(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 969 381**

(51) Int. CI.:

G06Q 20/32 (2012.01)
G06Q 20/34 (2012.01)
G06Q 20/12 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.01.2020 PCT/US2020/015546**

(87) Fecha y número de publicación internacional: **06.08.2020 WO20160069**

(96) Fecha de presentación y número de la solicitud europea: **29.01.2020 E 20708841 (0)**

(97) Fecha y número de publicación de la concesión europea: **17.01.2024 EP 3918556**

(54) Título: **Pago con un solo toque mediante una tarjeta sin contacto**

(30) Prioridad:

01.02.2019 US 201916265974

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.05.2024

(73) Titular/es:

CAPITAL ONE SERVICES, LLC (100.0%)
1680 Capital One Drive
McLean, Virginia 22102, US

(72) Inventor/es:

RULE, JEFFREY;
MORETON, PAUL;
CODY, LEA;
HART, COLIN y
LUTZ, WAYNE

(74) Agente/Representante:

ELZABURU, S.L.P

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

DESCRIPCIÓN

Pago con un solo toque mediante una tarjeta sin contacto

Campo técnico

Las realizaciones de la presente memoria se refieren en general a plataformas informáticas y, más específicamente, a tocar una tarjeta sin contacto en un dispositivo informático para realizar un pago con un solo toque.

Antecedentes

Los usuarios a menudo completan transacciones utilizando plataformas de software en línea. Convencionalmente, los usuarios deben introducir manualmente toda la información de pago relevante en la plataforma de software en línea para completar una transacción. Sin embargo, los usuarios a menudo cometen errores al introducir su información de pago. Además, la transmisión de información de pago a través de un dispositivo de usuario puede plantear riesgos de seguridad.

El documento US2012/031969A1 describe la integración de tokens de verificación con dispositivos de comunicación móviles.

El documento US2014/074637A1 describe aparatos, procedimientos y sistemas NFC de cartera virtual basados en la nube.

El documento US2018/232722A1 describe procedimientos y sistemas de transacciones basados en la nube.

El documento WO2012/154915A1 describe sistemas, dispositivos y procedimientos para la aceptación de pagos móviles, autorizaciones móviles, carteras móviles y mecanismos de comunicación sin contacto.

Compendio

Las realizaciones divulgadas en la presente memoria proporcionan sistemas y procedimientos para tocar una tarjeta sin contacto en un dispositivo informático para realizar el pago con un solo toque.

Según un primer aspecto de la presente invención, se proporciona un procedimiento según la reivindicación 1.

Según un segundo aspecto de la presente invención, se proporciona un aparato según la reivindicación 11.

Según un tercer aspecto de la presente invención, se proporciona un almacenamiento legible por máquina según la reivindicación 12.

Breve descripción de los dibujos

Las figuras 1A-1C ilustran realizaciones de un sistema para tocar una tarjeta sin contacto en un dispositivo informático para realizar el pago con un solo toque.

Las figuras 2A-2D ilustran realizaciones de toque de una tarjeta sin contacto en un dispositivo informático para realizar el pago con un solo toque.

La figura 3 ilustra una realización de un primer flujo lógico.

La figura 4 ilustra una realización de un segundo flujo lógico.

La figura 5 ilustra una realización de un tercer flujo lógico.

La figura 6 ilustra una realización de un cuarto flujo lógico.

La figura 7 ilustra una realización de una arquitectura informática.

Descripción detallada

Las realizaciones descritas en la presente memoria proporcionan técnicas seguras para usar una tarjeta sin contacto para realizar el pago con un solo toque. Por ejemplo, cuando se utiliza una aplicación de comerciante que se ejecuta en un dispositivo informático, un usuario puede seleccionar uno o más artículos para comprar. A continuación, el usuario toca su tarjeta sin contacto en el dispositivo informático, lo que hace que la tarjeta sin contacto entre dentro del alcance de comunicación del dispositivo informático. Al hacerlo, la tarjeta sin contacto genera datos cifrados que se transmiten al dispositivo informático.

La aplicación de comerciante recibe los datos cifrados generados por la tarjeta sin contacto y transmite los datos cifrados a un servidor de autenticación para su validación. La aplicación de comerciante transmite además una indicación de un identificador de comerciante y un identificador de transacción con los datos cifrados. Una vez validados, el servidor de autenticación indica a un servidor de número de cuenta virtual que genere los datos de tarjeta para la cuenta asociada con la tarjeta sin contacto. Los datos de la tarjeta incluyen un número de cuenta virtual, una fecha de caducidad y un valor de verificación de la tarjeta (CVV). Un número de cuenta virtual puede ser un número de cuenta diferente al número de cuenta asociado con la tarjeta sin contacto. Los datos de la tarjeta generados se transmiten luego con el identificador de comerciante y el identificador de transacción a un servidor de comerciante asociado con el comerciante. El servidor de número de cuenta virtual y/o el servidor de autenticación también pueden proporcionar un nombre de usuario, una dirección de facturación del usuario y/o una dirección de envío del usuario al servidor de comerciante. A continuación, el servidor de comerciante puede completar la transacción utilizando los datos recibidos. El servidor de comerciante puede entonces transmitir una confirmación al dispositivo informático que se emite para visualizar la aplicación de comerciante al usuario. Desde el punto de vista del usuario del dispositivo informático, una vez que la tarjeta se toca en el dispositivo informático, la transacción se completa sin necesidad de entrada adicional del usuario, y el usuario recibe un mensaje de confirmación positivo que refleja que la transacción se ha completado.

Ventajosamente, las realizaciones descritas en la presente memoria mejoran la seguridad de todos los dispositivos y datos asociados. Por ejemplo, al transmitir datos de tarjetas entre servidores seguros, se evitan los riesgos asociados con el almacenamiento de datos en un dispositivo de usuario y la transmisión de datos utilizando el dispositivo de usuario. Además, los planteamientos convencionales requieren que el usuario introduzca manualmente los datos de la tarjeta en un formulario. Sin embargo, hacerlo puede permitir que otros usuarios o dispositivos capturen los datos de la tarjeta cuando el usuario introduce los datos de la tarjeta en el formulario. Al eliminar la necesidad de que el usuario introduzca manualmente los datos de la tarjeta, se mejora la seguridad de los datos de la tarjeta. Sin embargo, hacerlo puede permitir que otros usuarios o dispositivos capturen los datos de la tarjeta cuando el usuario introduce los datos de la tarjeta en el formulario. Al eliminar la necesidad de que el usuario introduzca manualmente los datos de la tarjeta en el formulario, se mejora la seguridad de los datos de la tarjeta. Además, la validación realizada por el servidor de autenticación proporciona una protección adicional para asegurar que se introducen los datos correctos de la tarjeta en el formulario. Además, la generación y cumplimentación de los números de tarjetas virtuales en el formulario protege la seguridad del número de cuenta real de la tarjeta sin contacto, ya que las soluciones convencionales requieren proporcionar el número de cuenta real de la tarjeta sin contacto en el formulario.

Con referencia general a las notaciones y nomenclatura utilizadas en la presente memoria, una o más partes de la descripción detallada que sigue pueden presentarse en términos de procedimientos de programa ejecutados en un ordenador o red de ordenadores. Los expertos en la materia utilizan estas descripciones y representaciones de procedimientos para transmitir de la forma más eficaz la sustancia de su trabajo a otros expertos en la materia. Un procedimiento aquí, y en general, se concibe como una secuencia autocoherente de operaciones que conducen a un resultado deseado. Estas operaciones son aquellas que requieren manipulaciones físicas de cantidades físicas. Normalmente, aunque no necesariamente, estas cantidades pueden adoptar la forma de señales eléctricas, magnéticas u ópticas que pueden almacenarse, transferirse, combinarse, compararse y, de alguna manera, manipularse. Se demuestra que es conveniente a veces, principalmente por razones de uso común, referirse a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números o similares. Obsérvese, sin embargo, que todos estos términos y/o similares han de asociarse con las cantidades físicas adecuadas y que son meramente etiquetas convenientes aplicadas a estas cantidades.

Además, a menudo se hace referencia a estas manipulaciones en términos como sumar o comparar, que se asocian habitualmente con operaciones mentales realizadas por un operador humano. Sin embargo, dicha capacidad de un operador humano no es necesaria, ni deseable en la mayoría de los casos, en cualquiera de las operaciones descritas en la presente memoria que forman parte de una o más realizaciones. Más bien, estas operaciones son operaciones de máquina. Las máquinas útiles para realizar operaciones de diversas realizaciones incluyen ordenadores digitales activadas o configuradas de forma selectiva mediante un programa informático almacenado en ellas que está escrito según las enseñanzas de la presente memoria, y/o incluyen aparatos especialmente construidos para el propósito requerido o un ordenador digital. Diversas realizaciones también se refieren a aparatos o sistemas para realizar estas operaciones. Estos aparatos pueden construirse especialmente para el fin requerido. La estructura requerida para una variedad de estas máquinas resultará evidente a partir de la descripción dada.

A continuación, se hace referencia a los dibujos, en los que se utilizan números de referencia parecidos para referirse a elementos parecidos en todas partes. En la siguiente descripción se exponen, con fines explicativos, numerosos detalles específicos para proporcionar una comprensión exhaustiva de los mismos. Sin embargo, puede resultar evidente que las nuevas realizaciones se pueden poner en práctica sin estos detalles específicos. En otros casos se muestran estructuras y dispositivos bien conocidos en forma de diagrama de bloques para facilitar la descripción de los mismos. La intención es cubrir todas las modificaciones, equivalentes y alternativas dentro del alcance de las reivindicaciones.

La figura 1A representa un esquema de un sistema 100 ejemplar, coherente con las realizaciones divulgadas. Como se muestra, el sistema 100 incluye una o más tarjetas 101 sin contacto, uno o más dispositivos 110 móviles, un servidor 120 de autenticación, un servidor 140 de número de cuenta virtual y uno o más servidores 150 de comerciantes. Las tarjetas 101 sin contacto son representativas de cualquier tipo de tarjetas de pago, tales como tarjetas de crédito, tarjetas de débito, tarjetas de cajero automático, tarjetas regalo y similares. Las tarjetas 101 sin contacto pueden comprender una o más interfaces 107 de comunicaciones, tales como un chip de identificación por radiofrecuencia (RFID), configurado para comunicarse con los dispositivos 110 móviles por medio de NFC, el estándar EMV u otros protocolos de corto alcance en comunicación inalámbrica. Aunque el NFC se utiliza como protocolo de comunicaciones de ejemplo, la divulgación es igualmente aplicable a otros tipos de comunicaciones inalámbricas, tal como el estándar EMV, Bluetooth y/o wifi. Los dispositivos 110 móviles son representativos de cualquier tipo de dispositivos informáticos habilitados para la red, tales como teléfonos inteligentes, tabletas informáticas, dispositivos ponibles, ordenadores portátiles, dispositivos de juegos portátiles y similares. Los servidores 120, 140, 150 son representativos de cualquier tipo de dispositivo informático, tal como un servidor, una estación de trabajo, un clúster informático, una plataforma informática en la nube, un sistema informático virtualizado y similares.

Como se muestra, una memoria 111 del dispositivo 110 móvil incluye una instancia de un sistema 112 operativo (OS). Los sistemas 112 operativos de ejemplo incluyen los sistemas operativos Android®, iOS®, Linux® y Windows®. Como se muestra, el OS 112 incluye una o más aplicaciones 113 de comerciante. Las aplicaciones 113 de comerciante son representativas de cualquier tipo de aplicación en la que un usuario pueda proporcionar información de pago para completar una transacción. Por ejemplo, las aplicaciones 113 de comerciante pueden permitir a los usuarios seleccionar y comprar bienes, productos y/o servicios. En una realización, las aplicaciones 113 de comerciante pueden ser aplicaciones basadas en la web a las que se accede mediante un navegador web (no se representa). Por ejemplo, en aplicaciones basadas en la web, el navegador web puede acceder a un sitio web del comerciante y/o aplicaciones web progresivas proporcionadas por el comerciante.

Como se muestra, las aplicaciones 113 de comerciante incluyen un módulo 114 de un solo toque, un identificador 115 de comerciante y un identificador 116 de transacción. Como se describe con más detalle en la presente memoria, el módulo 114 de un solo toque es software, hardware y/o una combinación de software y hardware que permite a los usuarios pagar las transacciones iniciadas en las aplicaciones 113 de comerciante usando un solo toque de la tarjeta 101 sin contacto en el dispositivo 110 móvil. El identificador 115 de comerciante es un identificador único asociado con un comerciante y/o un servidor 150 de comerciante asociado con el comerciante. El identificador 116 de transacción identifica de forma única una transacción determinada. Por ejemplo, el identificador 116 de transacción puede ser un identificador alfanumérico único, un identificador alfanumérico de sesión único, un archivo, etc. El identificador 116 de transacción puede generarse mediante el servidor 150 de comerciante correspondiente y transmitirse a la aplicación 113 de comerciante y/o generarse mediante la aplicación 113 de comerciante y transmitirse al servidor 150 de comerciante correspondiente.

