(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 985 691**

(51) Int. Cl.:

G06Q 20/34 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/20 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/02 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.04.2013 E 21156501 (5)**

(97) Fecha y número de publicación de la concesión europea: **17.04.2024 EP 3848874**

(54) Título: **Sistemas y métodos para facilitar una transacción usando una tarjeta virtual en un dispositivo móvil**

(30) Prioridad:

16.04.2012 US 201261624947 P
18.07.2012 US 201261673096 P
12.10.2012 US 201261713302 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.11.2024

(73) Titular/es:

STICKY.IO, INC. (100.0%)
150 Spear Street, Suite 900
San Francisco, CA 94105, US

(72) Inventor/es:

LAW, SIMON;
SHVARTSMAN, MICHAEL;
ROBERGE, PIERRE ANTOINE y
DUONG, PETER THIEN

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Sistemas y métodos para facilitar una transacción usando una tarjeta virtual en un dispositivo móvil

Campo técnico

Lo siguiente se refiere en general a facilitar una transacción de pago en una ubicación de comerciante usando una tarjeta virtual en un dispositivo móvil, y más específicamente a un método en un servidor de pasarela de pagos y un medio legible por ordenador.

Descripción de la técnica relacionada

Los dispositivos móviles pueden usarse para facilitar una transacción de pago, por ejemplo, a cambio de un bien o servicio en una tienda comercial. Un dispositivo móvil puede estar equipado con un sistema de comunicación de campo cercano (NFC) que puede usarse para transferir la credencial de pago del comprador, tal como información de tarjeta de crédito, a un terminal de punto de venta que también está equipado con un sistema compatible con NFC para completar la transacción de pago.

El documento WO 2003/023674 describe un sistema para pago de tarjeta de crédito usando un código de barras y un dispositivo de teléfono móvil que comprende: un dispositivo de teléfono móvil que almacena datos de código de barras requeridos para un pago de tarjeta de crédito, y que incluye una parte de visualización para visualizar dichos datos de código de barras en el mismo; un dispositivo lector de código de barras que lee el código de barras visualizado en la parte de visualización de dicho dispositivo de teléfono móvil; y un dispositivo de validación de tarjeta de crédito, que está conectado a dicho dispositivo lector de código de barras, que recupera los datos de información de pago de tarjeta de crédito del código de barras que se leen por dicho dispositivo lector de código de barras, que transmite dicha información a un servidor VAN de tarjeta de crédito y, a continuación, que recibe una señal de autenticación de pago de tarjeta de crédito de dicho servidor de VAN de tarjeta de crédito.

El documento US 2003/126094 describe un método para realizar un pago de un pagador a un comerciante del tipo donde el pago implica que el comerciante acepte un pago propuesto en forma de un número de cuenta que tiene una sintaxis convencional del pagador al completar una compra, seguido por el comerciante que solicita una autorización para el pago propuesto de una institución financiera, realizando, mediante un servicio de terceros de confianza, autenticar al pagador y autorizar el pago propuesto en un único proceso integrado realizado sin la implicación del comerciante

El documento WO 2009/112793 describe un sistema para generar un testigo de pago para realizar pagos usando un terminal móvil, comprendiendo dicho sistema un servidor de aplicaciones y un servidor de pago, comprendiendo dicho terminal móvil un módulo de identidad, y en donde el servidor de aplicaciones está adaptado para recibir en un servidor de aplicaciones un mensaje de registro, comprendiendo dicho primer mensaje un número de teléfono asociado con el módulo de identidad, para generar un identificador único y almacenar el identificador único con el número de teléfono, y para enviar el identificador único al terminal móvil; el terminal móvil está adaptado para generar y almacenar un bloque de datos que comprende el identificador único, y el bloque de datos se asegura usando la identidad de suscriptor asociada con el módulo de identidad y un identificador de terminal asociado con el terminal móvil; y el servidor de pago está adaptado para validar una solicitud de un testigo de pago desde el terminal móvil basándose en el identificador único contenido en la solicitud, en donde el identificador único se recupera del bloque de datos almacenado en el terminal móvil

El documento US 2011/113237 describe un método para generar un código de acceso legible por humanos para un usuario autorizado que incluye proporcionar un dato de acceso de control y un PIN, y generar un identificador de máquina único para la máquina de usuario. El método incluye además modificar el dato de acceso controlado, cifrar el dato de acceso controlado usando el PIN y/o un identificador de máquina único para camuflar el dato, y generar un código de acceso usando el dato camuflado y el PIN y/o el identificador de máquina único. Puede usarse un dispositivo de usuario móvil para ejecutar el método en una realización. El código de acceso puede usarse para obtener autorización de transacción y/o acceso a un sistema seguro o datos seguros. El identificador de máquina único puede definirse mediante una calibración de velocidad efectiva de máquina derivada de información recopilada de y única para la máquina de usuario.

El documento US 2011/153498 describe una plataforma central que proporciona valores dinámicos de intermediario para uno cualquiera de un número de dispositivos de pago portátiles de un titular de tarjeta, tras una solicitud de tal información realizada durante una transacción. El valor dinámico de intermediario puede proporcionarse al comerciante, que, a continuación, puede enrutarlo a la red de aceptación para iniciar el proceso de autenticación. La plataforma central proporciona el número de cuenta primario real asociado con el valor dinámico de intermediario durante el proceso de autenticación.

El documento US 2011/161233 describe un método para proporcionar transacciones seguras que incluye recibir un identificador de una cuenta financiera en un sistema de procesador de pagos. Puede generarse un testigo que está

vinculado con el identificador de la cuenta financiera en el sistema de procesador de pagos. El identificador de la cuenta financiera y el testigo pueden almacenarse de forma segura en el sistema de procesador de pagos. El testigo puede transmitirse sin el identificador de la cuenta financiera a al menos un sistema receptor o un dispositivo receptor donde el testigo reemplaza el identificador de la cuenta financiera.

