidor de pago 205, 312, la información de seguridad de comprador se cifra por separado en el momento de la entrada y no se envía en el mismo paquete al servidor de pago 205. El bloque de código PIN cifrado se transmite desde el dispositivo móvil del comprador 208 al servidor de pago 312 por Internet 204. El cifrado usado en el dispositivo móvil 208 puede cumplir con los requisitos de las normas de seguridad a nivel mundial de la transferencia en línea de detalles de tarjetas de crédito. El cifrado puede mejorarse adicionalmente usando la técnica de capa de conexión segura para la transmisión por Internet 204.

El servidor de pago 205 recibe el bloque de código PIN cifrado 313 y, si está disponible, la información de seguridad de comprador desde el dispositivo móvil 208. El servidor de pago 205 descifra y almacena la información de seguridad de comprador, si está presente. En una variante, el servidor de pago 205 puede comparar la información de seguridad de comprador con información de seguridad de comprador ya almacenada o con la información de identificación de comprador para determinar si el comprador es legítimo o no.

La verificación del código PIN puede realizarse o bien en línea con el banco o bien fuera de línea 314 con la información almacenada en la tarjeta de crédito en el lector de tarjetas de crédito del comerciante. El realizar una verificación en línea o fuera de línea puede determinarse de diferentes maneras 314. Una manera es que se decide (por ejemplo se elige desde un menú o basándose en información de conectividad del servidor de pago) en el dispositivo del comerciante 202, 203 cuando se inicia el pago o puede decidirse automáticamente en el servidor de pago 205 (dependiendo de la conectividad actual al servidor de banco 207 o dependiendo de una configuración en el servidor de pago 205).

En caso de que se determine que la verificación del código PIN será una verificación fuera de línea 315, el servidor de pago 205 enviará el bloque de código PIN cifrado al lector de tarjetas del comerciante 202 para la verificación usando el chip seguro en la tarjeta de pago EMV 201. El bloque de código PIN se descifra en dicho lector de tarjetas y se verifica con la información de PIN en dicha tarjeta de crédito insertada. El método de cifrado usado en la transmisión cumple con los requisitos de las normas de seguridad a nivel mundial de la transferencia en línea de detalles de tarjetas de crédito.

En caso de que el código PIN se verifique en la tarjeta de crédito, todavía es necesario verificar la cantidad de la compra con la cuenta del banco en un servidor de banco 207. La verificación de la cantidad de la compra se lleva a cabo enviando la información de venta con la cantidad de la compra desde el dispositivo del comerciante 202, 203 al servidor de pago 205, donde se lleva a cabo la autorización de la cantidad enviando la información de tarjeta de crédito y la información de venta en un formato cifrado por una comunicación de capa de conexión segura con un

método de cifrado que cumple con los requisitos de las normas de seguridad a nivel mundial de la transferencia en línea de información de tarjetas de débito o crédito, al servidor de banco 207. El servidor de banco 207 verifica si la cantidad de la compra puede cargarse o no, y transmite un mensaje de verificación de compra 317 por una comunicación de capa de conexión segura de vuelta al servidor de pago 205, 318.

En caso de que se determine que la verificación del código PIN será una verificación en línea 316, el servidor de pago 205 transmitirá el bloque de código PIN cifrado previamente recibido y almacenado, información de venta junto con la información de tarjeta de crédito, al servidor de banco 207 para su verificación en línea. La transmisión se cifra con un método que cumple con los requisitos de las normas de seguridad a nivel mundial de la transferencia en línea de detalles de tarjetas de crédito a través de una capa de conexión segura. El servidor de banco 207 recibe la información de tarjeta de crédito cifrada, información de venta (con la cantidad de la compra) y el bloque de código PIN cifrado, los descifra, y verifica el código PIN. El servidor de banco 207 completa la verificación en línea transmitiendo un mensaje de verificación 317 al servidor de pago 205, 318 con una verificación que manifiesta que el código PIN se ha aprobado. La comunicación con el servidor de banco 207 se produce según la norma EMV lo que significa que interacciona con el banco. La información de venta se transfiere al banco como una parte de la comunicación para verificar la cantidad de la compra con la cuenta bancaria del comprador y el bloque de PIN cifrado y la información de tarjeta de crédito como otra parte de la comunicación. El banco responde que la información de venta (la cantidad) puede cargarse como una parte de la comunicación y que el bloque de PIN y la información de tarjeta de crédito es correcta, como otra.