En general, un usuario puede usar la aplicación 113 de comerciante (y/o un sitio web de comerciante en realizaciones donde la aplicación 113 es un navegador web) para seleccionar uno o más artículos y/o servicios para comprar. Cuando el usuario ha seleccionado los artículos y/o servicios deseados, el usuario puede encontrar una interfaz para completar la transacción (p. ej., una página de carrito, una página de proceso de compra, etc.) en la aplicación 113 de comerciante. Convencionalmente, se requiere que el usuario introduzca manualmente su nombre, número de tarjeta, fecha de caducidad, CVV y/o información de dirección en la aplicación 113 de comerciante para completar la compra. Además, las soluciones convencionales pueden requerir que el usuario inicie sesión en su cuenta en la aplicación 113 de comerciante (p. ej., utilizando un nombre de usuario/contraseña, credenciales biométricas, etc.). Ventajosamente, sin embargo, el módulo 114 de un solo toque facilita el proceso de compra (p. ej., pago) con un solo toque usando la tarjeta 101 sin contacto, independientemente de si el usuario ha iniciado sesión en su cuenta en la aplicación 113 de comerciante. En general, el módulo 114 de un solo toque emite una notificación en la interfaz para completar la transacción. La notificación da instrucciones al usuario para tocar la tarjeta 101 sin contacto en el dispositivo 110 móvil, por lo que lleva la tarjeta 101 sin contacto lo suficientemente cerca del lector 119 de tarjetas del dispositivo 110 móvil para permitir la transferencia de datos (p. ej., transferencia de datos NFC, transferencia de datos Bluetooth, etc.) entre la interfaz 107 de comunicaciones de la tarjeta 101 sin contacto y el lector 119 de tarjetas del dispositivo 110 móvil. En algunas realizaciones, el dispositivo 110 móvil puede activar el lector 119 de tarjetas por medio de una llamada de interfaz de programa de aplicación (API). En un ejemplo, el dispositivo 110 móvil activa el lector de tarjetas por medio de una llamada API en respuesta a que el usuario toque o seleccione de otro modo un elemento de la interfaz de usuario, tal como un campo de formulario. De forma adicional o alternativa, el dispositivo 110 móvil puede activar el lector 119 de tarjetas basándose en un sondeo periódico del lector 119 de tarjetas. De manera más general, el dispositivo 110 móvil puede activar el lector 119 de tarjetas para participar en las comunicaciones utilizando cualquier procedimiento factible.

Después de que se ha establecido la comunicación entre el dispositivo 110 móvil y la tarjeta 101 sin contacto, el subprograma 103 que se ejecuta en un procesador (no se representa) de la tarjeta 101 sin contacto genera y transmite datos 106 cifrados al dispositivo 110 móvil por medio de la interfaz 107 de comunicaciones. Por ejemplo, el subprograma 103 de la tarjeta 101 sin contacto utiliza un algoritmo criptográfico para generar una carga útil criptográfica de datos 106 cifrados basándose por lo menos en parte en la clave 104 privada almacenada en la memoria 102 de la tarjeta 101 sin contacto. La clave 104 privada y otros datos (p. ej., el identificador 105 de cliente, un identificador de cuenta, etc.) se proporcionan como entrada al algoritmo criptográfico, que emite los datos 106

cifrados. En general, el subprograma 103 puede usar cualquier tipo de algoritmo y/o sistema criptográfico para generar los datos 106 cifrados, y el uso de un algoritmo criptográfico específico como ejemplo en la presente memoria no debe considerarse limitativo de la divulgación. En algunas realizaciones, el subprograma 103 puede realizar cifrado utilizando una técnica de diversificación de claves para generar los datos 106 cifrados. En la solicitud de patente estadounidense 16/205.119, presentada el 29 de noviembre de 2018, se describen ejemplos de técnicas de diversificación de claves.

Una vez generado, el subprograma 103 transmite los datos 106 cifrados al módulo 114 de un solo toque del dispositivo 110 móvil, p. ej., por medio de NFC. En algunos ejemplos que no forman parte de la invención según se reivindica, el módulo 114 de un solo toque puede requerir que el usuario inicie sesión en su cuenta en los datos 124 de cuenta asociados con la tarjeta 101 sin contacto (p. ej., proporcionar un nombre de usuario/contraseña y/o credenciales biométricas). El módulo 114 de un solo toque transmite los datos 106 cifrados, el identificador 115 de comerciante y el identificador 116 de transacción a la aplicación 123 de autenticación del servidor 120 de autenticación. El módulo 114 de un solo toque transmite datos adicionales que describen el dispositivo 110 móvil: una huella digital del software del dispositivo 110 móvil y datos de ubicación (p. ej., sistema de posicionamiento global (GPS)) del dispositivo 110 móvil. Los datos adicionales que describen el dispositivo móvil transmitidos por el módulo 114 de un solo toque pueden incluir además un identificador único del dispositivo 110 móvil, etc.

Una vez recibidos, la aplicación 123 de autenticación autentica los datos 106 cifrados. La aplicación 123 de autenticación intenta descifrar los datos 106 cifrados usando una copia de la clave 104 privada almacenada en la memoria 122 del servidor 120 de autenticación. La clave 104 privada puede ser idéntica a la clave 104 privada almacenada en la memoria 102 de la tarjeta 101 sin contacto, donde cada tarjeta 101 sin contacto se fabrica para incluir una clave 104 privada única (y el servidor 120 de autenticación almacena una copia correspondiente de cada clave 104 privada única). Por lo tanto, la aplicación 123 de autenticación puede descifrar satisfactoriamente los datos 106 cifrados, de este modo verifica los datos 106 cifrados. Aunque la clave 104 privada se representa almacenada en la memoria 122, en ejemplos que no se encuentran dentro del alcance de la invención según se reivindica, la clave 104 privada puede almacenarse en otro lugar, tal como en un elemento seguro y/o un módulo de seguridad de hardware. (HSM). En dichos ejemplos, el elemento seguro y/o el HSM pueden descifrar los datos 106 cifrados usando la clave 104 privada y una función criptográfica.

Por ejemplo, como se ha indicado, el identificador 105 de cliente puede usarse para generar los datos 106 cifrados. En dicho ejemplo, la aplicación 123 de autenticación descifra los datos 106 cifrados usando la clave 104 privada del servidor 120 de autenticación. Si el resultado del descifrado produce el identificador 105 de cliente asociado con la cuenta en los datos 124 de cuenta, la aplicación 123 de autenticación verifica los datos 106 cifrados y da instrucciones al generador 142 de VAN para generar datos de tarjeta virtual para la cuenta asociada con la tarjeta 101 sin contacto. Si la aplicación 123 de autenticación no puede descifrar los datos cifrados para producir el resultado previsto (p. ej., el identificador 105 de cliente de la cuenta asociada con la tarjeta 101 sin contacto), la aplicación 123 de autenticación no valida los datos 106 cifrados. A causa de la verificación fallida, la aplicación 123 de autenticación no da instrucciones al generador 142 de VAN para generar datos de tarjeta virtual para mantener la seguridad de la cuenta asociada.

La aplicación 123 de autenticación procesa los datos adicionales recibidos desde el dispositivo 110 móvil como condición para dar instrucciones al generador 142 de VAN para generar los datos de la tarjeta virtual. El usuario no inicia sesión en la cuenta de comerciante y/o en la cuenta en los datos 124 de cuenta. Por ejemplo, la aplicación 123 de autenticación puede determinar si el identificador de dispositivo del dispositivo 110 móvil se especifica como un identificador de dispositivo conocido para la cuenta asociada en los datos 124 de cuenta. Si el identificador de dispositivo no es un identificador conocido, la aplicación 123 de autenticación puede abstenerse de dar instrucciones al generador 142 de VAN para generar los datos de la tarjeta virtual. De lo contrario, la aplicación 123 de autenticación puede dar instrucciones al generador 142 de VAN para generar los datos de la tarjeta virtual. La aplicación 123 de autenticación determina si la huella digital del software coincide con una huella digital del software conocida para la cuenta asociada en los datos 124 de cuenta. Si la huella digital del software no es una huella digital del software conocida, la aplicación 123 de autenticación se abstiene de dar instrucciones al generador 142 de VAN para generar los datos de la tarjeta virtual.

De lo contrario, la aplicación 123 de autenticación da instrucciones al generador 142 de VAN para generar los datos de la tarjeta virtual. La aplicación 123 de autenticación determina si las coordenadas GPS indican que el usuario está en casa, en el trabajo o en alguna otra dirección conocida asociada con la cuenta en los datos 124 de cuenta. Si la ubicación del dispositivo no está dentro de una distancia umbral de la dirección conocida, la aplicación 123 de autenticación se abstiene de dar instrucciones al generador 142 de VAN para generar los datos de la tarjeta virtual. De lo contrario, la aplicación 123 de autenticación da instrucciones al generador 142 de VAN para generar los datos de la tarjeta virtual. Más aún, la aplicación 123 de autenticación determina si el usuario ha realizado compras previamente con el comerciante asociado con el identificador 115 de comerciante recibido. Si el usuario no ha realizado una compra previa con el comerciante, la aplicación 123 de autenticación se abstiene de dar instrucciones al generador 142 de VAN para generar los datos de la tarjeta virtual. De lo contrario, la aplicación 123 de autenticación da instrucciones al generador 142 de VAN para generar los datos de la tarjeta virtual.

La figura 1B representa que la aplicación 123 de autenticación valida los datos 106 cifrados y da instrucciones al generador 142 de número de cuenta virtual (VAN) en la memoria 141 del servidor 140 de número de cuenta virtual para generar los datos 126 de tarjeta virtual que comprenden un número de cuenta virtual, la fecha de caducidad y el CVV para la cuenta asociada con la tarjeta 101 sin contacto. El generador 142 de VAN genera el número de cuenta virtual, la fecha de caducidad y el CVV. En otros ejemplos que no entran dentro del alcance de la invención según se reivindica, el generador 142 de VAN genera el número de cuenta virtual y selecciona una fecha de caducidad y/o CVV existente (p. ej., a partir de los datos 124 de cuenta). En un ejemplo que no se encuentra dentro del alcance de la invención según se reivindica, la fecha de caducidad y/o el CVV existente puede ser la fecha de caducidad y/o el CVV de la tarjeta 101 sin contacto, u otra tarjeta asociada con la cuenta en los datos 124 de cuenta. El generador 142 de VAN puede recibir además el nombre del titular de la cuenta y una o más direcciones conocidas (p. ej., una dirección de facturación, dirección de envío, etc.) de la cuenta en los datos 124 de cuenta asociados con la tarjeta 101 sin contacto. En por lo menos una realización, los datos 126 de la tarjeta, incluido el número de cuenta virtual generado por el generador 142 de VAN, están restringidos al comerciante asociado con el identificador 115 de comerciante. El número de cuenta virtual y/o los datos 126 de la tarjeta pueden incluir además otras restricciones (p. ej., restricciones de tiempo , restricciones de cantidad, etc.). Una vez generado, el generador 142 de VAN transmite los datos 126 de la tarjeta virtual, el identificador 115 de comerciante y el identificador 116 de transacción al servidor 150 de comerciante. El generador 142 de VAN y/o el servidor 120 de autenticación pueden transmitir además el nombre del titular de la cuenta, la dirección de facturación y la dirección de envío al servidor 150 de comerciante. En una realización, el generador 142 de VAN determina una ubicación del servidor 150 de comerciante basándose en el identificador 115 de comerciante (p. ej., en una tabla de consulta que asocia identificadores 115 de comerciante con un servidor 150 de comerciante correspondiente).

La figura 1C representa que el servidor 150 de comerciante recibe los datos 126 de la tarjeta virtual, el identificador 115 de comerciante, el identificador 116 de transacción y cualquier otro dato (p. ej., el nombre y las direcciones del titular de la cuenta) desde el generador 142 de VAN y/o el servidor 120 de autenticación. En general, el servidor 150 de comerciante procesa la transacción utilizando los datos recibidos del generador 142 de VAN y/o el servidor 120 de autenticación. Más específicamente, el servidor 150 de comerciante puede generar un registro 152 de transacción en la base de datos 151 de transacciones utilizando el número de cuenta virtual, la fecha de caducidad, el CVV, el nombre y/o las direcciones recibidas. El registro 152 de transacción en la base de datos 151 de transacciones puede especificar además el identificador 116 de transacción. Al hacerlo, se utilizan los datos 126 de la tarjeta virtual para pagar la transacción sin requerir que el usuario introduzca ninguna información de pago usando la aplicación 113 de comerciante que se ejecuta en el dispositivo 110 móvil. En cambio, la transacción se paga y se procesa utilizando los datos 126 de la tarjeta virtual generados y transmitidos de forma segura.

Como se muestra, el servidor 150 de comerciante puede generar una confirmación 153 que indica que se ha recibido el pago de la transacción y que la transacción se ha procesado. El servidor 150 de comerciante puede transmitir la confirmación 153 a la aplicación 113 de comerciante, que puede emitir la confirmación 153 en un visualizador del dispositivo 110 móvil. En otras realizaciones, la confirmación 153 puede ser una confirmación por correo electrónico, confirmación por mensaje de texto, notificación push, etc. Al hacerlo, se informa al usuario que la transacción se ha completado y puede incluir información adicional sobre la entrega de artículos, prestación de servicios, etc.

La figura 2A es un esquema 200 que representa una realización de ejemplo de toque de la tarjeta 101 sin contacto para realizar el pago con un solo toque. Como se muestra, la aplicación 113 de comerciante que se ejecuta en el dispositivo 110 móvil muestra una interfaz gráfica de usuario (GUI) para completar una compra. Por ejemplo, la GUI puede ser una página de carrito de la compra, una página de proceso de compra o cualquier otra página de la aplicación 113 de comerciante. Como se muestra, una notificación 201 da instrucciones a un usuario para tocar la tarjeta 101 sin contacto en el dispositivo 110 móvil para pagar los artículos de su carrito de la compra usando el pago con un solo toque. Una vez que se detecta el toque, como se muestra en el esquema 210 de la figura 2B, la aplicación 113 de comerciante puede emitir una notificación 202 que indica que se está generando un número virtual seguro.