El documento GB 24 76 989 A describe un dispositivo informático móvil que comprende un módulo de comunicación para comunicarse con una etiqueta de autenticación, en el que la etiqueta de autenticación es para habilitar una función segura; en donde el módulo de comunicación está dispuesto para hacer que la etiqueta de autenticación transmita primeros datos de autenticación que pueden recibirse por el módulo de comunicación; y en donde el dispositivo determina si los primeros datos de autenticación son válidos, cuando son recibidos por el módulo de comunicación, y si los primeros datos de autenticación son válidos, el dispositivo ejecuta la función segura.

El documento US 2011/184867 describe un método para generar un valor de tarjeta dinámico (DCV) desde un dispositivo de usuario móvil para su uso en una transacción entre un titular de tarjeta de usuario y un proveedor de transacciones. El DCV puede configurarse para su uso como un valor de verificación de tarjeta (CVV), también conocido como un código de seguridad de tarjeta (CSC), un número de cuenta primario (PAN) o una porción de un PAN. El DCV puede generarse usando un generador de DCV que puede incluir un algoritmo y una clave de generación de DCV. La clave de generación de DCV puede camuflarse. Obtener una DCV desde el dispositivo de usuario puede requerir introducir un PIN, un identificador de dispositivo, un desafío o información de transacción. La DCV puede usarse para cualquier transacción que requiera la entrada de un número de identificación de usuario y un valor de verificación, incluyendo transacciones de tarjeta de crédito, transacciones de tarjeta de débito, transacciones en línea o telefónicas.

El documento US 2011/246324 describe un sistema para procesar una transacción de débito entre un comerciante y un consumidor. El sistema incluye uno o más procesadores programados para recibir información de pago para el consumidor, recopilar datos de autenticación para la tarjeta de débito del consumidor, transmitir un número de cuenta de alias único para la transacción de débito al comerciante, recibir un mensaje de autorización de crédito que incluye el número de cuenta de alias del comerciante, traducir el mensaje de autorización de crédito a un mensaje de autorización de débito usando los datos de autenticación, y transmitir el mensaje de autorización de débito a un procesador de pago.

El documento WO 2012/014231 A1 describe un método para generar una clave de cifrado de múltiples factores usando una contraseña sencilla para acceder al control sobre la información almacenada en una segunda entidad desde una primera entidad a través de al menos una red de comunicación, comprendiendo el método: tener una aplicación preinstalada o solicitar recibir una aplicación en la primera entidad desde la segunda entidad a través de la red de comunicación; activar la primera entidad para generar una clave secreta compartida, en donde la clave secreta compartida se calcula a partir de un primer ID específico de entidad y un número aleatorio generado en la primera y segunda entidades; y permitir que el usuario se registre con la aplicación de la segunda entidad por la primera entidad, en donde el registro incluye la entrada de un PIN personal (número de identificación personal), un mensaje personal, etc.

Sumario

Se proporciona un método en un servidor de pasarela de pagos y un medio legible por ordenador como se define en las reivindicaciones, respectivamente.

Breve descripción de los dibujos

La Figura 1 es un diagrama esquemático de un ejemplo de un sistema de pagos.

La Figura 2 es un diagrama esquemático de un ejemplo de un lado de una tarjeta de crédito de financiación

La Figura 3 es un diagrama esquemático del otro lado de la tarjeta de crédito de financiación en la Figura 2.

La Figura 4 es un diagrama esquemático de una realización de ejemplo de un sistema de pagos que muestra el flujo de datos cuando se usa una tarjeta virtual para facilitar un pago.

La Figura 5 es otra vista de diagrama esquemático de las entidades implicadas en una realización de ejemplo de una transacción de pago usando una tarjeta virtual para facilitar un pago.

La Figura 6 es un diagrama de bloques de una realización de ejemplo de un dispositivo móvil.

La Figura 7 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para generar y usar una tarjeta virtual en una transacción de pago de acuerdo con la perspectiva de un usuario, las instrucciones realizadas por al menos un dispositivo móvil, un terminal de punto de venta y un servidor de pasarela de pagos.

La Figura 8 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para facilitar la transacción de pago usando una tarjeta virtual, mostrando las instrucciones la interacción entre al menos un comerciante y un servidor de pasarela de pagos.

La Figura 9a es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para calcular detalles de tarjeta virtual por el servidor de pasarela de pagos, implementándose las instrucciones como parte del proceso de transacción de la Figura 7.

La Figura 9a es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para autorizar detalles de tarjeta virtual por el servidor de pasarela de pagos, implementándose las instrucciones como parte del proceso de transacción de la Figura 8.

La Figura 10 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para un proceso de registro entre un dispositivo móvil y un servidor de pasarela de pagos.

La Figura 11 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para calcular detalles de tarjeta virtual que incluyen un número de cuenta primario y datos discrecionales, usando los datos intercambiados durante el proceso de registro de la Figura 10.

La Figura 12 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para verificar los datos discrecionales de la Figura 11.

La Figura 13 es un diagrama esquemático que muestra componentes de ejemplo de un sistema usado para facilitar una transacción de comercio electrónico usando una tarjeta virtual.

La Figura 14 es una captura de pantalla de una realización de ejemplo de una interfaz gráfica de usuario (GUI) para realizar una transacción de comercio electrónico usando una tarjeta virtual.

La Figura 15 es una captura de pantalla de otra realización de ejemplo de una GUI para realizar una transacción de comercio electrónico usando una tarjeta virtual.

La Figura 16 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para realizar una transacción de comercio electrónico usando una tarjeta virtual, las instrucciones realizadas por al menos un dispositivo móvil, un terminal de punto de venta y un servidor de pasarela de pagos.

La Figura 17 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para realizar una transacción de comercio electrónico usando una tarjeta virtual, mostrando las instrucciones la interacción entre al menos un comerciante y un servidor de pasarela de pagos.

La Figura 18 es un diagrama de flujo que muestra una transferencia de valor de parte a parte.

La Figura 19 es un diagrama esquemático que muestra componentes de ejemplo de un sistema usado para facilitar una transferencia de valor de parte a parte usando un ID de transferencia.