Cuando el servidor de pago 205 ha recibido las verificaciones con respecto al código PIN y la cantidad, el servidor de pago 205 genera un mensaje de recepción 319 como prueba de la transacción. El comprador y el comerciante obtendrán entonces el mensaje de recepción, transmitiéndose dicho mensaje de recepción a dicho dispositivo móvil del comprador y dicho dispositivo del comerciante a través de dicho servidor de pago 320, informándoles de que la transacción se ha aprobado mediante uno o varios de los siguientes: en una aplicación dedicada, por SMS, por MMS, por correo electrónico, por mensajería instantánea o cualquier otro método de comunicación al que pueda accederse desde un teléfono móvil 203, 208. El mensaje de recepción enviado desde el servidor de pago 205 se visualiza en la pantalla del dispositivo 321, cuando lo reciben el dispositivo del comerciante 202, 203 y el dispositivo móvil del comprador 208, indicando por tanto que el pago se ha recibido y que es correcto.

Si alguna de las etapas de verificación mencionadas anteriormente en la descripción anterior no funciona, se rechaza o es errónea, se genera un mensaje de error y se transmite al dispositivo del comerciante o al dispositivo móvil del comprador 208, o a ambos, y se termina o interrumpe el proceso de pago.

El mensaje de recepción también puede almacenarse en el servidor de pago 205 y el comprador y/o el comerciante pueden acceder al mismo en un momento posterior usando por ejemplo un navegador web que se conecta al servidor de pago 205. También puede accederse al mensaje de recepción ordenándolo desde (por tanto el servidor de pago lo enviaría) o accediendo directamente al mismo en el servidor de pago 205 usando el dispositivo del comerciante o el dispositivo móvil del comprador 208.

REIVINDICACIONES

1. Método para llevar a cabo pagos electrónicos con tarjeta de crédito a un adquiriente de pago usando un dispositivo del comerciante (202, 203), un dispositivo móvil del comprador (208), un servidor de pago (205) y un servidor de banco (207), comprendiendo el dispositivo del comerciante un lector de tarjetas (202) y un teléfono móvil (203), comprendiendo dicho método:

- iniciar una transacción de pago electrónico con tarjeta de crédito ejecutando una aplicación de pago en dicho dispositivo del comerciante (301);

- introducir información de venta en dicho dispositivo del comerciante (302);

- introducir una tarjeta de crédito (201) en dicho lector de tarjetas de dicho dispositivo del comerciante (303);

- introducir información de identificación de comprador y generar una petición de entrada de número de identificación personal (PIN) en dicho dispositivo del comerciante (304);

- transmitir un mensaje de compra cifrado desde dicho dispositivo del comerciante a dicho servidor de pago, en el que dicho mensaje de compra cifrado comprende una petición de entrada de PIN y al menos una de información de venta, información de identificación de comprador e información de tarjeta de crédito cifrada leída desde dicha tarjeta de crédito en dicho lector de tarjetas (305);

- recibir y descifrar dicho mensaje de compra cifrado en dicho servidor de pago (306);

- determinar, en el servidor de pago, dicha información de contacto del comprador usando dicha información de identificación del comprador en dicho mensaje de compra cifrado descifrado (307);

- transmitir, desde dicho servidor de pago, una petición de código PIN a dicho dispositivo móvil del comprador basándose en dicha información de contacto del comprador (308);

- recibir dicha petición de código PIN en dicho dispositivo móvil del comprador, y lanzar una aplicación de entrada de PIN segura en dicho dispositivo móvil del comprador (309);