Como se ha indicado, una vez que el usuario toca la tarjeta 101 sin contacto al dispositivo 110 móvil, la tarjeta 101 sin contacto genera los datos 106 cifrados y transmite los datos 106 cifrados al dispositivo 110 móvil. Una vez recibido, el módulo 114 de un solo toque transmite los datos 106 cifrados, el ID 115 del comerciante y el ID 116 de transacción al servidor 120 de autenticación. A continuación, la aplicación 123 de autenticación verifica los datos 106 cifrados descifrando los datos 106 cifrados con la clave 104 privada almacenada en la memoria 122 del servidor 120. Una vez verificada, la aplicación 123 de autenticación indica al generador 142 de VAN que genere los datos 126 de la tarjeta virtual (es decir, un número de tarjeta virtual, la fecha de caducidad y el CVV). Como se ha indicado, en algunos ejemplos que no entran dentro del alcance de la invención reivindicada, el generador 142 de VAN puede generar el número de la tarjeta virtual y recuperar la fecha de caducidad y/o CVV de los datos 124 de cuenta. El generador 142 de VAN también puede recibir el ID 115 del comerciante, el ID 116 de transacción y datos adicionales que describen al usuario (p. ej., nombres, dirección de facturación, dirección de envío, etc.) a partir de los datos 124 de cuenta. A continuación, el generador 142 de VAN transmite los datos 126 de la tarjeta virtual, el ID 115 del comerciante, el ID 116 de transacción y cualquier nombre de usuario y/o dirección al servidor 150 de comerciante. El servidor 150 de comerciante procesa la transacción usando los datos recibidos del generador 142 de VAN, p. ej., generando un registro 152 de transacción en la base de datos 151 de transacciones usando por lo menos el número de la tarjeta virtual recibido, la fecha de caducidad, el CVV. El registro 152 de transacción puede incluir además el nombre de usuario, la dirección de facturación, la dirección de envío y una indicación de cada artículo y/o servicio adquirido. El servidor 150

de comerciante puede entonces transmitir una confirmación de pedido al dispositivo 110 móvil. La figura 2D es un esquema 230 que representa un ejemplo de confirmación enviada por la aplicación 113 de comerciante en el dispositivo 110 móvil.

En algunas realizaciones, el servidor 150 de comerciante puede requerir la resolución de conflictos de datos antes de procesar la transacción utilizando los datos recibidos del generador 142 de VAN. Por ejemplo, los datos 124 de cuenta pueden especificar una dirección de facturación de "123 Main St." para la cuenta del usuario, mientras que el perfil del usuario en el servidor 150 de comerciante puede especificar "300 Bowles Dr." como la dirección de facturación de la cuenta del usuario. Por lo tanto, como se representa en el esquema 220 de la figura 2C, el servidor 150 de comerciante puede hacer que la aplicación 113 de comerciante envíe la notificación 203 en el dispositivo 110 móvil. Como se muestra, la notificación 203 permite al usuario seleccionar una de las dos direcciones diferentes. Una vez seleccionada, la aplicación 113 de comerciante transmite una indicación de la dirección seleccionada al servidor 150 de comerciante. El servidor 150 de comerciante puede entonces procesar la transacción utilizando la dirección seleccionada. Aunque se utiliza una dirección como ejemplo, el servidor 150 de comerciante y/o la aplicación 113 de comerciante pueden resolver de forma similar conflictos de datos para otros tipos de datos (p. ej., nombres, direcciones de envío, etc.).

La figura 3 ilustra un flujo 300 lógico. El flujo 300 lógico puede ser representativo de algunas o todas las operaciones ejecutadas por una o más realizaciones descritas en la presente memoria. Por ejemplo, el flujo 300 lógico puede incluir algunas o todas las operaciones para usar una tarjeta sin contacto para realizar un pago con un solo toque. Las realizaciones no están limitadas en este contexto.

Como se muestra, el flujo 300 lógico comienza en el bloque 305, donde un usuario proporciona opcionalmente credenciales de autenticación para autenticar una cuenta de usuario en la aplicación 113 de comerciante, donde la aplicación 113 de comerciante incluye el módulo 114 de un solo toque para admitir el proceso de compra con un solo toque como se describe en la presente memoria. Sin embargo, el bloque 305 se encuentra fuera del alcance de la invención según se reivindica, según el cual el usuario no se autentica en su cuenta con la aplicación 113 de comerciante. En el bloque 310, el usuario puede seleccionar uno o más artículos y/o servicios para comprar como parte de una transacción. Por ejemplo, el usuario puede especificar solicitar un servicio de automóvil que lo lleve desde su casa al aeropuerto. Para mencionar otro ejemplo, el usuario puede especificar pedir alimentos para que se entreguen en su oficina. Como se ha indicado, la aplicación 113 del comerciante está asociada con un ID 115 del comerciante único. De forma similar, los artículos y/o servicios seleccionados por el usuario están asociados con un ID 116 de transacción. A medida que el usuario selecciona y/o elimina artículos y/o servicios de su carrito de la compra, la aplicación 113 de comerciante puede transmitir una indicación del ID 116 de transacción y los artículos seleccionados y/o eliminados al servidor 150 de comerciante, de este modo el servidor 150 de comerciante puede saber qué artículos y/o servicios están asociados con un ID 116 de transacción determinada. En el bloque 315, el módulo 114 de un solo toque de la aplicación 113 de comerciante emite una notificación que especifica que debe tocar una tarjeta 101 sin contacto en el dispositivo 110 móvil. En una realización, el módulo 114 de un solo toque emite la notificación tras determinar que la aplicación 113 de comerciante emite un elemento (p. ej., un formulario, un campo de formulario, etc.) que está asociado con completar una transacción y/o pagar una transacción.

En el bloque 320, un usuario toca la tarjeta 101 sin contacto al dispositivo 110 móvil para hacer que la tarjeta 101 sin contacto genere y transmita datos 106 cifrados. El subprograma 103 de la tarjeta 101 sin contacto genera entonces los datos 106 cifrados utilizando la clave 104 privada, los datos de entrada (p. ej., el identificador 105 de cliente) y un algoritmo criptográfico. El subprograma 103 transmite entonces los datos 106 cifrados al dispositivo 110 móvil. En el bloque 325, el módulo 114 de un solo toque y/o la aplicación 113 de comerciante reciben los datos 106 cifrados desde la interfaz 107 de comunicaciones de la tarjeta sin contacto. En el bloque 330, el módulo 114 de un solo toque y/o la aplicación 113 de comerciante transmite los datos 106 cifrados, el identificador 115 de comerciante y el identificador 116 de transacción al servidor 120 de autenticación.

En el bloque 335, la aplicación 123 de autenticación descifra los datos 106 cifrados usando la clave 104 privada en la memoria 122 del servidor 120 de autenticación para validar los datos 106 cifrados. En el bloque 340, la aplicación 123 de autenticación transmite una indicación al generador 142 de VAN que especifica que debe generar datos de tarjeta que comprenden un número de cuenta virtual, la fecha de caducidad y el CVV. La aplicación 123 de autenticación puede transmitir además el identificador 115 de comerciante y/o el identificador 116 de transacción al generador 142 de VAN. En el bloque 345, el generador 142 de VAN genera el número de cuenta virtual, la fecha de caducidad y el CVV. En el bloque 350, el generador 142 de VAN transmite el número de cuenta virtual, la fecha de caducidad, el CVV, el ID 115 del comerciante y el ID 116 de transacción al servidor 150 de comerciante. El generador 142 de VAN puede incluir además el nombre, la dirección de facturación y la dirección de envío del titular de la cuenta, que pueden almacenarse localmente por el generador 142 de VAN y/o recibirse desde el servidor 120 de autenticación.

En el bloque 355, el servidor 150 de comerciante procesa la transacción asociada con el ID 116 de transacción usando los datos recibidos del generador 142 de VAN. Más específicamente, el servidor 150 de comerciante procesa el pago de la transacción utilizando por lo menos el número de la tarjeta virtual, la fecha de caducidad y el CVV generado por el generador 142 de VAN. Como se ha indicado, el servidor 150 de comerciante puede procesar el pago de la transacción generando un registro 152 de transacción en la base de datos 151 de transacciones utilizando por lo menos el número de la tarjeta virtual recibido, la fecha de caducidad y el CVV. El registro 152 de transacción puede

incluir además el nombre de usuario, la dirección de facturación, la dirección de envío y una indicación de cada artículo y/o servicio asociado con el ID 116 de transacción. En el bloque 360, el servidor 150 de comerciante puede transmitir una confirmación de pago a la aplicación 113 de comerciante en el dispositivo móvil. La confirmación en general puede indicar que el pago se ha procesado utilizando los datos de la tarjeta virtual generados por el generador VAN.

La figura 4 ilustra una realización de un flujo 400 lógico. El flujo 400 lógico puede ser representativo de algunas o todas las operaciones ejecutadas por una o más realizaciones descritas en la presente memoria. Por ejemplo, el flujo 400 lógico puede incluir algunas o todas las operaciones realizadas para autorizar un pago con un solo toque usando la tarjeta 101 sin contacto. Las realizaciones no están limitadas en este contexto.

Como se muestra, el flujo 400 lógico comienza en el bloque 405, donde el módulo 114 de un solo toque y/o la aplicación 113 de comerciante transmite los datos 106 cifrados generados por la tarjeta 101 sin contacto, el ID 115 del comerciante, el ID 116 de transacción y un identificador de dispositivo al servidor 120 de autenticación. Como se ha indicado, el identificador de dispositivo puede ser una huella digital del software del dispositivo 110 móvil, un identificador único del dispositivo 110 móvil (p. ej., una dirección de control de acceso al medio (MAC)) y similares. En el bloque 410, la aplicación 123 de autenticación puede determinar que el identificador de dispositivo recibido no está asociado con la cuenta de la tarjeta 101 sin contacto. Por ejemplo, los datos 124 de cuenta pueden incluir identificadores de dispositivos conocidos para una cuenta determinada. Si el identificador de dispositivo recibido no se especifica como un identificador de dispositivo conocido en los datos 124 de cuenta, la aplicación 123 de autenticación puede requerir información adicional para mantener la seguridad de la cuenta. Como tal, la aplicación 123 de autenticación puede dar instrucciones al módulo 114 de un solo toque que emita una indicación para recibir credenciales de autenticación para la cuenta en los datos 124 de cuenta. Por ejemplo, el módulo 114 de un solo toque puede emitir una notificación que especifique que el usuario proporciona su huella digital como entrada biométrica para autenticarse en su cuenta asociada con la cuenta en los datos 124 de cuenta. Para mencionar otro ejemplo, el módulo 114 de un solo toque puede emitir una notificación que especifica que el usuario proporciona el inicio de sesión y la contraseña asociados con la cuenta en los datos 124 de cuenta. En otras realizaciones, el usuario puede iniciar sesión en la cuenta utilizando FaceID, otros identificadores biométricos o cualquier otro tipo de credencial.

En el bloque 415, el usuario proporciona las credenciales (p. ej., entrada biométrica, inicio de sesión/contraseña, etc.) para la cuenta en los datos 124 de cuenta al módulo 114 de un solo toque y/o a la aplicación 113 de comerciante. El módulo 114 de un solo toque puede incluir lógica para verificar las credenciales recibidas. En otras realizaciones, el módulo 114 de un solo toque puede transmitir las credenciales recibidas al servidor 120 de autenticación. En el bloque 420, la aplicación 123 de autenticación autentica las credenciales de cuenta recibidas y los datos 106 cifrados generados por la tarjeta 101 sin contacto. La aplicación 123 de autenticación puede determinar si las credenciales de cuenta recibidas coinciden con las credenciales de la cuenta almacenada en los datos 124 de cuenta y descifrar los datos 106 cifrados usando la clave 104 privada. En el bloque 425, el servidor 120 de autenticación puede determinar dar instrucciones al generador 142 de VAN que genere un número de tarjeta virtual, una fecha de caducidad y un CVV. El servidor 120 de autenticación además puede transmitir, con la instrucción, un nombre, una dirección de facturación y una dirección de envío desde los datos 124 de cuenta al generador 142 de VAN.

La figura 5 ilustra una realización de un flujo 500 lógico. El flujo 500 lógico puede ser representativo de algunas o todas las operaciones ejecutadas por una o más realizaciones descritas en la presente memoria. Por ejemplo, el flujo 500 lógico puede incluir algunas o todas las operaciones para proporcionar el pago de transacciones con un solo toque utilizando una tarjeta sin contacto. Las realizaciones no están limitadas en este contexto.

Como se muestra, el flujo 500 lógico comienza en el bloque 505, donde el servidor 150 de comerciante genera un identificador 116 de transacción para una transacción. Como se ha indicado, el identificador 116 de transacción puede ser cualquier tipo de identificador, tal como un identificador alfanumérico único, un identificador alfanumérico de sesión único, un archivo, etc. En el bloque 510, la aplicación 113 de comerciante recibe el identificador 116 de transacción del servidor 150 de comerciante por medio de la red 130. La aplicación 113 de comerciante y/o el módulo 114 de un solo toque transmiten el identificador 116 de transacción recibido con los datos 106 cifrados al servidor 120 de autenticación. En el bloque 515, la aplicación 113 de comerciante transmite indicaciones de artículos y/o servicios añadidos y/o eliminados del carrito de la compra del usuario para la transacción asociada con el identificador 116 de transacción. En el bloque 520, el servidor 150 de comerciante recibe los datos 126 de la tarjeta virtual, la información del usuario y el identificador 116 de transacción del generador 142 de VAN. En el bloque 525, el servidor de comerciante procesa el pago de la transacción asociada con el identificador 116 de transacción generando un registro de transacción en la base de datos 151 de transacciones.