La Figura 20 es una realización de ejemplo que ilustra el dispositivo móvil de un emisor y el dispositivo móvil de un receptor, mostrando el dispositivo móvil del emisor una interfaz gráfica de usuario (GUI) para seleccionar una tarjeta de financiación.

La Figura 21 es una realización de ejemplo que ilustra el dispositivo móvil del emisor y el dispositivo móvil del receptor de la Figura 20 antes de "tocarse" juntos para facilitar una transferencia de valor de parte a parte.

La Figura 22 es una realización de ejemplo que ilustra el dispositivo móvil del emisor y el dispositivo móvil del receptor, después del toque en la Figura 21, mostrando ambos dispositivos una GUI que indica que se ha completado la transferencia de valor de parte a parte.

La Figura 23 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para calcular un ID de transferencia por el servidor de pasarela de pagos y el dispositivo móvil, de manera que el ID de transferencia se usa para facilitar la transferencia de valor.

La Figura 24 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para validar el ID de transferencia y emitir una tarjeta virtual de prepago al receptor, completando de este modo la transferencia de valor de parte a parte, implementándose las instrucciones como una continuación del proceso de la Figura 23.

La Figura 25 es un diagrama esquemático que muestra componentes de ejemplo de un sistema usado para facilitar una transferencia de valor de parte a parte usando una tarjeta virtual.

La Figura 26 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para calcular detalles de tarjeta virtual por el servidor de pasarela de pagos y el dispositivo móvil.

La Figura 27 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para autorizar detalles de tarjeta virtual y completar la transferencia de valor de parte a parte, implementándose las instrucciones como una continuación del proceso de la Figura 26.

La Figura 28 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para un proceso de registro entre un dispositivo móvil del emisor y un servidor de pasarela de pagos.

La Figura 29 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para calcular detalles de tarjeta virtual que incluyen un número de cuenta primario y datos discrecionales, usando los datos intercambiados durante el proceso de registro de la Figura 28.

La Figura 30 es un diagrama de flujo de una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para verificar los datos discrecionales de la Figura 29.

Descripción detallada

Se apreciará que, por simplicidad y claridad de ilustración, cuando se considere apropiado, los números de referencia pueden repetirse entre las figuras para indicar elementos correspondientes o análogos. Además, se exponen numerosos detalles específicos para proporcionar una comprensión completa de los ejemplos o las realizaciones de ejemplo descritas en el presente documento

La Figura 1 muestra un ejemplo de un flujo de pago en persona típico entre un titular de tarjeta 101, un comerciante 102, un adquirente de comerciante 103, una red de pagos 109 y un emisor de tarjeta 104. El comerciante 102, el adquirente de comerciante 103, la red de pagos 109 y el emisor de tarjeta están cada uno asociado con dispositivos informáticos que incluyen procesadores y memoria. A modo de antecedentes, este flujo de pago también se conoce como un modelo convencional de 4 partes, o un protocolo convencional de 4 partes. El emisor de tarjeta 104 es típicamente un banco que está asociado con una red de pagos. Facilita el uso por parte del titular de la tarjeta de la tarjeta de pago para pagar bienes o servicios basándose en la promesa del titular de la tarjeta de reembolsar al emisor de la tarjeta por la compra. Los ejemplos no limitantes de redes de pago incluyen Visa, MasterCard, American Express y Diners Club/Discover. El emisor de tarjeta 104 emite la tarjeta de pago, que está asociada con una red de pagos 109, al titular de tarjeta 101 (bloque 105). Se entiende que todas las referencias a tarjeta de crédito también se aplicarían a tarjeta de débito, tarjeta de prepago u otras credenciales de pago usadas para facilitar el pago en una ubicación de comerciante. La expresión "tarjeta de financiación" en el presente documento se refiere a tarjetas de débito, tarjetas de crédito, tarjetas de prepago y similares.

Para realizar una compra o pago, el titular de tarjeta 101 (por ejemplo, una persona) proporciona información de tarjeta de financiación al comerciante 102 (bloque 106). Por ejemplo, la tarjeta de financiación se puede "pasar" usando un dispositivo lector de tarjetas de banda magnética, o el número de tarjeta de financiación se puede leer al comerciante 102. El comerciante 102 (por ejemplo, un dispositivo informático) envía la autorización de pago, incluyendo los detalles de la tarjeta de financiación, a un adquirente de comerciante 103 (bloque 107). Un adquirente 103 es una organización que recopila solicitudes de autorización de pago de comerciantes y facilita la transacción de pago con la red de pagos en nombre de los comerciantes.

Cuando el adquirente 103 obtiene la solicitud de autorización de pago de tarjeta de financiación, el adquirente envía la transacción de pago (bloque 108) a la red de pagos 109.

Cuando la red de pagos 109 recibe la solicitud de autorización de pago de tarjeta de financiación, la red de pagos reenvía la transacción de pago (bloque 110) a la autorización de mérito del emisor de tarjeta.

Cuando el emisor de tarjeta 104 recibe la transacción de pago, comprueba la validez de los detalles de transacción. Esto incluye comprobar el número de tarjeta, la fecha de caducidad, el límite de la tarjeta de financiación, etc. El emisor de tarjeta 104 responde al adquiriente de comerciante 103 con un código de autorización de pago (respuesta aprobada o rechazada, número de identificación de transacción, etc.) a través de la red de pagos 109. El adquiriente de comerciante 103 reenvía la respuesta al comerciante 102. A continuación, el comerciante 102 comparte los resultados de autorización de pago con el titular de la tarjeta.

Se reconoce que un sistema de pagos informático establecido de este tipo está bien establecido y es adoptado por

muchos usuarios y grandes empresas. Se reconoce, sin embargo, que un sistema de pagos informático de este tipo no proporciona medios de procesamiento de datos para realizar pagos en un dispositivo móvil. Un sistema de pagos informático de este tipo también requiere que los detalles de la tarjeta de financiación pasen a través del comerciante 102 y el adquiriente de comerciante 103, que puede exponer o revelar datos financieros sensibles. Este riesgo de seguridad planteado por un sistema de pagos informático de este tipo no es deseable.