- introducir un código PIN en dicha aplicación de entrada de PIN segura (310);

- cifrar el código PIN en un bloque de código PIN, en el dispositivo móvil del comprador;

- transmitir dicho bloque de código PIN que comprende dicho código PIN cifrado desde dicho dispositivo móvil del comprador a dicho servidor de pago (312);

- recibir dicho bloque de código PIN en dicho servidor de pago (313);

- determinar, en dicho servidor de pago, si va a realizarse una verificación de dicho código PIN fuera de línea o en línea (314); en caso de que se determine que la verificación del código PIN es una verificación fuera de línea (315), realizar las etapas de:

i. transmitir dicho bloque de código PIN desde dicho servidor de pago a dicho lector de tarjetas de dicho dispositivo del comerciante;

ii. descifrar, en dicho lector de tarjetas de dicho dispositivo del comerciante, dicho bloque de código PIN y verificar dicho bloque de código PIN con información de PIN en dicha tarjeta de crédito;

iii. transmitir información de venta desde dicho dispositivo del comerciante a dicho servidor de pago;

iv. transmitir dicha información de tarjeta de crédito y dicha información de venta desde dicho servidor de pago a dicho servidor de banco; y

v. verificar dicha información de tarjeta de crédito e información de venta en dicho servidor de banco;

en caso de que se determine que la verificación del código PIN es una verificación en línea (316), realizar las etapas de:

i. transmitir dicho bloque de código PIN, dicha información de tarjeta de crédito y dicha información de venta desde dicho servidor de pago a dicho servidor de banco; y

ii. verificar dicho código PIN, dicha información de tarjeta de crédito y dicha información de venta en dicho servidor de banco;

- producir un mensaje de verificación en dicho servidor de banco basándose en dicha verificación (317);

- transmitir dicho mensaje de verificación desde dicho servidor de banco a dicho servidor de pago (318);

- generar un mensaje de recepción en dicho servidor de pago basándose en el mensaje de verificación recibido (319);

- transmitir dicho mensaje de recepción a dicho dispositivo móvil del comprador y dicho dispositivo del comerciante a través de dicho servidor de pago (320); y

- visualizar dicho mensaje de recepción en dicho dispositivo móvil del comprador y en dicho dispositivo del comerciante completando dicho pago electrónico (321) con tarjeta de débito o crédito.

2. Método para llevar a cabo pagos electrónicos con tarjeta de crédito según la reivindicación 1, en el que la etapa de introducir código PIN en dicha aplicación de entrada de PIN segura también comprende:

- introducir información de seguridad de comprador; y

- cifrar dicha información de seguridad de comprador e incluirla en dicho bloque de código PIN.

3. Método para llevar a cabo pagos electrónicos con tarjeta de crédito según la reivindicación 2, en el que la etapa de recibir dicho bloque de código PIN en dicho servidor de pago también comprende:

- descifrar dicha información de seguridad de comprador en dicho servidor de pago, y

- verificar dicha información de seguridad de comprador con dicha información de identificación de comprador.

4. Método para llevar a cabo pagos electrónicos con tarjeta de crédito según cualquiera de las reivindicaciones anteriores, en el que dicha información de identificación de comprador puede ser cualquiera de: el número de teléfono móvil del comprador, una dirección de correo electrónico, una dirección postal, un número de seguridad social, una firma, un código de un solo uso, un número de identificación previamente registrado, una fotografía e información biométrica.

5. Método para llevar a cabo pagos electrónicos con tarjeta de crédito según cualquiera de las reivindicaciones anteriores, en el que dicha etapa de lanzar una aplicación de entrada de PIN segura en dicho dispositivo móvil del comprador implica lanzar una interfaz web cifrada que se cifra de manera única para cada evento de entrada de PIN, o un navegador web dedicado que puede descifrar el componente web de entrada de PIN y garantizar una entrada segura del código PIN.