La figura 6 ilustra una realización de un flujo 600 lógico. El flujo 600 lógico puede ser representativo de algunas o todas las operaciones ejecutadas por una o más realizaciones descritas en la presente memoria. Por ejemplo, el flujo 600 lógico puede incluir algunas o todas las operaciones realizadas por la aplicación 113 de comerciante y/o el servidor 150 de comerciante. Las realizaciones no están limitadas en este contexto.

Como se muestra, el flujo 600 lógico comienza en el bloque 605, donde el servidor 150 de comerciante recibe los datos 126 de la tarjeta virtual (p. ej., número de cuenta virtual, fecha de caducidad y CVV), datos del titular de la cuenta (p. ej., nombre, dirección de facturación, dirección de envío, etc.), y el ID 116 de transacción del generador 142 de VAN. En el bloque 610, el servidor 150 de comerciante determina que por lo menos un elemento de los datos recibidos

no es por lo menos como un elemento de los datos de usuario en un perfil de usuario asociado con el comerciante. Por ejemplo, es posible que las direcciones de correo y/o facturación recibidas no coincidan con ninguna dirección especificada en el perfil de usuario.

En el bloque 615, el servidor 150 de comerciante da instrucciones a la aplicación 113 de comerciante que emita las indicaciones de los elementos de datos identificados en el bloque 610. Por ejemplo, la aplicación 113 de comerciante puede emitir una lista de direcciones. En el bloque 620, la aplicación 113 de comerciante recibe una selección del usuario de uno de los elementos de datos (p. ej., una primera dirección emitida en el bloque 615). En el bloque 625, la aplicación 113 de comerciante transmite una indicación del elemento de datos seleccionado en el bloque 620 al servidor 150 de comerciante. En el bloque 630, el servidor 150 de comerciante procesa la transacción utilizando los datos recibidos del generador 142 de VAN y el elemento de datos seleccionado por el usuario en el bloque 620. Más específicamente, el servidor 150 de comerciante genera un registro de transacción para la transacción en la base de datos 151 de transacciones.

La figura 7 ilustra una realización de una arquitectura 700 informática ejemplar que comprende un sistema 702 informático que puede ser adecuado para implementar diversas realizaciones como se describen previamente. En diversas realizaciones, la arquitectura 700 informática puede comprender o implementarse como parte de un dispositivo electrónico. En algunas realizaciones, la arquitectura 700 informática puede ser representativa, por ejemplo, de un sistema que implementa uno o más componentes del sistema 100. En algunas realizaciones, el sistema 702 informático puede ser representativo, por ejemplo, de la tarjeta 101 sin contacto, los dispositivos 110 móviles, el servidor 120 de autenticación, el servidor 140 de número de cuenta virtual y/o el servidor 150 de comerciante del sistema 100. Las realizaciones no están limitadas en este contexto. De manera más general, la arquitectura 700 informática está configurada para implementar toda la lógica, aplicaciones, sistemas, procedimientos, aparatos y funcionalidad descritos en la presente memoria con referencia a las figuras 1 a 6.

Tal como se utilizan en la presente solicitud, los términos "sistema" y "componente" y "módulo" pretenden referirse a una entidad relacionada con la informática, ya sea hardware, una combinación de hardware y software, software o software en ejecución, ejemplos de los cuales se proporcionan en la arquitectura 700 informática ejemplar. Por ejemplo, un componente puede ser, pero no se limita a ser, un proceso que se ejecuta en un procesador de ordenador, un procesador de ordenador, una unidad de disco duro, múltiples unidades de almacenamiento (de medio de almacenamiento óptico y/o magnético), un objeto, un ejecutable, un hilo de ejecución, un programa y/o un ordenador. A modo de ilustración, una aplicación que se ejecuta en un servidor, así como el propio servidor, puede ser un componente. Uno o más componentes pueden residir dentro de un proceso y/o hilo de ejecución, y un componente puede estar ubicado en un ordenador y/o estar distribuido entre dos o más ordenadores. Además, los componentes pueden acoplarse de forma comunicativa entre sí mediante diversos tipos de medios de comunicación para coordinar operaciones. La coordinación puede implicar el intercambio de información unidireccional o bidireccional. Por ejemplo, los componentes pueden comunicar información en forma de señales comunicadas a través de los medios de comunicación. La información se puede implementar como señales asignadas a diversas líneas de señales. En dichas asignaciones, cada mensaje es una señal. Sin embargo, otras realizaciones pueden emplear de forma alternativa mensajes de datos. Dichos mensajes de datos pueden enviarse a través de diversas conexiones. Las conexiones ejemplares incluyen interfaces paralelas, interfaces en serie e interfaces de bus.

El sistema 702 informático incluye diversos elementos informáticos habituales, tales como uno o más procesadores, procesadores multinúcleo, coprocesadores, unidades de memoria, conjuntos de chips, controladores, periféricos, interfaces, osciladores, dispositivos de sincronización, tarjetas de vídeo, tarjetas de audio, componentes de entrada/salida (E/S) multimedia, fuentes de alimentación, etc. Las realizaciones, sin embargo, no se limitan a la implementación mediante el sistema 702 informático.

Como se muestra en la figura 7, el sistema 702 informático comprende un procesador 704, una memoria 706 del sistema y un bus 708 del sistema. El procesador 704 puede ser cualquiera de diversos procesadores de ordenador disponibles comercialmente, incluidos, entre otros, procesadores AMD® Athlon®, Duron® y Opteron®; aplicación ARM®, procesadores integrados y seguros; procesadores IBM® y Motorola® DragonBall® y PowerPC®; procesadores IBM y Sony® Cell; procesadores Intel® Celeron®, Core®, Core (2) Duo®, Itanium®, Pentium®, Xeon® y XScale®; y procesadores similares. También se pueden emplear como procesador 704 microprocesadores duales, procesadores multinúcleo y otras arquitecturas multiprocesador.

El bus 708 del sistema proporciona una interfaz para los componentes del sistema que incluyen, entre otros, la memoria 706 del sistema al procesador 704. El bus 708 del sistema puede ser cualquiera de varios tipos de estructura de bus que pueden interconectarse además con un bus de memoria (con o sin un controlador de memoria), un bus periférico y un bus local utilizando cualquiera de una variedad de arquitecturas de bus disponibles comercialmente. Los adaptadores de interfaz pueden conectarse al bus 708 del sistema por medio de una arquitectura de ranuras. Las arquitecturas de ranuras de ejemplo pueden incluir, entre otras, puerto de gráficos acelerados (AGP), bus de tarjeta, arquitectura estándar de la industria (extendida) ((E)ISA), arquitectura de microcanal (MCA), NuBus, interconexión de componentes periféricos (extendida) (PCI(X)), PCI Express, Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales (PCMCIA) y similares.

La memoria 706 del sistema puede incluir diversos tipos de medios de almacenamiento legibles por ordenador en forma de una o más unidades de memoria de mayor velocidad, tales como memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM), RAM dinámica (DRAM), DRAM de doble tasa de datos (DDRAM), DRAM síncrona (SDRAM), RAM estática (SRAM), ROM programable (PROM), ROM programable y borrable (EPROM), ROM programable y borrable eléctricamente (EEPROM), memoria flash (p. ej., una o más matrices flash), memorias poliméricas tales como memorias poliméricas ferroeléctricas, memorias ovónicas, memorias de cambio de fase o ferroeléctricas, memorias de silicio-óxido-nitruro-óxido-silicio (SONOS), tarjetas magnéticas u ópticas, una matriz de dispositivos tales como unidades de matrices redundantes de discos independientes (RAID), dispositivos de memoria de estado sólido (p. ej., memoria USB, unidades de estado sólido (SSD) y cualquier otro tipo de medio de almacenamiento adecuado para almacenar información. En la realización ilustrada que se muestra en la figura 7, la memoria 706 del sistema puede incluir memoria 710 no volátil y/o memoria 712 volátil. Un sistema básico de entrada/salida (BIOS) puede almacenarse en la memoria 710 no volátil.

El sistema 702 informático puede incluir diversos tipos de medios de almacenamiento legibles por ordenador en forma de una o más unidades de memoria de menor velocidad, incluidos una unidad de disco 714 duro (HDD) interna (o externa), una unidad de disquete 716 magnético (FDD) para leer o escribir en un disco 718 magnético extraíble, y una unidad de disco 720 óptico para leer o escribir en un disco 722 óptico extraíble (p. ej., un CD-ROM o DVD). El HDD 714, el FDD 716 y la unidad de disco 720 óptico se pueden conectar al bus 708 del sistema mediante una interfaz 724 HDD, una interfaz 726 FDD y una interfaz 728 de unidad óptica, respectivamente. La interfaz 724 HDD para las implementaciones de unidad externa puede incluir por lo menos una o ambas de las tecnologías de interfaz del bus serie universal (USB) e IEEE 1394. El sistema 702 informático en general está configurado para implementar toda la lógica, sistemas, procedimientos, aparatos y funcionalidades descritos en la presente memoria con referencia a las figuras 1 a 6.

Las unidades y los medios legibles por ordenador asociados proporcionan almacenamiento volátil y/o no volátil de datos, estructuras de datos, instrucciones ejecutables por ordenador, etc. Por ejemplo, se pueden almacenar varios módulos de programa en las unidades de disco y de memoria 710, 712, incluido un sistema 730 operativo, uno o más programas 732 de aplicación, otros módulos 734 de programa y datos 736 de programa. En una realización, el uno o más programas 732 de aplicación, otros módulos 734 de programa y datos 736 de programa pueden incluir, p. ej., las diversas aplicaciones y/o componentes del sistema 100, p. ej., el subprograma 103, claves 104 privadas, datos 106 cifrados, sistema 112 operativo, aplicaciones 113 de comerciante, el módulo 114 de un solo toque, la aplicación 123 de autenticación, el generador 142 de VAN y/o el servidor 150 de comerciante.

Un usuario puede introducir comandos e información en el sistema 702 informático a través de uno o más dispositivos de entrada cableados/inalámbricos, por ejemplo, un teclado 738 y un dispositivo apuntador, tal como un ratón 740. Otros dispositivos de entrada pueden incluir micrófonos, controles remotos de infrarrojos (IR), controles remotos de radiofrecuencia (RF), mandos para juegos, lápices ópticos, lectores de tarjetas, mochilas, lectores de huellas dactilares, guantes, tabletas gráficas, palancas de mandos, teclados, lectores de retina, pantallas táctiles (p. ej., capacitivas, resistivas, etc.), bolas de seguimiento, paneles táctiles, sensores, lápices ópticos y similares. Estos y otros dispositivos de entrada a menudo se conectan al procesador 704 a través de una interfaz 742 del dispositivo de entrada que está acoplada al bus 708 del sistema, pero se pueden conectar mediante otras interfaces tales como un puerto paralelo, un puerto serie IEEE 1394, un puerto de juego, un puerto USB, una interfaz IR, etc.

Un monitor 744 u otro tipo de dispositivo de visualización también está conectado al bus 708 del sistema por medio de una interfaz, tal como un adaptador 746 de vídeo. El monitor 744 puede ser interno o externo al sistema 702 informático. Además del monitor 744, un ordenador típicamente incluye otros dispositivos de salida periféricos, tales como altavoces, impresoras, etc.

El sistema 702 informático puede funcionar en un entorno de red utilizando conexiones lógicas por medio de comunicaciones cableadas y/o inalámbricas a uno o más ordenadores remotos, tales como un ordenador 748 remoto. El ordenador 748 remoto puede ser una estación de trabajo, un ordenador servidor, un enrutador, un ordenador personal, un ordenador portátil, un electrodoméstico de entretenimiento basado en microprocesador, un dispositivo par u otro nodo de red habitual, y típicamente incluye muchos o todos los elementos descritos en relación con el sistema 702 informático, aunque, por motivos de brevedad, solo se ilustra un dispositivo 750 de memoria/almacenamiento. Las conexiones lógicas representadas incluyen conectividad por cable/inalámbrica a una red de área local (LAN) 752 y/o redes más grandes, por ejemplo, una red de área amplia (WAN) 754. Dichos entornos de redes LAN y WAN son comunes en oficinas y empresas, y facilitan redes informáticas en toda la empresa, tales como intranets, todas las cuales pueden conectarse a una red de comunicaciones global, por ejemplo, Internet. En realizaciones, la red 130 de la figura 1 es una o más de la LAN 752 y la WAN 754.

Cuando se utiliza en un entorno de red LAN, el sistema 702 informático se conecta a la LAN 752 a través de una interfaz o adaptador 756 de red de comunicación cableada y/o inalámbrica. El adaptador 756 puede facilitar comunicaciones cableadas y/o inalámbricas con la LAN 752, que también puede incluir un punto de acceso inalámbrico dispuesto en la misma para comunicarse con la funcionalidad inalámbrica del adaptador 756.