A modo de antecedentes, se muestra un ejemplo de una tarjeta de crédito 201 en la Figura 2 y la Figura 3. Un lado de la tarjeta de crédito, según la Figura 2, muestra un logotipo 202 o marca que identifica al emisor de la tarjeta. Típicamente, el emisor de la tarjeta es un banco. También se muestra un logotipo 203 o marca para identificar la red de pagos. La tarjeta 201 también muestra el número de tarjeta de crédito 204. El número de tarjeta de crédito 204 se denomina a veces como un número de cuenta primario (PAN). La longitud y el formato del número de tarjeta de crédito 204 varía dependiendo del emisor de la tarjeta y la red de pagos. En general, el primer dígito en el número de tarjeta de crédito 204 identifica la red de pagos. El último dígito del número de tarjeta de crédito 204 es un dígito de control. Un dígito de control es una forma de comprobación de redundancia usada para la detección de errores. Los números intermediarios pueden significar un número de banco (por ejemplo, asociado con el emisor de la tarjeta) y un número de cuenta (por ejemplo, del banco).

En el ejemplo mostrado en la Figura 2, según el bloque 207, el primer dígito "4" identifica que Visa es la red de pagos. Los dígitos dos a seis son el número de identificación del banco emisor. Los dígitos siete a quince son el número de cuenta. El dígito dieciséis es el dígito de control.

La tarjeta de crédito 201 también incluye un intervalo de fechas 205 en las que la tarjeta de crédito es válida. El intervalo de fechas incluye una fecha de caducidad de la tarjeta de crédito. También se muestra el nombre 206 del titular de la tarjeta.

En la Figura 3, en el otro lado de la tarjeta de crédito 201, hay una banda magnética 301, la firma 302 del nombre del titular de la tarjeta y un código de seguridad estático 303. El código de seguridad estático está impreso en la tarjeta de crédito 201.

La banda magnética 301, también denominada en ocasiones banda magnética, está compuesta típicamente de partículas magnéticas a base de hierro diminutas en una película de tipo plástico. La banda 301 tiene información que está escrita en ella.

A menudo hay dos o tres pistas en datos codificados en la banda 301. En una realización de ejemplo, cada pista tiene aproximadamente una décima parte de una pulgada de anchura. La norma ISO/IEC 7811, que se usa por los bancos, especifica que la pista uno es de 210 bits por pulgada (bpi), y contiene 79 caracteres de solo lectura de 6 bits más el bit de paridad; la pista dos es de 75 bpi, y contiene 40 caracteres de 4 bits más el bit de paridad; y la pista tres es de 210 bpi, y contiene 107 caracteres de 4 bits más el bit de paridad. Pueden aplicarse otros formatos de datos.

En un ejemplo, el formato para la pista dos, desarrollado por la industria bancaria, es como sigue (máximo de 40 caracteres):

- Centinela de inicio - un carácter (generalmente "=")
- Número de cuenta principal - hasta 19 dígitos
- Separador - un carácter (generalmente '=')
- Fecha de caducidad - cuatro dígitos en forma de los dos últimos dígitos del año y los dos dígitos que representan el mes (por ejemplo, AAMM)
- Código de servicio - tres dígitos. El primer dígito especifica las reglas de intercambio, el segundo especifica el procesamiento de autorización y el tercero especifica el intervalo de servicio
- Datos discrecionales - equilibrio del espacio disponible para llenar la longitud de la pista dos (por ejemplo, 10 dígitos si el PAN tiene una longitud de 19 dígitos)
- Centinela de finalización - un carácter (generalmente "?")
- Comprobación de redundancia longitudinal (LRC) - un carácter

Los datos anteriores se denominan en el presente documento generalmente como datos de la pista dos.

Se reconoce que, además del factor de forma de tarjeta de plástico típico, como se muestra en la Figura 2 y la Figura 3, hay un número creciente de otros factores de forma que pueden usarse para el pago. Los ejemplos no limitantes incluyen una mini tarjeta, llavero, dispositivo móvil, etc. También se aprecia que otros tipos de tarjeta de financiación además de tarjetas de crédito, incluyen información similar (por ejemplo, PAN, fecha de caducidad, datos de pista dos, etc.).

La forma en que los propios datos de la tarjeta se almacenan en una tarjeta de financiación y se comparten con un terminal de pago tiene muchas variantes, tales como almacenar los datos de la tarjeta en una banda magnética y leer los datos usando un lector de tarjetas magnéticas, o almacenar los datos de la tarjeta usando tecnología de chip y usar un lector compatible con lector de chip para interactuar con la tarjeta. Por ejemplo, aunque no se muestra en la

Figura 2 y la Figura 3, la tarjeta de crédito puede incluir un circuito integrado o chip lógico que puede realizar cálculos. Diversos ejemplos de tecnología de tarjeta basada en chip incluyen emulación de banda magnética sin contacto, EMV de contacto, EMV sin contacto, etc., EMV significa Europay, MasterCard y VISA, una norma global para la interoperación de tarjetas de circuito integrado (tarjetas de CI o "tarjetas de chip") y lector de tarjetas de CI. Además de facilitar el intercambio de información a través de la interfaz de contacto de la tarjeta, también puede intercambiarse información usando las capacidades sin contacto de la tarjeta con capacidad. Tales tarjetas sin contacto en ocasiones se denominan PayPass, payWave y ExpressPay.

Se reconoce que el pago sin contacto es muy adecuado para un dispositivo móvil. Por ejemplo, algunos dispositivos móviles tienen un sistema de comunicación de campo cercano (NFC) que permite transferir datos de forma inalámbrica, usando la norma ISO/IEC 18092 u otras normas compatibles, a lo largo de una distancia relativamente corta. Un dispositivo móvil habilitado para NFC puede establecer comunicación de radio con otro dispositivo habilitado sin contacto tocándolos juntos o manteniéndolos en proximidad cercana. Las expresiones "dispositivo móvil" y "teléfono móvil" se usan de manera intercambiable en el presente documento.