6. Método para llevar a cabo pagos electrónicos con tarjeta de crédito según cualquiera de las reivindicaciones anteriores, en el que dicha transmisión entre dicho dispositivo del comerciante y dicho servidor de pago, entre dicho servidor de pago y dicho dispositivo móvil del comprador, y entre dicho servidor de pago y dicho servidor de banco se cifra usando una comunicación de capa de conexión segura convencional.

7. Método para llevar a cabo pagos electrónicos con tarjeta de crédito según cualquiera de las reivindicaciones anteriores, en el que dicho mensaje de recepción se almacena en el servidor de pago, y es accesible por el comprador y/o el comerciante usando un navegador web, el dispositivo del comerciante o el dispositivo móvil del comprador.

8. Sistema (200) para llevar cabo pagos electrónicos con tarjeta de crédito que comprende un dispositivo del comerciante (202, 203) que comprende un lector de tarjetas (202) y un teléfono móvil (203), un servidor de pago (205), un teléfono móvil del comprador (208) y un servidor de banco (207), en el que dicho dispositivo del comerciante, servidor de pago, dispositivo del comprador y servidor de banco tienen medios transceptores y medios procesadores para llevar a cabo las etapas indicadas en las reivindicaciones 1-7.

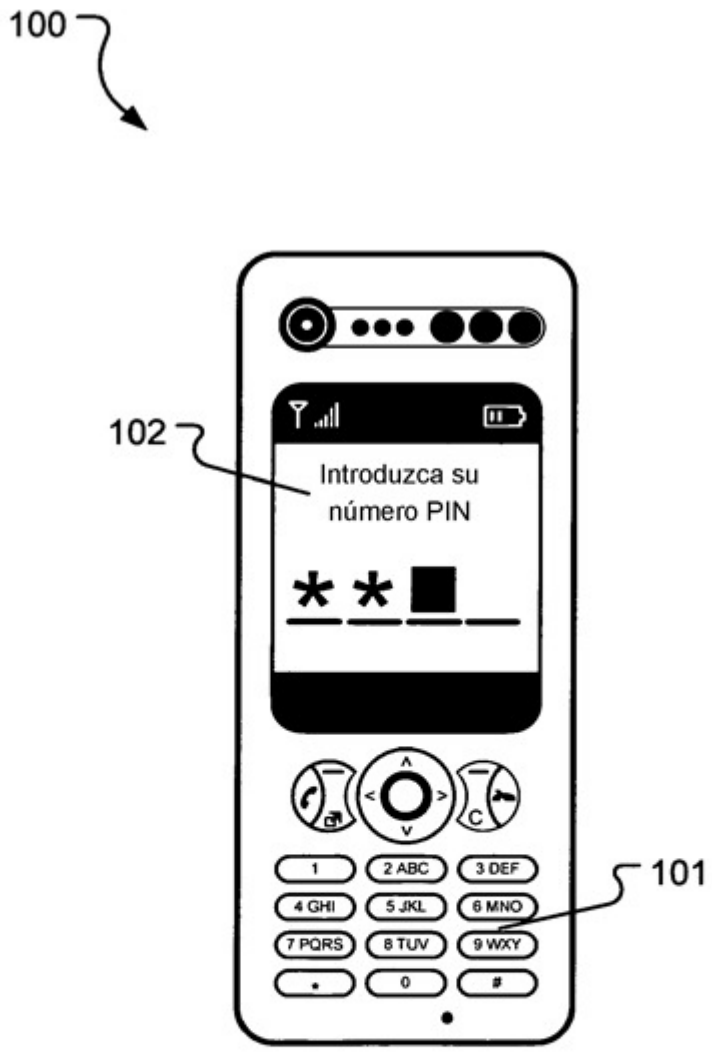

100
102
Introduzca su
número PIN
101
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXY
0