Cuando se usa en un entorno de red WAN, el sistema 702 informático puede incluir un módem 758, o está conectado a un servidor de comunicaciones en la WAN 754, o tiene otros medios para establecer comunicaciones a través de la WAN 754, tal como a través de Internet. El módem 758, que puede ser interno o externo y un dispositivo cableado y/o inalámbrico, se conecta al bus 708 del sistema por medio de la interfaz 742 del dispositivo de entrada. En un entorno en red, los módulos de programa representados en relación con el sistema 702 informático, o partes del mismo, pueden almacenarse en el dispositivo 750 de almacenamiento/memoria remoto. Se apreciará que las conexiones de red mostradas son ejemplares y que se pueden utilizar otros medios para establecer un enlace de comunicaciones entre los ordenadores.

El sistema 702 informático es operativo para comunicarse con dispositivos o entidades cableados e inalámbricos usando la familia de estándares IEEE 802, tales como dispositivos inalámbricos dispuestos de forma operativa en comunicación inalámbrica (p. ej., técnicas de modulación por aire IEEE 802.16). Esto incluye por lo menos las tecnologías inalámbricas wifi (o fidelidad inalámbrica), WiMax y Bluetooth^{MT}, entre otras. Así, la comunicación puede ser una estructura predefinida como en una red convencional o sencillamente una comunicación ad hoc entre por lo menos dos dispositivos. Las redes wifi utilizan tecnologías de radio denominadas IEEE 802.11x (a, b, g, n, etc.) para proporcionar una conectividad inalámbrica segura, fiable y rápida. Se puede utilizar una red wifi para conectar ordenadores entre sí, a Internet y a redes cableadas (que utilizan medios y funciones relacionados con el IEEE 802.3).

Se pueden implementar diversas realizaciones utilizando elementos de hardware, elementos de software o una combinación de ambos. Ejemplos de elementos de hardware pueden incluir procesadores, microprocesadores, circuitos, elementos de circuito (p. ej., transistores, resistencias, condensadores, inductores, etc.), circuitos integrados, circuitos integrados de aplicaciones específicas (ASIC), dispositivos lógicos programables (PLD), procesadores de señales digitales (DSP), matrices de puertas programables in situ (FPGA), puertas lógicas, registros, dispositivos semiconductores, chips, microchips, conjuntos de chips, etc. Los ejemplos de software pueden incluir componentes de software, programas, aplicaciones, programas informáticos, programas de aplicación, programas de sistema, programas de máquina, software de sistema operativo, middleware, firmware, módulos de software, rutinas, subrutinas, funciones, procedimientos, procedimientos, interfaces de software, interfaces de programas de aplicación (API), conjuntos de instrucciones, código informático, código informático, segmentos de código, segmentos de código informático, palabras, valores, símbolos o cualquier combinación de los mismos. La determinación de si una realización se implementa usando elementos de hardware y/o elementos de software puede variar según un número cualquiera de factores, tales como la velocidad computacional deseada, niveles de potencia, tolerancias térmicas, presupuesto del ciclo de procesamiento, velocidades de datos de entrada, velocidades de datos de salida, recursos de memoria, velocidades del bus de datos y otras limitaciones de diseño o rendimiento.

Uno o más aspectos de por lo menos una realización pueden implementarse mediante instrucciones representativas almacenadas en un medio legible por máquina que representa lógica diversa dentro del procesador, que cuando es leída por una máquina hace que la máquina fabrique la lógica para realizar las técnicas descritas en la presente memoria. Dichas representaciones, conocidas como "núcleos IP", pueden almacenarse en un medio tangible legible por máquina y suministrarse a diversos clientes o instalaciones de fabricación para cargarlas en las máquinas de fabricación que realizan la lógica o el procesador. Algunas realizaciones pueden implementarse, por ejemplo, usando un medio o artículo legible por máquina que puede almacenar una instrucción o un conjunto de instrucciones que, si son ejecutadas por una máquina, pueden hacer que la máquina realice un procedimiento y/o las operaciones según las realizaciones. Dicha máquina puede incluir, por ejemplo, cualquier plataforma de procesamiento, plataforma informática, dispositivo informático, dispositivo de procesamiento, sistema informático, sistema de procesamiento, ordenador, procesador o similar adecuado, y puede implementarse usando cualquier combinación adecuada de hardware y/o software. El medio o artículo legible por máquina puede incluir, por ejemplo, cualquier tipo adecuado de unidad de memoria, dispositivo de memoria, artículo de memoria, medio de memoria, dispositivo de almacenamiento, artículo de almacenamiento, medio de almacenamiento y/o unidad de almacenamiento, por ejemplo, memoria, medios extraíbles o no extraíbles, medios borrables o no borrables, medios grabables o regrabables, medios digitales o analógicos, disco duro, disquete, disco compacto con memoria de solo lectura (CD-ROM), disco compacto grabable (CD-R), disco compacto regrabable (CD-RW), disco óptico, medios magnéticos, medios magnetoópticos, tarjetas o discos de memoria extraíbles, diversos tipos de disco versátil digital (DVD), una cinta, un casete o similares. Las instrucciones pueden incluir cualquier tipo adecuado de código, tal como código fuente, código compilado, código interpretado, código ejecutable, código estático, código dinámico, código cifrado y similares, implementado utilizando cualquier lenguaje de programación adecuado de alto nivel, bajo nivel, orientado a objetos, visual, compilado y/o interpretado.

La descripción anterior de realizaciones ejemplares se ha presentado con fines de ilustración y descripción. No pretende ser exhaustiva ni limitar la presente divulgación a las formas exactas divulgadas. Son posibles muchas modificaciones y variaciones a la luz de la presente divulgación. Se pretende que el alcance de la presente divulgación no esté limitado por la presente descripción detallada, sino más bien por las reivindicaciones adjuntas a la misma.

REIVINDICACIONES

1. Un procedimiento, que comprende:

emitir, mediante una aplicación (113) que se ejecuta en un dispositivo (110) móvil, una indicación (201) que especifica que debe leer una tarjeta (101) sin contacto para completar una transacción iniciada en la aplicación, la transacción asociada con un identificador (116) de transacción;

recibir, mediante la aplicación desde una interfaz (107) de comunicaciones de la tarjeta sin contacto, datos (106) cifrados generados por la tarjeta sin contacto basándose por lo menos en parte en una clave (104) privada para la tarjeta sin contacto almacenada en una memoria (102) de la tarjeta sin contacto;

transmitir, mediante la aplicación: (i) un identificador de comerciante (115) de un comerciante asociado con la aplicación, (ii) el identificador de transacción, (iii) los datos cifrados, (iv) una ubicación del dispositivo móvil, y (v) una huella digital del software del dispositivo móvil a un servidor (120) de autenticación;

verificar, mediante el servidor de autenticación, los datos cifrados al descifrar los datos cifrados basándose por lo menos en parte en una copia de la clave privada de la tarjeta sin contacto almacenada en una memoria (122) del servidor de autenticación;

determinar, mediante el servidor de autenticación, que la tarjeta sin contacto se ha utilizado previamente para realizar una compra con el comerciante asociado con el identificador de comerciante recibido;

determinar, mediante el servidor de autenticación, que la huella digital del software coincide con una huella digital del software del dispositivo móvil almacenada asociada con una cuenta asociada con la tarjeta sin contacto;

determinar, mediante el servidor de autenticación, que la ubicación del dispositivo móvil está dentro de una distancia umbral de una ubicación conocida asociada con la tarjeta sin contacto, comprendiendo la ubicación conocida por lo menos una de una ubicación doméstica o una ubicación de trabajo asociada con la cuenta;

determinar, mediante el servidor de autenticación, procesar la transacción sin autenticar las credenciales de inicio de sesión para la cuenta por medio de la aplicación basándose en: la verificación de los datos cifrados, la determinación de que la tarjeta sin contacto se ha utilizado previamente para realizar una compra con el comerciante, la determinación de que la huella digital del software coincide con la huella digital del software almacenada y la determinación de que el dispositivo móvil está dentro de la distancia umbral de la ubicación conocida;

dar instrucciones, mediante el servidor de autenticación basándose en la determinación de procesar la transacción sin autenticar las credenciales de inicio de sesión para la cuenta por medio de la aplicación, a un servidor (140) de número de cuenta virtual para que genere un número de cuenta virtual para la transacción;

generar, mediante el servidor de número de cuenta virtual, el número de cuenta virtual para la transacción, una fecha de caducidad asociada con el número de cuenta virtual y un valor de verificación de la tarjeta, CVV, asociado con el número de cuenta virtual;

transmitir, mediante el servidor de número de cuenta virtual, el identificador de comerciante, el identificador de transacción, el número de cuenta virtual, la fecha de caducidad y el CVV a un servidor (150) de comerciante, el servidor de comerciante asociado con el comerciante; y

procesar, mediante el servidor de comerciante, la transacción utilizando el identificador de transacción, el número de cuenta virtual, la fecha de caducidad y el CVV.

2. El procedimiento de la reivindicación 1, que además comprende:

recibir, mediante el servidor de número de cuenta virtual desde una base de datos (124) de cuentas, un nombre del titular de una cuenta asociada con la tarjeta sin contacto y una dirección asociada con la cuenta; y

transmitir, mediante el servidor de número de cuenta virtual, el nombre y la dirección del titular de la cuenta al servidor de comerciante, para que el servidor de comerciante procese posteriormente la transacción utilizando el nombre y la dirección del titular de la cuenta.

3. El procedimiento de la reivindicación 2, que además comprende:

generar, mediante el servidor de comerciante, un registro de transacción en una base de datos (151) de transacciones que comprende el identificador de transacción, el número de cuenta virtual, la fecha de caducidad, el CVV, el nombre del titular de la cuenta, la dirección y por lo menos una de una indicación de un producto adquirido y una indicación de un servicio adquirido;

transmitir, mediante el servidor de comerciante a la aplicación, una indicación de que la transacción se ha procesado; y

enviar, mediante la aplicación, la indicación de que la transacción se ha procesado en un visualizador del dispositivo móvil.

4. El procedimiento de la reivindicación 3, que además comprende:

determinar, mediante el servidor de comerciante, un conflicto de direcciones basándose en que la dirección es diferente de una dirección conocida especificada en un perfil de usuario;

transmitir, mediante el servidor de comerciante, la dirección y la dirección conocida a la aplicación;

emitir, mediante la aplicación en un visualizador, una indicación de la dirección y la dirección conocida;

recibir, mediante la aplicación, la dirección seleccionada y la dirección conocida; y

transmitir, mediante la aplicación, la dirección seleccionada y la dirección conocida al servidor de comerciante, para que el servidor de comerciante procese la transacción utilizando la dirección seleccionada y la dirección conocida.

5. El procedimiento de la reivindicación 4, en el que la aplicación recibe los datos cifrados según la comunicación de campo cercano (NFC) o el estándar EMV.

6. El procedimiento de la reivindicación 5, que además comprende:

recibir, mediante el servidor de autenticación, un identificador de dispositivo del dispositivo móvil desde la aplicación;

determinar, mediante el servidor de autenticación, que el identificador de dispositivo está asociado con la cuenta; y en el que el servidor de autenticación da instrucciones al servidor de número de cuenta virtual para que genere el número de cuenta virtual para la transacción basándose en la determinación de que el identificador de dispositivo está asociado con la cuenta.

7. El procedimiento de la reivindicación 6, en el que el número de cuenta virtual es diferente de un número de cuenta asociado con la tarjeta sin contacto.

8. El procedimiento de la reivindicación 7, que además comprende:

generar, mediante el servidor de comerciante, el identificador de transacción para la transacción; y

transmitir, mediante el servidor de comerciante, el identificador de transacción a la aplicación.

9. El procedimiento de la reivindicación 1, en el que la interfaz de comunicaciones de la tarjeta sin contacto está configurada para admitir comunicación de campo cercano (NFC), Bluetooth y wifi.

10. Un sistema (100) que comprende una aplicación (113) que se ejecuta en un dispositivo (110) móvil, una tarjeta (101) sin contacto que comprende una interfaz (107) de comunicaciones y una memoria (102), un servidor (120) de autenticación que comprende una memoria (122), un servidor (140) de número de cuenta virtual y un servidor (150) de comerciante, en el que el sistema (100) está configurado para realizar un procedimiento según se reivindica en cualquier reivindicación anterior.