Un dispositivo móvil habilitado para NFC puede estar equipado con una aplicación de "tarjeta de pago de software" (por ejemplo, una implementación de software de una tarjeta de pago sin contacto) que se ejecuta dentro del dispositivo móvil. La tarjeta de pago de software usa las capacidades de comunicación sin contacto compatibles del dispositivo para interactuar con el terminal de POS habilitado sin contacto para facilitar las transacciones de pago.

En muchos casos, la tarjeta de pago de software se almacena en el elemento seguro para proteger los datos de pago sensibles tales como los usados para generar los datos dinámicos necesarios para completar una transacción de pago sin contacto típica. Se reconoce que los elementos seguros están limitados en sus capacidades de almacenamiento. Típicamente están disponibles en forma de un chip integrado, tal como en una tarjeta de circuito integrado universal (UICC), o en una tarjeta de módulo de identidad de abonado (SIM).

En parte para mantener la seguridad de las diversas aplicaciones que se ejecutan dentro del elemento seguro, el elemento seguro se gestiona típicamente por un operador de telefonía móvil que distribuye el elemento seguro con el dispositivo móvil. Parte del servicio gestionado incluye entregar aplicaciones en el elemento seguro directamente, o dar permiso a una organización de terceros para desplegar su aplicación en un elemento seguro particular. El servicio gestionado se entrega típicamente usando lo que la industria denomina como un gestor de servicios de confianza (TSM).

Todas las aplicaciones almacenadas y que se ejecutan dentro del elemento seguro, tal como la "tarjeta de pago de software" individual, necesitan su propio espacio. Las tarjetas de pago se emiten a los consumidores por el emisor de la tarjeta. El despliegue de tarjetas de pago de software en teléfonos móviles requiere un alto nivel de coordinación entre el operador de telefonía móvil y el emisor de tarjeta donde el operador de telefonía móvil proporciona acceso a elementos seguros individuales, uno cada vez, al emisor. Únicamente las tarjetas de emisores de tarjetas de financiación que tienen la infraestructura y el acuerdo con el operador de telefonía móvil pueden usarse en el teléfono móvil para pago sin contacto. Esto es limitante tanto para los emisores de tarjetas como para los titulares de tarjetas.

En los Estados Unidos, por ejemplo, hay miles de bancos emisores y decenas de operadores de telefonía móvil. Los operadores de telefonía móvil usan el TSM, en parte, para emitir y gestionar credenciales de pago en el teléfono móvil. El TSM posibilita que los operadores de telefonía móvil (también denominados proveedores de servicio) u otras entidades que controlan el elemento seguro en teléfonos móviles distribuyan y gestionen remotamente las aplicaciones seguras que se ejecutan dentro del elemento seguro asegurando el acceso al elemento seguro en dispositivos habilitados para móviles. Un ejemplo de aplicación segura es una tarjeta de pago de software. Los bancos emisores también interactúan con los operadores de telefonía móvil a través de un servicio (en una realización de ejemplo, denominado ISIS) para gestionar credenciales de pago emitidas a dispositivos habilitados para NFC. Como un ejemplo no limitante, en Canadá, Rogers Communication es un operador móvil que está asociado con el Banco Imperial Canadiense de Comercio (CIBC), un banco emisor, para emitir una tarjeta de pago de software al teléfono del titular de la tarjeta CIBC en la red de Rogers. Establecer sistemas y métodos para gestionar la emisión y gestión seguras de tarjetas de pago de software entre los bancos emisores, los operadores de telefonía móvil y el dispositivo móvil es costoso y complejo. Implica acuerdos preestablecidos entre las partes, así como algunas personalizaciones del software y sistemas informáticos para satisfacer las necesidades de todas las entidades participantes. Esto puede dificultar que los emisores de tarjetas de menor tamaño adopten la tecnología NFC para facilitar los pagos. También significa que el banco emisor probablemente requerirá numerosas conexiones punto a punto con los diversos operadores móviles que desea soportar, lo que requiere capacidades de hardware y software adicionales para soportar y organizar comunicaciones de datos entre diferentes operadores móviles. Los sistemas y métodos descritos en el presente documento intentan abordar al menos uno de estos problemas.

También se reconoce que, desde la perspectiva del usuario, el proceso de asociar su dispositivo móvil con su tarjeta de financiación que va a usarse para pago sin contacto depende mucho de relaciones preestablecidas entre el operador de telefonía móvil y los emisores de tarjetas. Por lo tanto, un usuario tiene opciones limitadas o ninguna opción cuando determina si su tarjeta de financiación actual puede asociarse con su teléfono móvil para pagos sin contacto. Por ejemplo, un usuario tiene una tarjeta de financiación del emisor de tarjeta de pago A. El usuario también

tiene un teléfono móvil habilitado para NFC del operador de teléfono móvil B. Sin embargo, el operador de teléfono móvil B únicamente tiene un acuerdo e infraestructura preestablecidos para facilitar los pagos sin contacto con el emisor de tarjeta de financiación B. Por lo tanto, incluso si el usuario quisiera usar su teléfono móvil para realizar un pago sin contacto, el usuario no podría hacerlo porque no existe un acuerdo preestablecido e infraestructura de red informática entre el operador de teléfono móvil B y el emisor de tarjeta de financiación A para emitir una tarjeta de pago de software en el teléfono del usuario. Esta limitación de la infraestructura de red informática limita la capacidad del usuario para realizar pagos de tipo NFC con su dispositivo móvil.

En un ejemplo típico de realizar un pago usando un dispositivo móvil habilitado para NFC, un usuario solicita en primer lugar a su emisor que cargue una tarjeta de financiación en su dispositivo móvil. Cuando se completa este proceso, se ha entregado e instalado de forma segura una tarjeta de financiación de software en el elemento seguro en el dispositivo móvil del usuario. El usuario puede usar ahora la tarjeta de financiación en el dispositivo móvil para facilitar transacciones de pago sin contacto en ubicaciones de comerciante que están equipadas para aceptar tal tipo de transacción de pago. Una vez que el usuario intenta pagar con su dispositivo móvil en un comerciante, los detalles de pago se envían y se verifican por el servidor de emisión de tarjetas de financiación de manera similar a otra transacción de pago.