Fig. 1

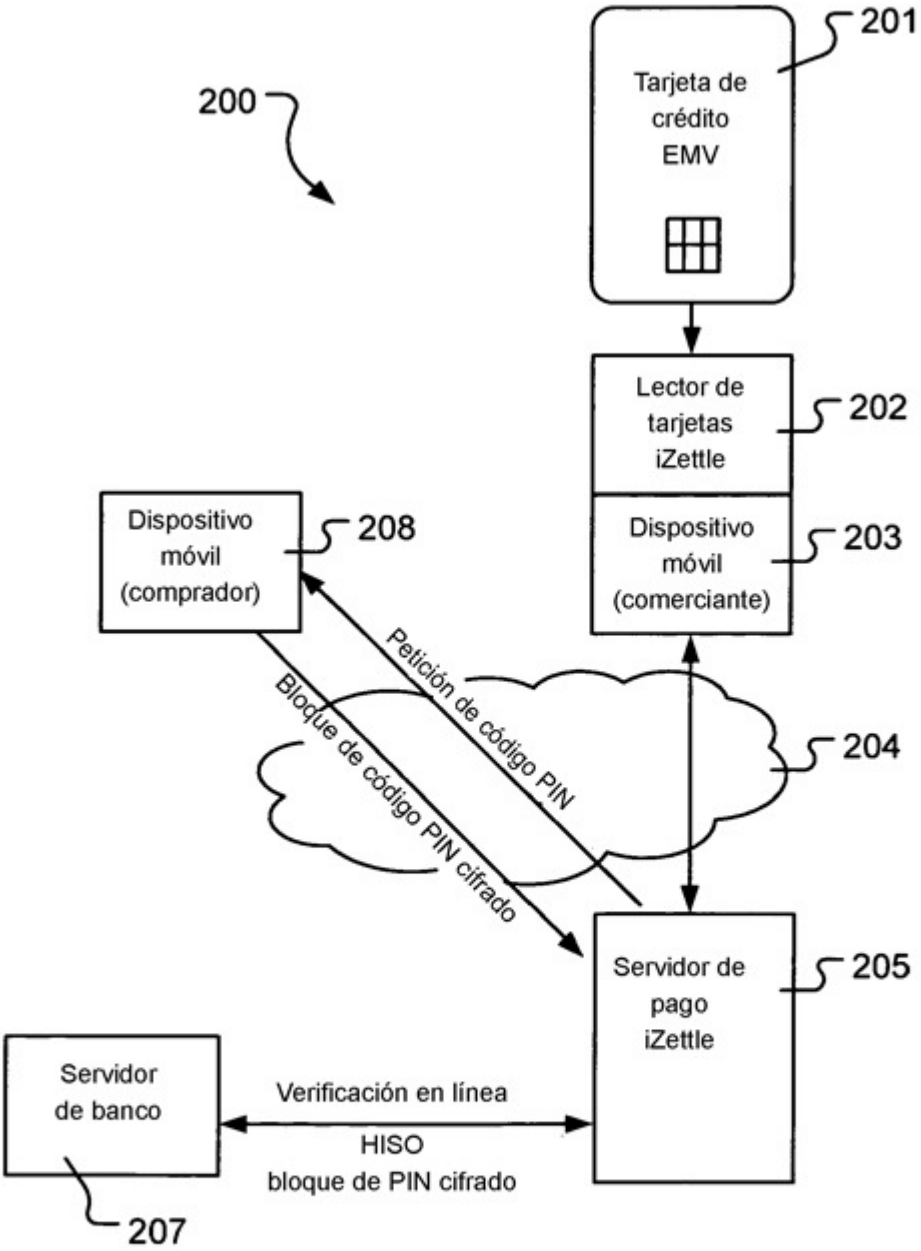