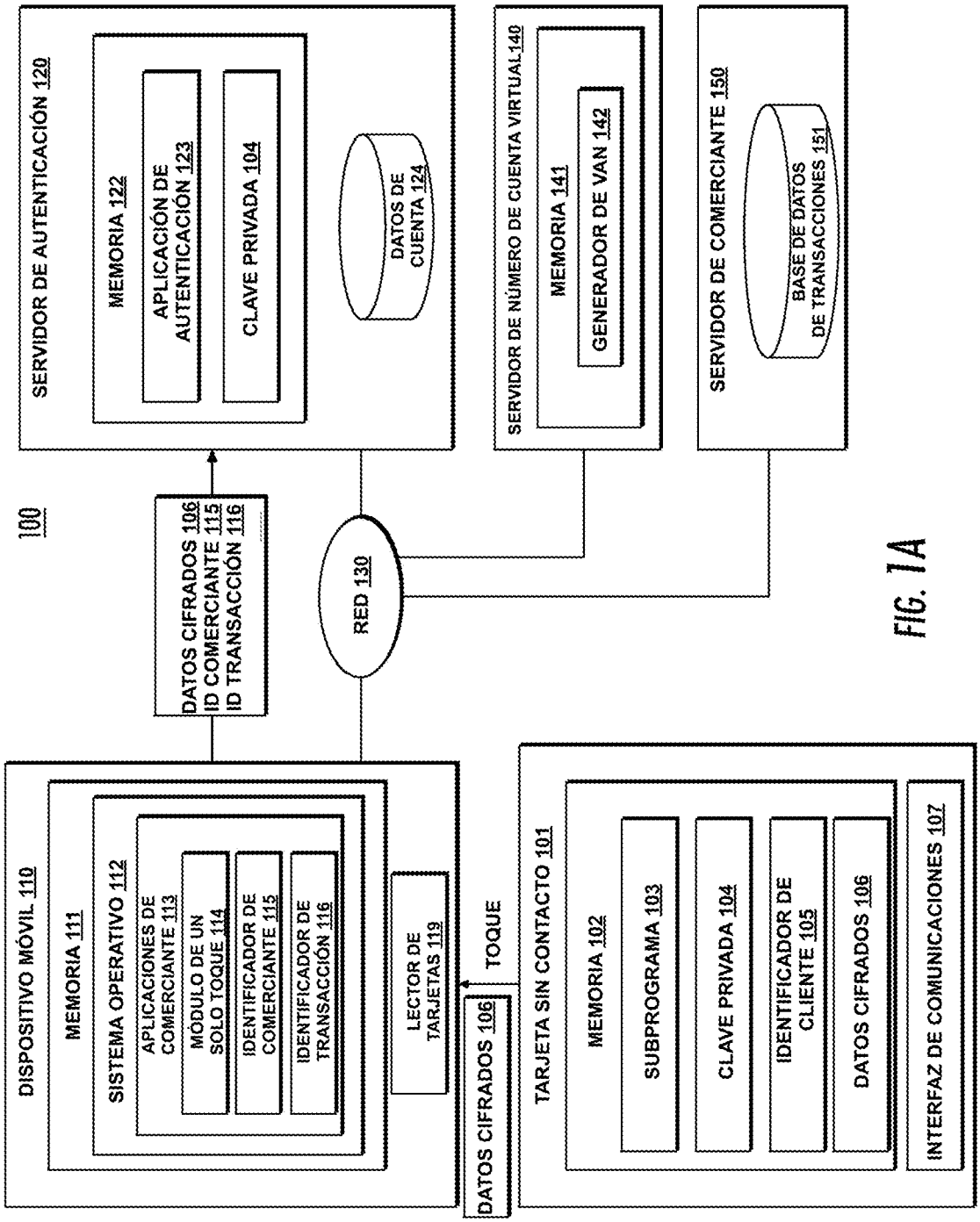
100
SERVIDOR DE AUTENTICACIÓN 120
MEMORIA 122
APLICACIÓN DE AUTENTICACIÓN 123
CLAVE PRIVADA 104
DATOS DE CUENTA 124
SERVIDOR DE NÚMERO DE CUENTA VIRTUAL 140
MEMORIA 141
GENERADOR DE VAN 142
SERVIDOR DE COMERCIANTE 150
BASE DE DATOS DE TRANSACCIONES 151
DATOS CIFRADOS 106
ID COMERCIANTE 115
ID TRANSACCIÓN 116
RED 130
DISPOSITIVO MÓVIL 110
MEMORIA 111
SISTEMA OPERATIVO 112
APLICACIONES DE COMERCIANTE 113
MÓDULO DE UN SOLO TOQUE 114
IDENTIFICADOR DE COMERCIANTE 115
IDENTIFICADOR DE TRANSACCIÓN 116
LECTOR DE TARJETAS 119
TOQUE
DATOS CIFRADOS 106
TARJETA SIN CONTACTO 101
MEMORIA 102
SUBPROGRAMA 103
CLAVE PRIVADA 104
IDENTIFICADOR DE CLIENTE 105
DATOS CIFRADOS 106
INTERFAZ DE COMUNICACIONES 107

FIG. 1A

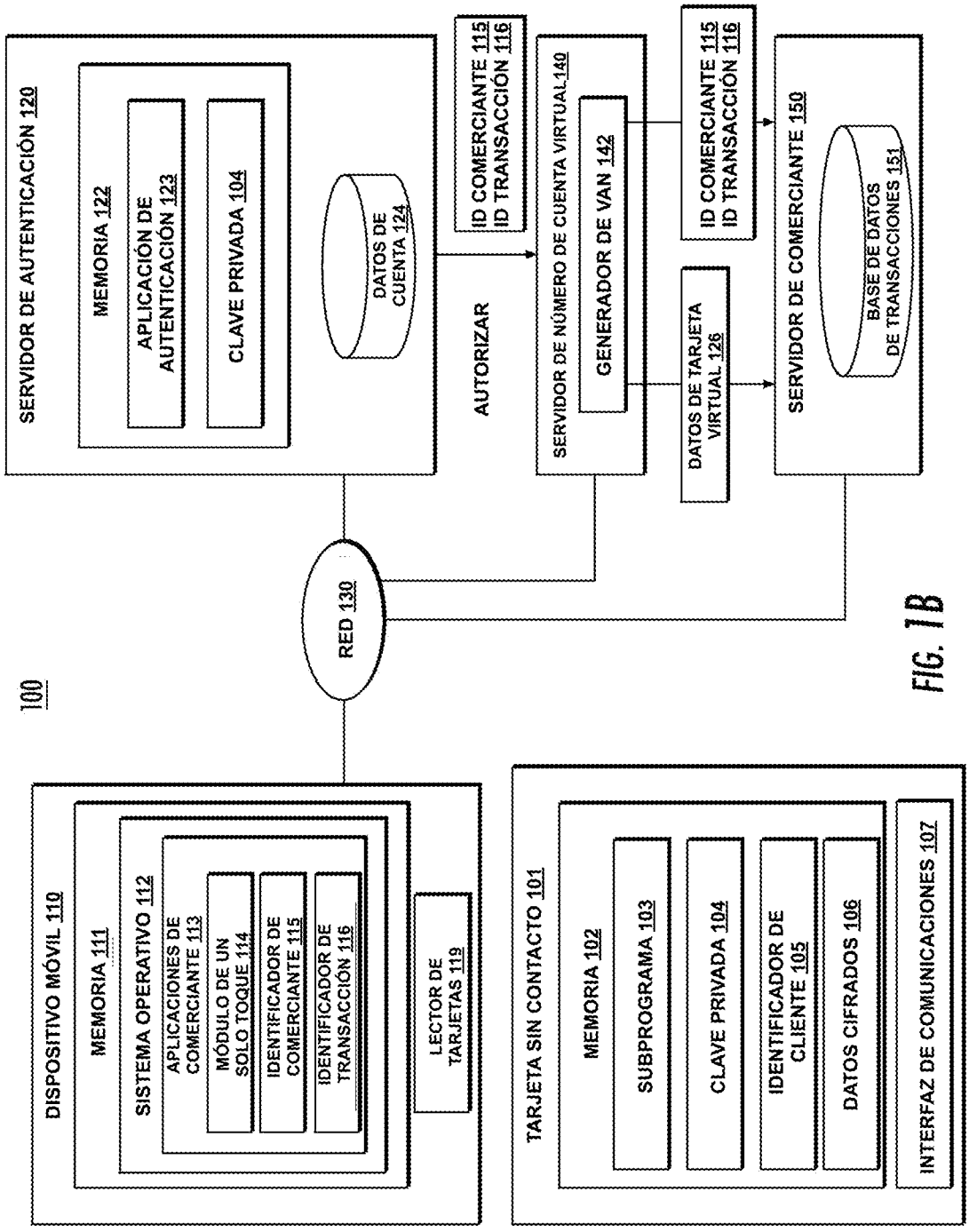
100
SERVIDOR DE AUTENTICACIÓN 120
MEMORIA 122
APLICACIÓN DE AUTENTICACIÓN 123
CLAVE PRIVADA 104
DATOS DE CUENTA 124
ID COMERCIANTE 115
ID TRANSACCIÓN 116
AUTORIZAR
SERVIDOR DE NÚMERO DE CUENTA VIRTUAL 140
GENERADOR DE VAN 142
ID COMERCIANTE 115
ID TRANSACCIÓN 116
DATOS DE TARJETA VIRTUAL 126
SERVIDOR DE COMERCIANTE 150
BASE DE DATOS DE TRANSACCIONES 151
RED 130
DISPOSITIVO MÓVIL 110
MEMORIA 111
SISTEMA OPERATIVO 112
APLICACIONES DE COMERCIANTE 113
MÓDULO DE UN SOLO TOQUE 114
IDENTIFICADOR DE COMERCIANTE 115
IDENTIFICADOR DE TRANSACCIÓN 116
LECTOR DE TARJETAS 119
TARJETA SIN CONTACTO 101
MEMORIA 102
SUBPROGRAMA 103
CLAVE PRIVADA 104
IDENTIFICADOR DE CLIENTE 105
DATOS CIFRADOS 106
INTERFAZ DE COMUNICACIONES 107

FIG. 1B

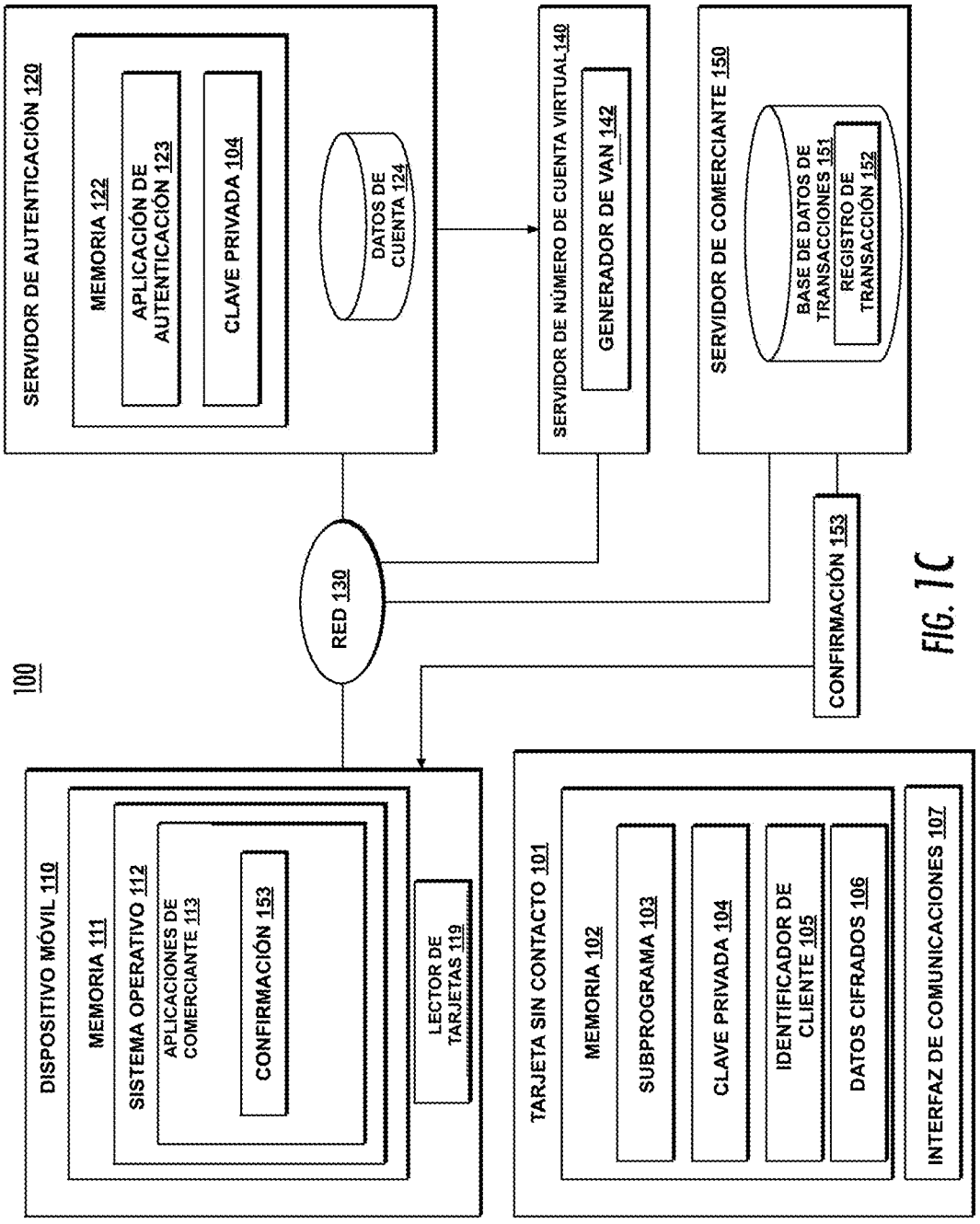
100
SERVIDOR DE AUTENTICACIÓN 120
MEMORIA 122
APLICACIÓN DE AUTENTICACIÓN 123
CLAVE PRIVADA 104
DATOS DE CUENTA 124
SERVIDOR DE NÚMERO DE CUENTA VIRTUAL 140
GENERADOR DE VAN 142
SERVIDOR DE COMERCIANTE 150
BASE DE DATOS DE TRANSACCIONES 151
REGISTRO DE TRANSACCIÓN 152
RED 130
CONFIRMACIÓN 153
DISPOSITIVO MÓVIL 110
MEMORIA 111
SISTEMA OPERATIVO 112
APLICACIONES DE COMERCIANTE 113
CONFIRMACIÓN 153
LECTOR DE TARJETAS 119
TARJETA SIN CONTACTO 101
MEMORIA 102
SUBPROGRAMA 103
CLAVE PRIVADA 104
IDENTIFICADOR DE CLIENTE 105
DATOS CIFRADOS 106
INTERFAZ DE COMUNICACIONES 107