Cuando se usa una credencial de tarjeta de financiación sin contacto para facilitar una transacción de pago, la transacción incluye más a menudo datos dinámicos de la tarjeta para autenticar de forma segura la credencial de pago. Los datos dinámicos cambian de valor cada vez que se usa la credencial. Si los datos dinámicos recibidos en el servidor de emisión de tarjetas de financiación coinciden con el valor esperado calculado por el servidor para la tarjeta, la autenticación de las credenciales de pago se considera satisfactoria y la autorización de pago puede continuar. Puede apreciarse que hay diversas formas en las que el dispositivo móvil y el servidor de emisión de tarjetas de financiación pueden calcular los datos dinámicos usados para autenticar la credencial de pago.

En un ejemplo para tarjetas de crédito, los datos dinámicos son un valor de verificación de tarjeta rotatoria (CVV, también denominado en algún momento CVV dinámico o dCVV). Este CVV rotatorio puede calcularse basándose en información cambiante proporcionada por el circuito integrado dentro de la tarjeta. En otro ejemplo, los datos dinámicos son datos de EMV dinámicos que se calculan usando datos aleatorios de la tarjeta de financiación, o datos aleatorios de un terminal de punto de venta del comerciante, o ambos. Una implementación común de datos dinámicos usa un contador de transacciones de aplicación (ATC) en la tarjeta de modo que cada transacción produce un flujo de datos diferente. Esto se logra a medida que el ATC se incrementa en '1' para cada transacción realizada. Cuando un usuario toca, pulsa o coloca su dispositivo móvil cerca de un terminal de punto de venta (POS) habilitado sin contacto, los datos de la tarjeta de financiación (número de tarjeta, datos dinámicos, fecha de caducidad, etc.), en lo sucesivo denominados datos de pista dos de la tarjeta datos, se envían desde el dispositivo móvil al terminal de POS. Esta información a continuación se dirige al servidor de emisión de tarjetas de financiación para su verificación. El emisor de la tarjeta de financiación realizará numerosas comprobaciones para validar la transacción, incluyendo comparar los datos dinámicos del dispositivo móvil con el valor generado por el servidor. Si los datos dinámicos coinciden, y todas las otras comprobaciones y controles realizados por el emisor de la tarjeta de financiación son satisfactorios, el emisor de la tarjeta de financiación responderá con una respuesta de autorización de pago positiva.

También se reconoce que una aplicación de tarjeta específica para una tarjeta de financiación dada puede instalarse en el dispositivo móvil y usarse para interactuar con el terminal de POS como se ha descrito anteriormente. También se reconoce que la aplicación de tarjeta se instala típicamente en el elemento seguro del dispositivo móvil. Típicamente, cada tarjeta de financiación tiene su propia aplicación de tarjeta correspondiente que reside en el elemento seguro del dispositivo móvil. Puede apreciarse que, como cada aplicación de tarjeta ocupa espacio de almacenamiento en el elemento seguro, y que el elemento seguro típicamente tiene un espacio de almacenamiento muy limitado, tener múltiples aplicaciones de tarjeta en el elemento seguro en algunos casos no es posible debido a espacio de almacenamiento insuficiente. A modo de antecedentes, el elemento seguro puede tener un sistema operativo nativo que se programe para realizar diversas tareas y actividades, incluyendo, por ejemplo, una aplicación de tarjeta que emula los datos de banda magnética de una tarjeta de financiación o una aplicación de tarjeta que emula los datos usados en un pago sin contacto EMV. También, a modo de antecedentes, y a modo de ejemplo, un elemento seguro típico tiene memoria de 256 kB, y cada aplicación de tarjeta puede consumir memoria de 40-80 kB. Por lo tanto, puede apreciarse que asociar múltiples tarjetas de financiación (y cada una de sus aplicaciones de tarjeta) con un dispositivo móvil para pagos de NFC puede estar limitado.

Por lo tanto, es deseable reducir la cantidad de espacio de almacenamiento que requieren las aplicaciones de tarjeta en el elemento seguro para no limitar el número de tarjetas de pago de software que un usuario puede cargar en un elemento seguro. En la misma línea, es deseable que los operadores de telefonía móvil reduzcan la cantidad de datos usados por la "aplicación de tarjeta" en el elemento seguro de modo que puedan cargarse otros tipos de aplicación en el mismo. También es deseable reducir costes incurridos por el emisor de tarjeta de financiación para emitir y operar tarjetas de pago de software en elementos seguros. A modo de antecedentes, un operador de telefonía móvil típicamente cobra a los proveedores de aplicaciones, tales como emisores de tarjetas de financiación, por la cantidad de espacio de almacenamiento usado en el elemento seguro. También es deseable reducir la cantidad de infraestructura requerida por el emisor de tarjeta de financiación para emitir una tarjeta de pago de software para el teléfono móvil. También es deseable reducir la cantidad de coordinación requerida entre el emisor de la tarjeta de

financiación y el operador de telefonía móvil para emitir una tarjeta de pago de software en un teléfono móvil particular. También es deseable permitir que el usuario (por ejemplo, el titular de la tarjeta) cargue cualquiera, y tantas, tarjetas de financiación que desee en su teléfono móvil habilitado para NFC, independientemente del emisor de la tarjeta de financiación que tenga la infraestructura o una relación comercial o acuerdo con un operador de telefonía móvil particular.

Los sistemas y métodos descritos en el presente documento intentan abordar los problemas anteriores.

Se apreciará que diferentes características de las realizaciones de ejemplo de los sistemas y métodos propuestos, como se describe en este documento, pueden combinarse entre sí de diferentes maneras. En otras palabras, una característica descrita con respecto a una realización de un sistema o método de pago móvil puede aplicarse a otra realización del sistema o método de pago móvil, aunque no se indica específicamente.