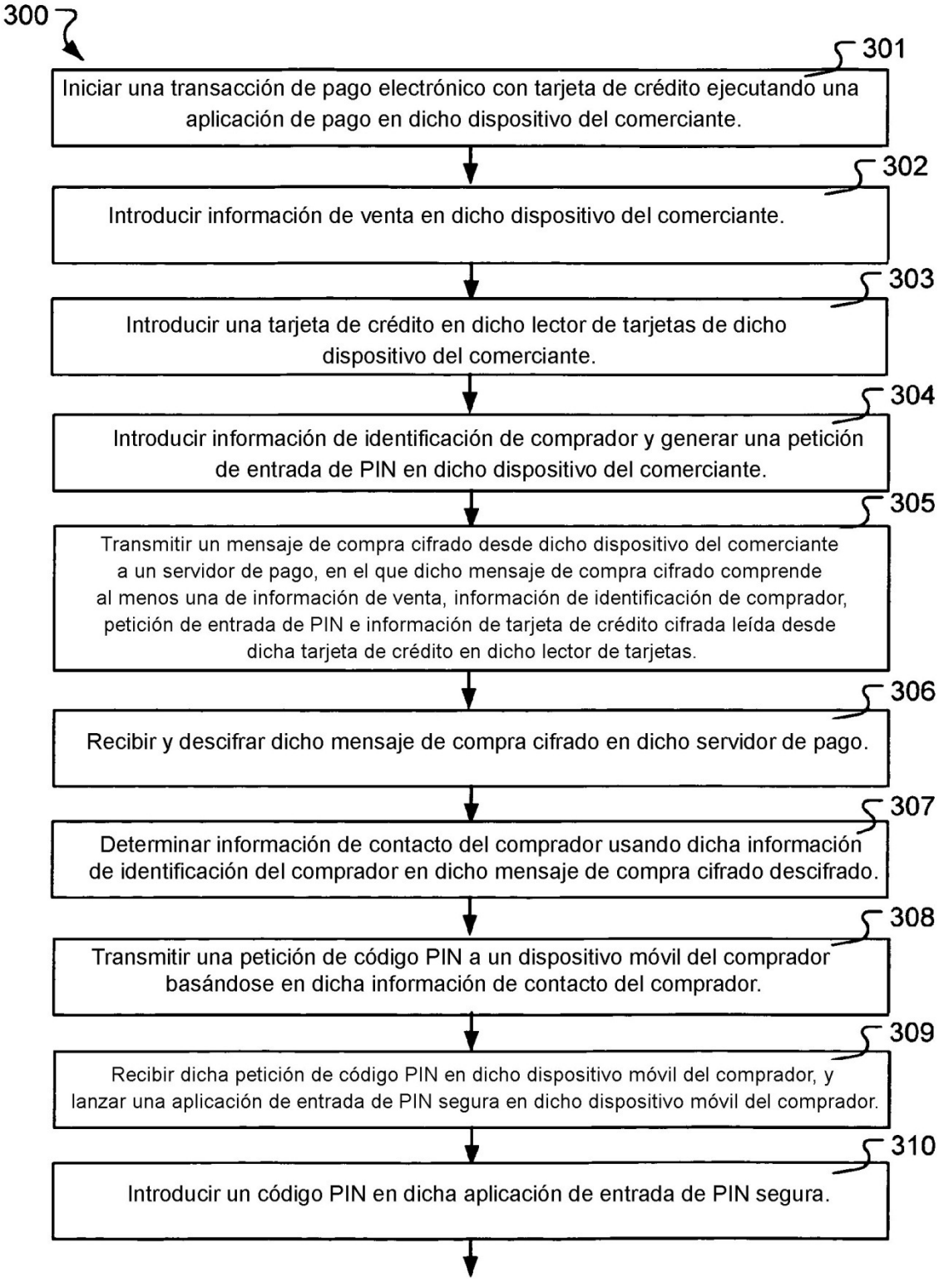