FIG. 1C

200
TU CARRITO
TOCA TU TARJETA PARA COMPRAR CON UN SOLO TOQUE
201
YUNQUE DE HIERRO FUNDIDO
Ctd. 1
PRECIO 19,99
CATAPULTA
Ctd. 1
PRECIO 20,00
TOTAL: 39,99 $
113
110
101

FIG. 2A

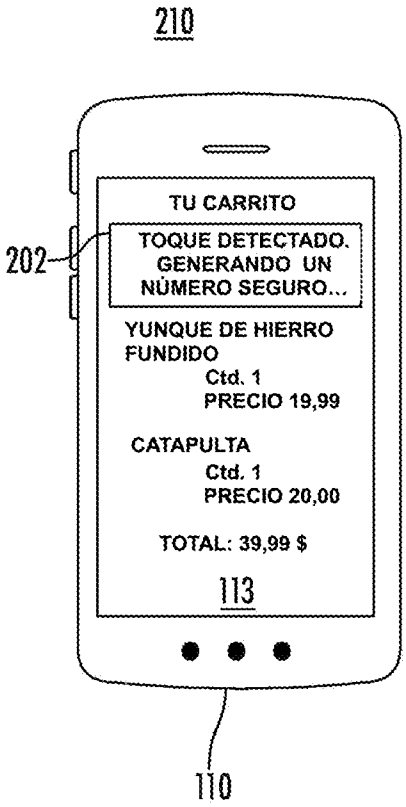
210
TU CARRITO
TOQUE DETECTADO. GENERANDO UN NÚMERO SEGURO...
202
YUNQUE DE HIERRO FUNDIDO
Ctd. 1
PRECIO 19,99
CATAPULTA
Ctd. 1
PRECIO 20,00
TOTAL: 39,99 $
113
110

FIG. 2B

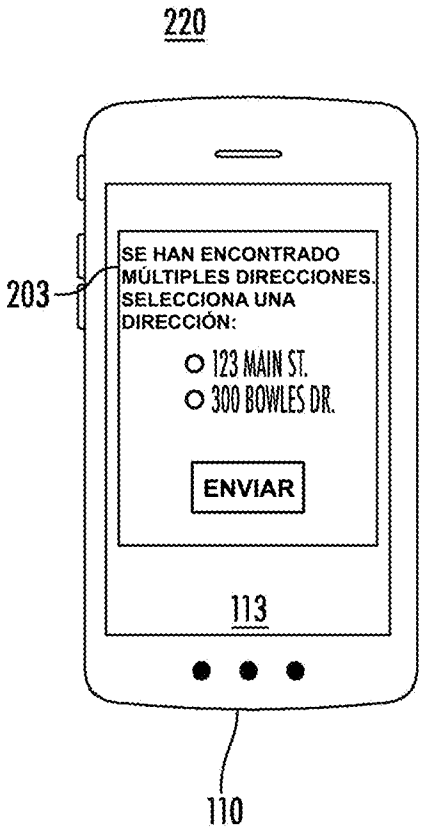
220
SE HAN ENCONTRADO MÚLTIPLES DIRECCIONES. SELECCIONA UNA DIRECCIÓN:
123 MAIN ST.
300 BOWLES DR.
ENVIAR
203
113
110

FIG. 2C

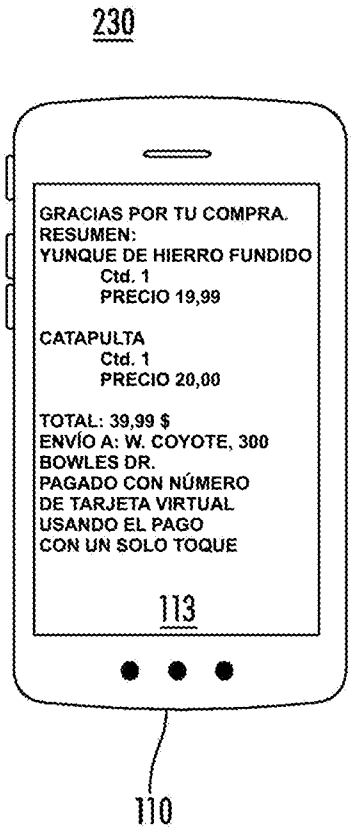
230
GRACIAS POR TU COMPRA.
RESUMEN:
YUNQUE DE HIERRO FUNDIDO
Ctd. 1
PRECIO 19,99
CATAPULTA
Ctd. 1
PRECIO 20,00
TOTAL: 39,99 $
ENVÍO A: W. COYOTE, 300 BOWLES DR.
PAGADO CON NÚMERO DE TARJETA VIRTUAL USANDO EL PAGO CON UN SOLO TOQUE
113
110

FIG. 2D

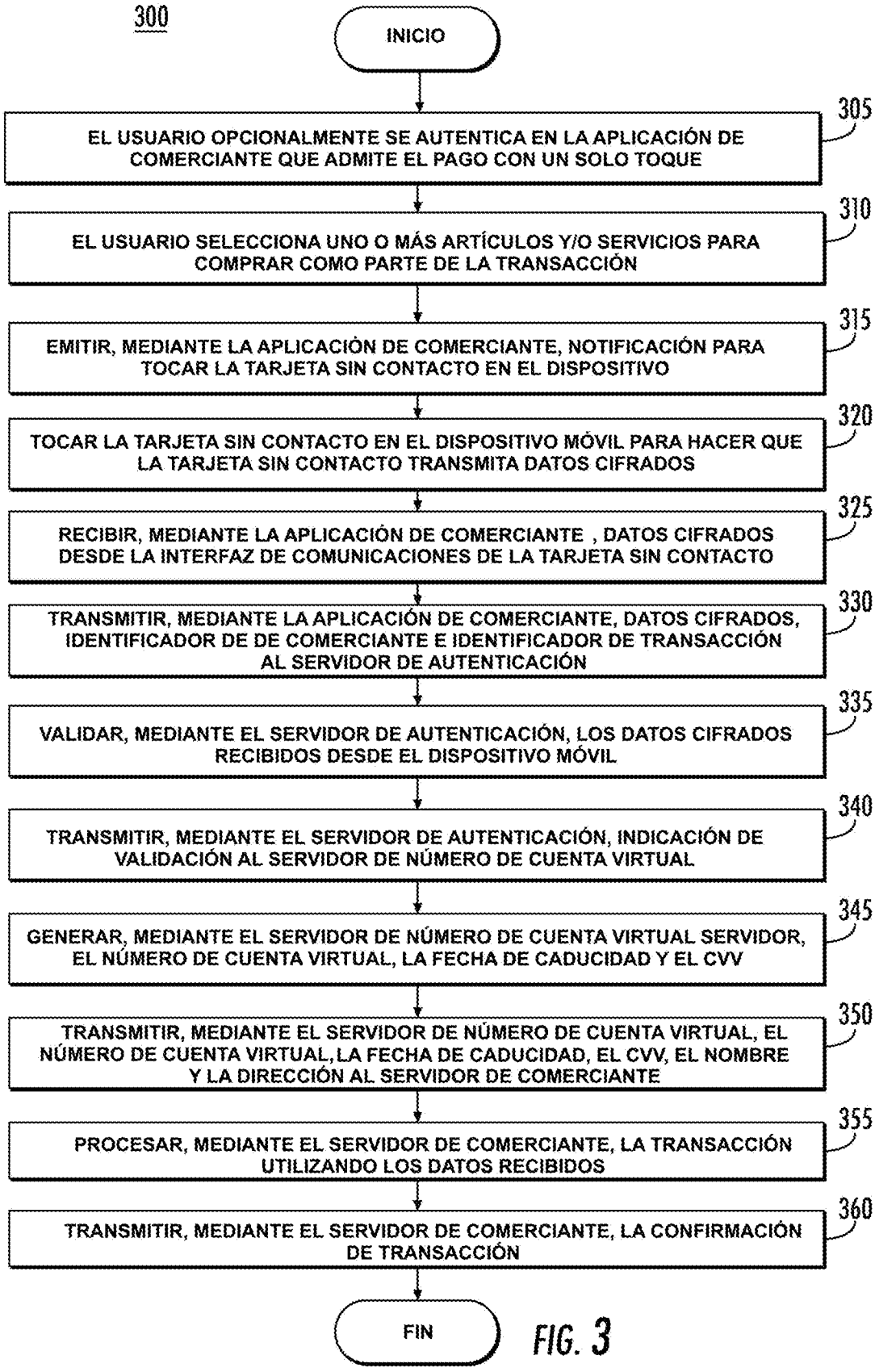
300
INICIO
EL USUARIO OPCIONALMENTE SE AUTENTICA EN LA APLICACIÓN DE COMERCIANTE QUE ADMITE EL PAGO CON UN SOLO TOQUE
305
EL USUARIO SELECCIONA UNO O MÁS ARTÍCULOS Y/O SERVICIOS PARA COMPRAR COMO PARTE DE LA TRANSACCIÓN
310
EMITIR, MEDIANTE LA APLICACIÓN DE COMERCIANTE, NOTIFICACIÓN PARA TOCAR LA TARJETA SIN CONTACTO EN EL DISPOSITIVO
315
TOCAR LA TARJETA SIN CONTACTO EN EL DISPOSITIVO MÓVIL PARA HACER QUE LA TARJETA SIN CONTACTO TRANSMITA DATOS CIFRADOS
320
RECIBIR, MEDIANTE LA APLICACIÓN DE COMERCIANTE , DATOS CIFRADOS DESDE LA INTERFAZ DE COMUNICACIONES DE LA TARJETA SIN CONTACTO
325
TRANSMITIR, MEDIANTE LA APLICACIÓN DE COMERCIANTE, DATOS CIFRADOS, IDENTIFICADOR DE DE COMERCIANTE E IDENTIFICADOR DE TRANSACCIÓN AL SERVIDOR DE AUTENTICACIÓN
330
VALIDAR, MEDIANTE EL SERVIDOR DE AUTENTICACIÓN, LOS DATOS CIFRADOS RECIBIDOS DESDE EL DISPOSITIVO MÓVIL
335
TRANSMITIR, MEDIANTE EL SERVIDOR DE AUTENTICACIÓN, INDICACIÓN DE VALIDACIÓN AL SERVIDOR DE NÚMERO DE CUENTA VIRTUAL
340
GENERAR, MEDIANTE EL SERVIDOR DE NÚMERO DE CUENTA VIRTUAL SERVIDOR, EL NÚMERO DE CUENTA VIRTUAL, LA FECHA DE CADUCIDAD Y EL CVV
345
TRANSMITIR, MEDIANTE EL SERVIDOR DE NÚMERO DE CUENTA VIRTUAL, EL NÚMERO DE CUENTA VIRTUAL, LA FECHA DE CADUCIDAD, EL CVV, EL NOMBRE Y LA DIRECCIÓN AL SERVIDOR DE COMERCIANTE
350
PROCESAR, MEDIANTE EL SERVIDOR DE COMERCIANTE, LA TRANSACCIÓN UTILIZANDO LOS DATOS RECIBIDOS
355
TRANSMITIR, MEDIANTE EL SERVIDOR DE COMERCIANTE, LA CONFIRMACIÓN DE TRANSACCIÓN
360
FIN