En general, los sistemas y métodos descritos en el presente documento permiten que un servidor de pasarela de pagos de monedero basado en la nube se sincronice con un dispositivo móvil habilitado para NFC y una aplicación para facilitar transacciones de pago sin contacto en una tienda de comerciante que acepta pago sin contacto. No se requiere un acuerdo preestablecido o infraestructura adicional entre el emisor de la tarjeta de financiación y el operador de telefonía móvil. Un usuario selecciona una tarjeta de financiación para realizar el pago sin contacto, a través de su dispositivo móvil. Se genera una segunda tarjeta, denominada en el presente documento como una tarjeta virtual, junto con todos los datos de tarjeta requeridos (por ejemplo, PAN, fecha de caducidad, datos dinámicos, datos discrecionales, etc.) para completar la transacción de pago. La tarjeta virtual está asociada con la tarjeta de financiación en el servidor de pasarela de pagos. En una realización de ejemplo, la asociación entre la tarjeta virtual y la tarjeta de financiación está limitada a algún periodo de tiempo.

En una realización de ejemplo, los datos requeridos para calcular el conjunto de datos de tarjeta virtual se envían al dispositivo móvil, típicamente cada vez que el usuario desea realizar un pago. Por ejemplo, se crea una nueva tarjeta virtual para todas y cada una de las transacciones de pago. En otro ejemplo, se crea una nueva tarjeta virtual basándose en límites de tiempo, o basándose en ciertos eventos, o ambos, y tiene un periodo de uso mucho más corto en comparación con una tarjeta de financiación convencional que puede usarse típicamente durante varios años. Cuando la tarjeta virtual se puede usar con la tarjeta de financiación para varias transacciones, no es necesario que se envíen datos para calcular una nueva tarjeta virtual al dispositivo móvil cada vez que el usuario realiza un pago.

Cuando se inicia un pago, los datos de tarjeta virtual se envían a través del sistema de NFC en el dispositivo móvil a un terminal de POS habilitado sin contacto. Esta información se envía desde el terminal de POS al sistema de comerciante; desde el sistema comercial hasta el banco de adquirente de comerciante; y desde el banco adquirente al servidor de pasarela de pagos de monedero basado en la nube (también denominado el "servidor de pasarela de pagos") a través de la red de pagos. El servidor de pasarela de pagos de cartera basado en la nube actúa como el servidor emisor de tarjeta virtual y verifica la tarjeta virtual. Si se verifica de manera satisfactoria, los detalles de la tarjeta de financiación asociados con la tarjeta virtual se recuperan y se envían al servidor emisor de la tarjeta de financiación a través de la red de pagos para completar la transacción de autorización de pago. El servidor emisor de tarjeta de financiación verifica la tarjeta de financiación y devuelve un código de autorización al servidor de pasarela de pagos. El servidor de pasarela de pagos envía de vuelta un código de autorización correspondiente al sistema de comerciante.

El pago puede liquidarse cuando el sistema de comerciante inicia una solicitud de liquidación, típicamente, aunque no necesariamente, al final de cada día laborable. Para completar la liquidación, el sistema de comerciante envía todos los números de tarjeta virtual y los correspondientes códigos de autorización recibidos durante el periodo al emisor de tarjeta virtual, a través del banco de adquirente de comerciante. El emisor de tarjeta virtual verifica los números de tarjetas virtuales y los códigos de autorización. Para todos los registros coincidentes, el emisor de tarjeta virtual recupera los números de tarjeta de financiación asociados y códigos de autorización y envía los datos al emisor de tarjeta de financiación para su liquidación a través del banco de adquirente del emisor de tarjeta virtual. El emisor de la tarjeta de financiación verifica los números de tarjeta de financiación y los códigos de autorización, y, si se verifican de manera satisfactoria, envía el dinero a través de un método convencional al originador de la transacción de pago, en este caso el emisor de la tarjeta virtual. En ese punto, el emisor de la tarjeta virtual envía el dinero al banco de adquirente de comerciante usando también un método convencional. En una realización de ejemplo, el emisor de tarjeta virtual es el servidor de pasarela de pagos, o un módulo dentro del servidor de pasarela de pagos.

En un ejemplo, los sistemas y métodos descritos en el presente documento permiten que un monedero basado en la nube (por ejemplo, asociado con una tarjeta de financiación) se sincronice con un dispositivo móvil habilitado para NFC (por ejemplo, asociado con una tarjeta virtual). En otro ejemplo, los sistemas y métodos descritos en el presente documento proporcionan rotación en tiempo real de un número de cuenta primario (PAN) y datos dinámicos usados para facilitar transacciones de pago sin contacto. En otra realización de ejemplo, los sistemas y métodos descritos en el presente documento usan credenciales de pago virtuales para completar una transacción de compra sin contacto en una tienda física sin divulgar los detalles de la tarjeta de financiación del usuario.

Volviendo a la Figura 4, se proporciona una realización de ejemplo que muestra el flujo de datos de pago usando una

tarjeta virtual. Un emisor de tarjeta, también denominado el emisor de tarjeta de financiación 104, emite una cuenta de tarjeta convencional, más a menudo en forma de una tarjeta de plástico, al usuario 101 (bloque 404). La tarjeta convencional es la tarjeta de financiación, y el usuario se convierte en el titular de la tarjeta.

Aunque no se muestra, el titular de tarjeta 101 registra una o muchas tarjetas de financiación y su dispositivo móvil con un emisor de tarjeta virtual 401. Puede apreciarse que, puede registrarse cualquier tarjeta de financiación, y no está limitada o depende de que el operador de telefonía móvil tenga un acuerdo con el emisor de la tarjeta de financiación. En otras palabras, incluso si la tarjeta de financiación y el operador de telefonía móvil no tienen ningún acuerdo o infraestructura informática de conexión, de acuerdo con los sistemas y métodos propuestos, la una o muchas tarjetas de financiación del usuario y el dispositivo móvil del usuario pueden registrarse con el emisor de tarjeta virtual 401. También puede apreciarse que puede registrarse cualquier número de tarjetas de financiación en asociación con el dispositivo móvil. El dispositivo móvil del titular de la tarjeta incluye una aplicación de pagos que puede interactuar con el emisor de tarjeta virtual 401.