200
201
Tarjeta de crédito EMV
Lector de tarjetas iZettle
202
Dispositivo móvil (comerciante)
203
Dispositivo móvil (comprador)
208
Petición de código PIN
Bloque de código PIN cifrado
204
Servidor de pago iZettle
205
Servidor de banco
Verificación en línea
HISO
bloque de PIN cifrado
207

Fig. 2



Cont. en la figura 3b

Fig. 3a

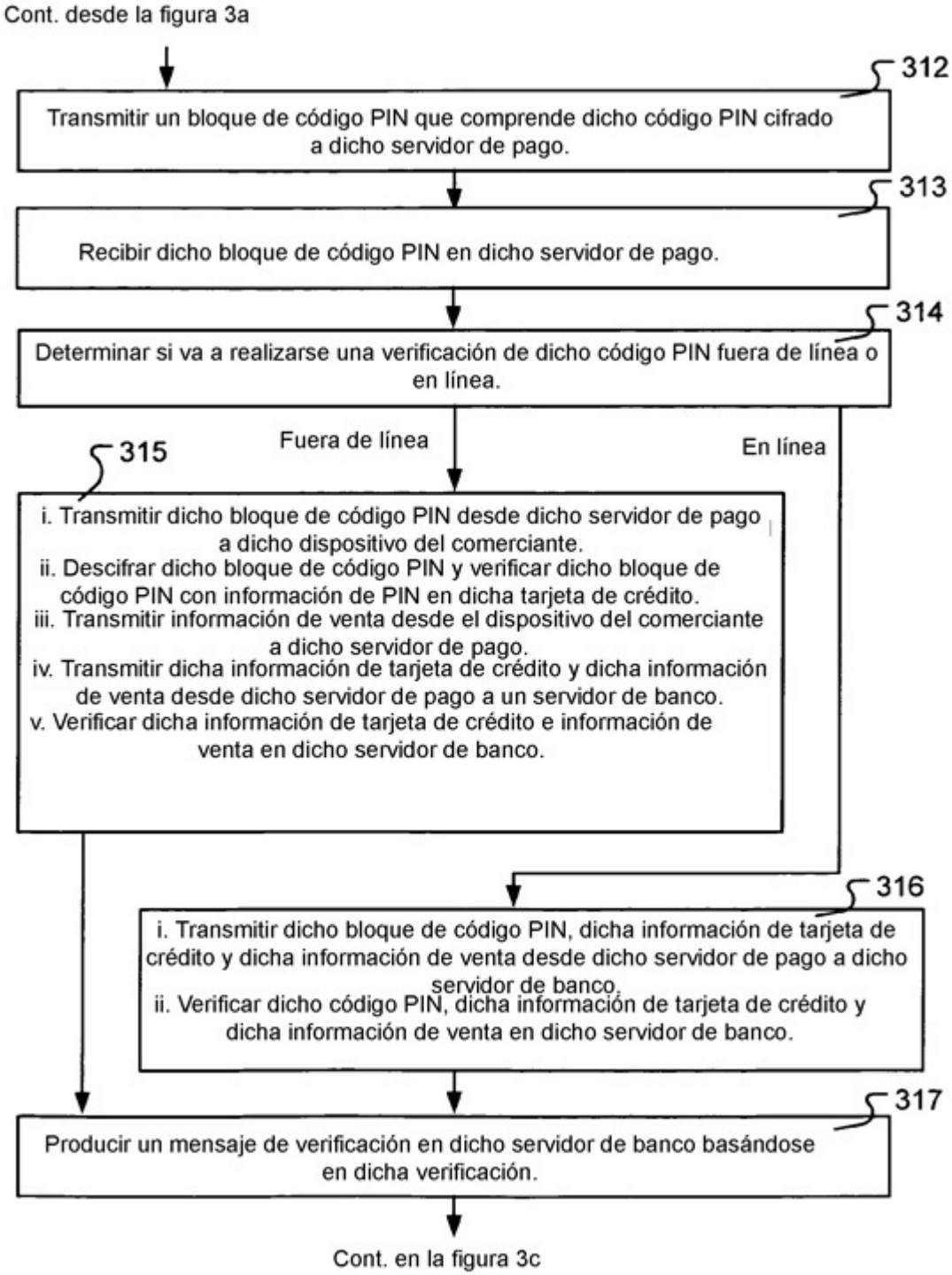

Cont. desde la figura 3a
312
Transmitir un bloque de código PIN que comprende dicho código PIN cifrado a dicho servidor de pago.
313
Recibir dicho bloque de código PIN en dicho servidor de pago.
314
Determinar si va a realizarse una verificación de dicho código PIN fuera de línea o en línea.
Fuera de línea
En línea
315
i. Transmitir dicho bloque de código PIN desde dicho servidor de pago a dicho dispositivo del comerciante.
ii. Descifrar dicho bloque de código PIN y verificar dicho bloque de código PIN con información de PIN en dicha tarjeta de crédito.
iii. Transmitir información de venta desde el dispositivo del comerciante a dicho servidor de pago.
iv. Transmitir dicha información de tarjeta de crédito y dicha información de venta desde dicho servidor de pago a un servidor de banco.