FIG. 3

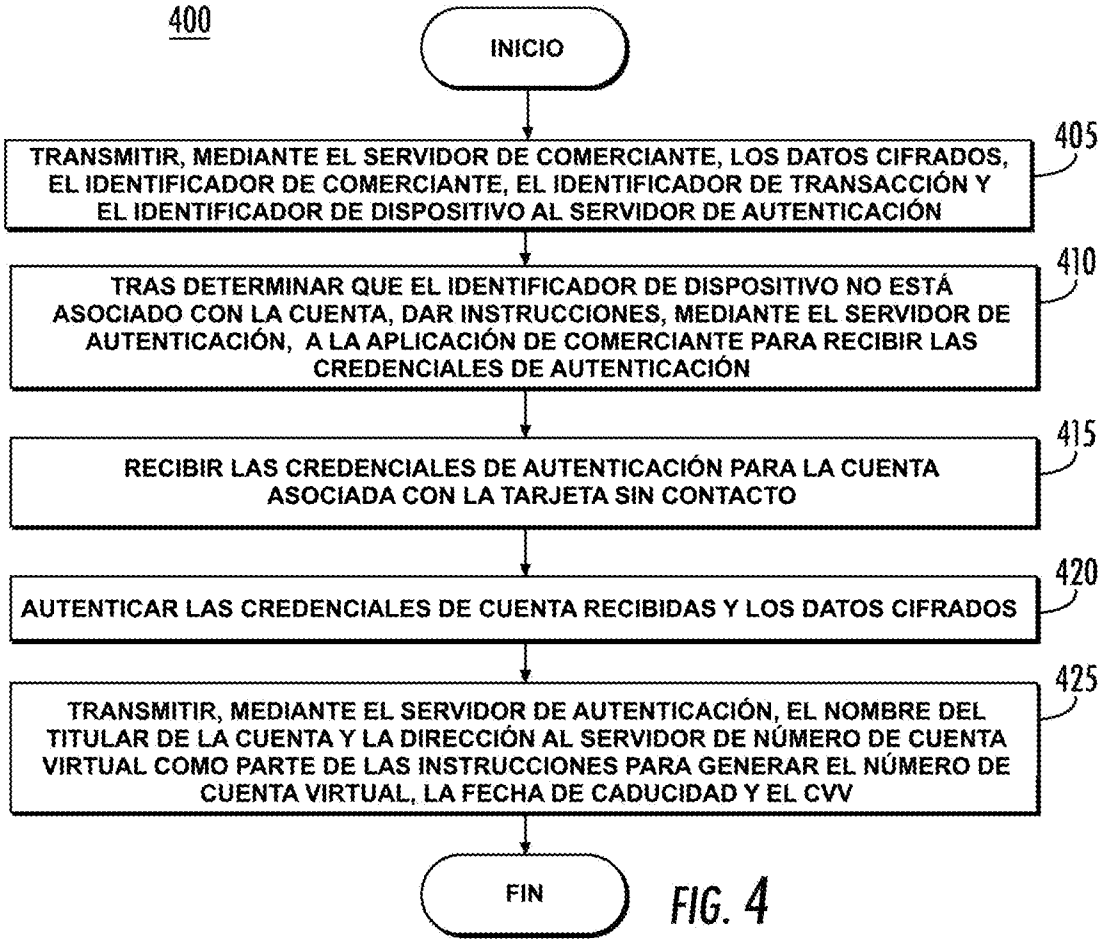
400
INICIO
TRANSMITIR, MEDIANTE EL SERVIDOR DE COMERCIANTE, LOS DATOS CIFRADOS, EL IDENTIFICADOR DE COMERCIANTE, EL IDENTIFICADOR DE TRANSACCIÓN Y EL IDENTIFICADOR DE DISPOSITIVO AL SERVIDOR DE AUTENTICACIÓN
405
TRAS DETERMINAR QUE EL IDENTIFICADOR DE DISPOSITIVO NO ESTÁ ASOCIADO CON LA CUENTA, DAR INSTRUCCIONES, MEDIANTE EL SERVIDOR DE AUTENTICACIÓN, A LA APLICACIÓN DE COMERCIANTE PARA RECIBIR LAS CREDENCIALES DE AUTENTICACIÓN
410
RECIBIR LAS CREDENCIALES DE AUTENTICACIÓN PARA LA CUENTA ASOCIADA CON LA TARJETA SIN CONTACTO
415
AUTENTICAR LAS CREDENCIALES DE CUENTA RECIBIDAS Y LOS DATOS CIFRADOS
420
TRANSMITIR, MEDIANTE EL SERVIDOR DE AUTENTICACIÓN, EL NOMBRE DEL TITULAR DE LA CUENTA Y LA DIRECCIÓN AL SERVIDOR DE NÚMERO DE CUENTA VIRTUAL COMO PARTE DE LAS INSTRUCCIONES PARA GENERAR EL NÚMERO DE CUENTA VIRTUAL, LA FECHA DE CADUCIDAD Y EL CVV
425
FIN

FIG. 4

500
INICIO
GENERAR, MEDIANTE EL SERVIDOR DE COMERCIANTE, EL IDENTIFICADOR DE TRANSACCIÓN PARA LA TRANSACCIÓN
505
RECIBIR, MEDIANTE LA APLICACIÓN DE COMERCIANTE, EL IDENTIFICADOR DE TRANSACCIÓN GENERADO POR EL SERVIDOR DE COMERCIANTE
510
TRANSMITIR, MEDIANTE LA APLICACIÓN DE COMERCIANTE, LOS IDENTIFICADORES DE ARTÍCULOS Y/O SERVICIOS AÑADIDOS Y/O ELIMINADOS DEL CARRITO
515
RECIBIR, MEDIANTE EL SERVIDOR DE COMERCIANTE, DATOS DEL SERVIDOR DE NÚMERO DE CUENTA VIRTUAL
520
PROCESAR, MEDIANTE EL SERVIDOR DE COMERCIANTE, EL PAGO DE LA TRANSACCIÓN GENERANDO UN REGISTRO EN LA BASE DE DATOS DE TRANSACCIONES
525
FIN

FIG. 5

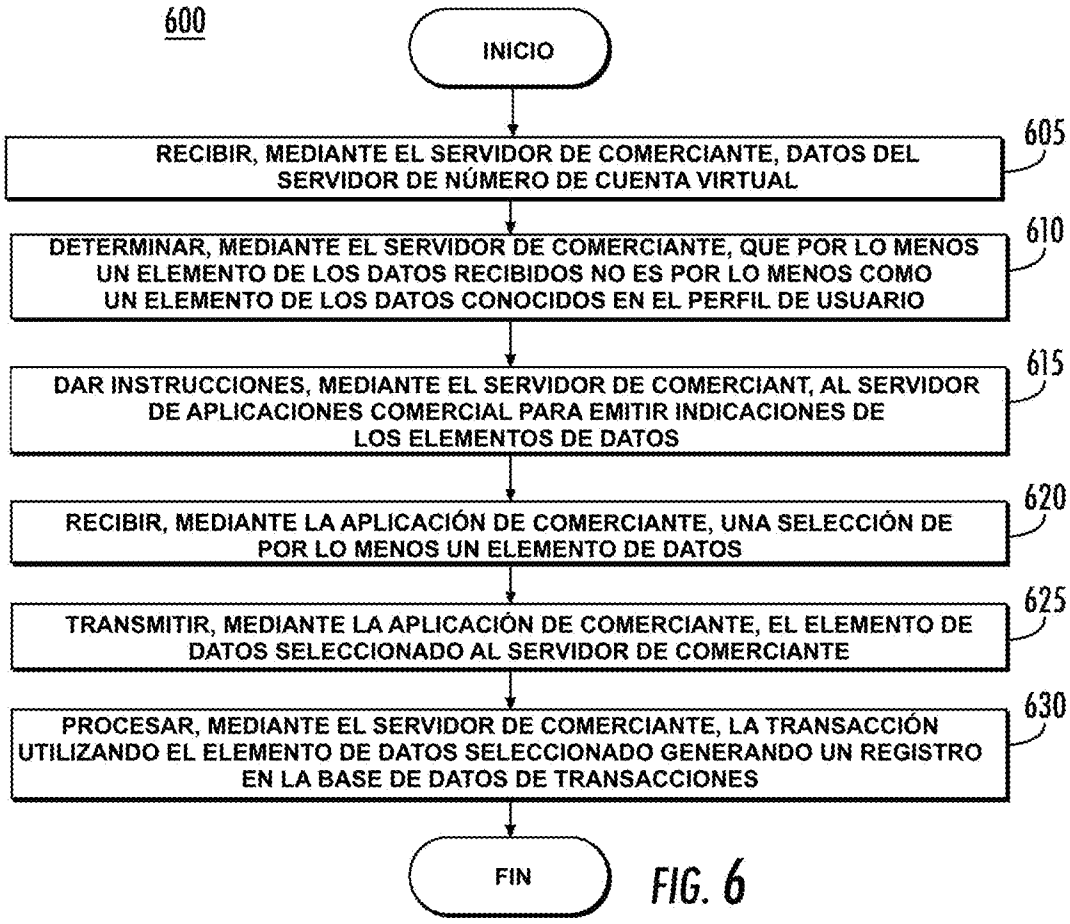
600
INICIO
RECIBIR, MEDIANTE EL SERVIDOR DE COMERCIANTE, DATOS DEL SERVIDOR DE NÚMERO DE CUENTA VIRTUAL
605
DETERMINAR, MEDIANTE EL SERVIDOR DE COMERCIANTE, QUE POR LO MENOS UN ELEMENTO DE LOS DATOS RECIBIDOS NO ES POR LO MENOS COMO UN ELEMENTO DE LOS DATOS CONOCIDOS EN EL PERFIL DE USUARIO
610
DAR INSTRUCCIONES, MEDIANTE EL SERVIDOR DE COMERCIANT, AL SERVIDOR DE APLICACIONES COMERCIAL PARA EMITIR INDICACIONES DE LOS ELEMENTOS DE DATOS
615
RECIBIR, MEDIANTE LA APLICACIÓN DE COMERCIANTE, UNA SELECCIÓN DE POR LO MENOS UN ELEMENTO DE DATOS
620
TRANSMITIR, MEDIANTE LA APLICACIÓN DE COMERCIANTE, EL ELEMENTO DE DATOS SELECCIONADO AL SERVIDOR DE COMERCIANTE
625
PROCESAR, MEDIANTE EL SERVIDOR DE COMERCIANTE, LA TRANSACCIÓN UTILIZANDO EL ELEMENTO DE DATOS SELECCIONADO GENERANDO UN REGISTRO EN LA BASE DE DATOS DE TRANSACCIONES
630
FIN

FIG. 6

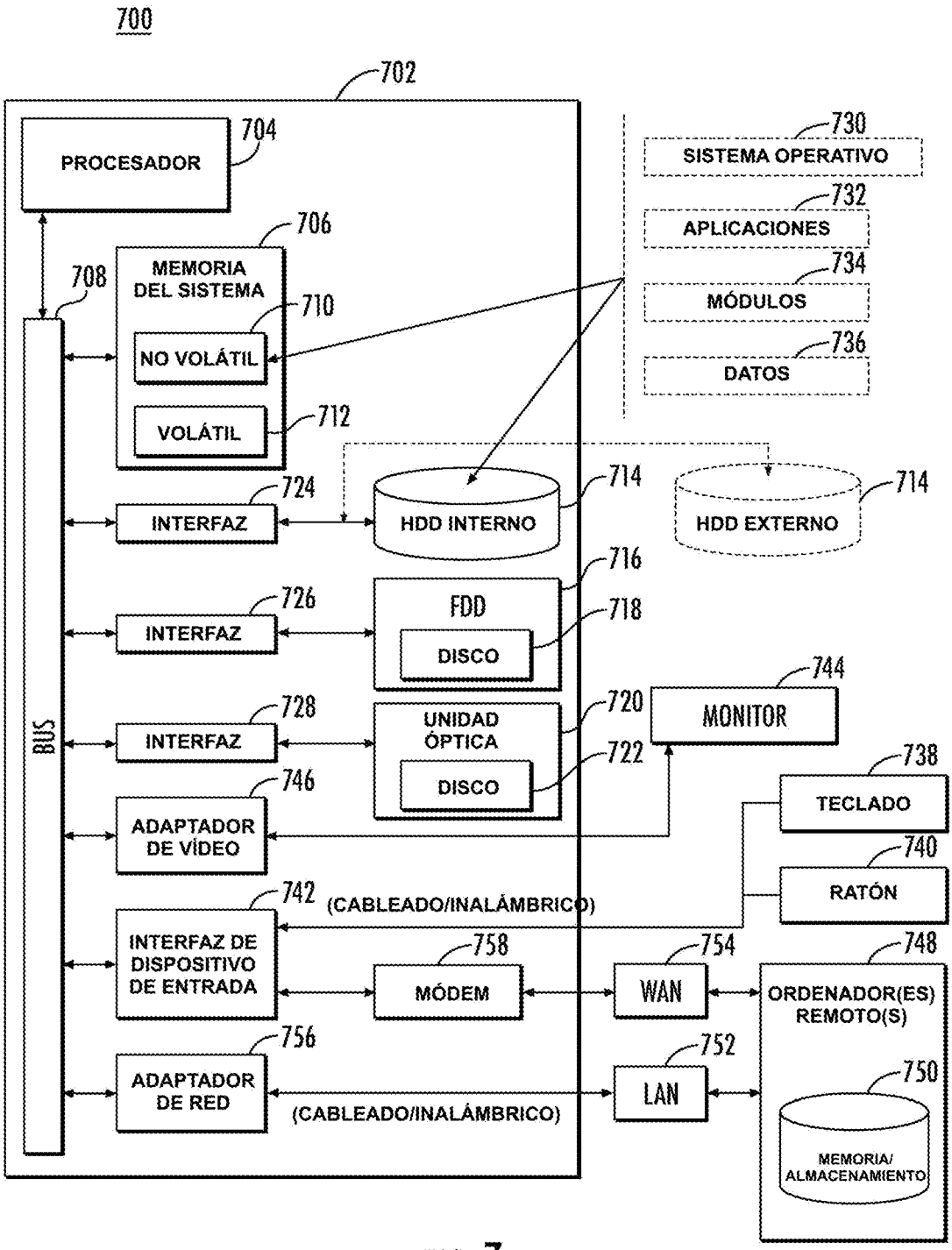
700
702
PROCESADOR
704
MEMORIA DEL SISTEMA
706
708
NO VOLÁTIL
710
VOLÁTIL
712
BUS
INTERFAZ
724
HDD INTERNO
714
HDD EXTERNO
714
INTERFAZ
726
FDD
716
DISCO
718
INTERFAZ
728
UNIDAD ÓPTICA
720
DISCO
722
ADAPTADOR DE VÍDEO
746
MONITOR
744
TECLADO
738
RATÓN
740
INTERFAZ DE DISPOSITIVO DE ENTRADA
742
(CABLEADO/INALÁMBRICO)
MÓDEM
758
WAN
754
ORDENADOR(ES) REMOTO(S)
748
ADAPTADOR DE RED
756
(CABLEADO/INALÁMBRICO)
LAN
752
MEMORIA/ ALMACENAMIENTO
750
SISTEMA OPERATIVO
730
APLICACIONES
732
MÓDULOS
734
DATOS
736

FIG. 7