v. Verificar dicha información de tarjeta de crédito e información de venta en dicho servidor de banco.
316
i. Transmitir dicho bloque de código PIN, dicha información de tarjeta de crédito y dicha información de venta desde dicho servidor de pago a dicho servidor de banco.
ii. Verificar dicho código PIN, dicha información de tarjeta de crédito y dicha información de venta en dicho servidor de banco.
317
Producir un mensaje de verificación en dicho servidor de banco basándose en dicha verificación.
Cont. en la figura 3c

Fig. 3b

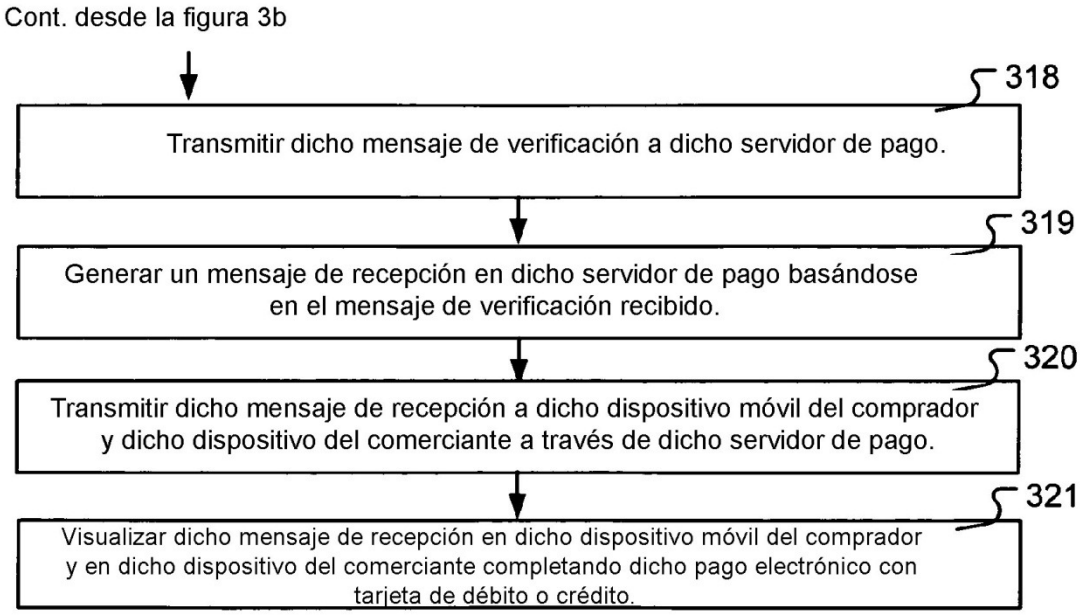

Cont. desde la figura 3b
318
Transmitir dicho mensaje de verificación a dicho servidor de pago.
319
Generar un mensaje de recepción en dicho servidor de pago basándose en el mensaje de verificación recibido.
320
Transmitir dicho mensaje de recepción a dicho dispositivo móvil del comprador y dicho dispositivo del comerciante a través de dicho servidor de pago.
321
Visualizar dicho mensaje de recepción en dicho dispositivo móvil del comprador y en dicho dispositivo del comerciante completando dicho pago electrónico con tarjeta de débito o crédito.

Fig. 3c