En una realización de ejemplo del registro, para cada tarjeta de financiación que el usuario desea registrar, el usuario introduce (por ejemplo, escribe) detalles de la tarjeta en el dispositivo móvil (por ejemplo, los detalles de la tarjeta incluyen el nombre impreso en la tarjeta de financiación, el PAN impreso en la tarjeta de financiación, la fecha de caducidad impresa en la tarjeta de financiación y el código de seguridad estático impreso en la tarjeta de financiación). De acuerdo con la invención, el dispositivo móvil envía estos datos, más un PIN proporcionado por el usuario y el ID de dispositivo móvil al servidor de pasarela de pagos. Para cada tarjeta de financiación, el servidor de pasarela de pagos calcula un identificador de tarjeta de financiación que identifica la tarjeta de financiación dada. El servidor de pasarela de pagos almacena el identificador de tarjeta de financiación en asociación con los detalles de tarjeta de financiación, ID de dispositivo móvil y PIN, y envía el identificador de tarjeta de financiación al dispositivo móvil para su almacenamiento. En una realización de ejemplo, el identificador de tarjeta de financiación es un valor que es diferente del PAN, fecha de caducidad o código de seguridad estático de la tarjeta de financiación. Por ejemplo, el identificador de tarjeta de financiación es un valor aleatorio de modo que, si es interceptado por un adversario, no sería capaz de reconocer ningún detalle de tarjeta de financiación. En una realización de ejemplo, el dispositivo móvil no almacena ningún detalle de tarjeta de financiación, sino que únicamente almacena detalles de tarjeta de financiación limitados (por ejemplo, el nombre del emisor de tarjeta de financiación y los últimos 4 dígitos del PAN). El dispositivo móvil almacena el identificador de tarjeta de financiación, que envía al servidor de pasarela de pagos para indicar una tarjeta de financiación específica. Puede apreciarse que, hay otros métodos para capturar los detalles de la tarjeta de financiación (por ejemplo, además de que el usuario escriba los datos), que pueden usarse con los principios descritos en el presente documento.

Puede apreciarse que, se requiere una única aplicación de pagos en el dispositivo móvil, que puede gestionar múltiples tarjetas de financiación. Si se registran múltiples tarjetas de financiación, se almacena cada uno de los identificadores de tarjeta de financiación asociados en el dispositivo móvil, dentro de la aplicación de pagos única. Los detalles de cada tarjeta de financiación individual se almacenan en el servidor de pasarela de pagos. De esta manera, el servidor de pasarela de pagos actúa como un servidor basado en la nube que almacena los detalles de múltiples tarjetas de financiación. Se describen a continuación detalles adicionales de un proceso de registro de tarjeta de financiación con respecto a la Figura 10.

Continuando con la Figura 4, cuando el titular de tarjeta registrado 101 desea realizar un pago sin contacto usando su dispositivo móvil, el usuario selecciona la tarjeta de financiación. La tarjeta de financiación seleccionada se transmite al emisor de tarjeta virtual 401, y el emisor de tarjeta virtual 401 emite una tarjeta virtual al titular de tarjeta 101, y, más específicamente, a la aplicación de pagos que se ejecuta en el dispositivo móvil (bloque 405). El titular de la tarjeta toca su dispositivo móvil en el sistema de comerciante y los detalles de la tarjeta virtual se entregan al comerciante 106, a través de un terminal de POS habilitado para NFC (bloque 406). El comerciante envía los detalles de la tarjeta virtual al adquirente de comerciante 103 (bloque 407). Basándose en algunos de los detalles de tarjeta virtual, el adquirente de comerciante 103 envía los detalles de tarjeta virtual al emisor de tarjeta virtual 401 (bloque 408) a través de la red de pagos. El emisor de tarjeta virtual 401 usa los detalles de tarjeta virtual para determinar la correspondiente tarjeta de financiación (bloque 409). El operador de tarjeta virtual 402 (por ejemplo, el emisor de tarjeta virtual que ahora actúa como un "comerciante") envía los correspondientes detalles de tarjeta de financiación, incluyendo la cantidad de transacción original, a su adquirente 403 (bloque 410). Esto es paralelo al proceso típico de un comerciante 106 que envía los detalles de la tarjeta de financiación al adquirente de comerciante 103. El adquirente de tarjeta virtual 403 envía los detalles de la tarjeta de financiación al emisor de la tarjeta de financiación 104 (bloque 411) a través de la red de pagos para una autorización de pago convencional.

El emisor de tarjeta de financiación 104, a continuación, puede autorizar, o no, la solicitud de pago y responde con un código de autorización al adquirente del emisor de tarjeta virtual, a través de la red de pagos, que, a su vez, notifica al emisor de tarjeta virtual. El emisor de tarjeta virtual notifica al adquirente de comerciante usando un código de autorización correspondiente para el sistema de comerciante a través de la red de pagos.

Para liquidar los fondos (no mostrado), el comerciante iniciará, o el adquirente de comerciante iniciará en nombre del comerciante, una solicitud de liquidación a la red de pagos a través del adquiriente de comerciante. La red de pagos reenviará las correspondientes transacciones de tarjeta virtual para liquidar al emisor de tarjeta virtual. Cuando el

emisor de tarjeta virtual recibe las transacciones, el emisor de tarjeta virtual enviará una solicitud de liquidación para las transacciones de tarjeta de financiación correspondientes a su propio adquirente. La solicitud de liquidación se enviará al emisor de tarjeta de financiación apropiado por la red de pagos. El emisor de la tarjeta de financiación recibe la solicitud de liquidación de transacciones, y enviará los fondos asociados con todas las transacciones coincidentes al originador de la transacción de pago, en este caso, el emisor de tarjeta virtual. Cuando el emisor de tarjeta virtual recibe los fondos, el emisor de tarjeta virtual enviará los fondos correspondientes al comerciante.

En una realización de ejemplo, el emisor de tarjeta virtual 401, el operador de tarjeta virtual 402 y el adquirente de tarjeta virtual 403 están representados por la misma entidad, denominada en el presente documento como el servidor de pasarela de pagos. El propio servidor de pasarela de pagos puede incluir uno o más servidores. Por ejemplo, cada una de las entidades 401, 402, 403 pueden ser servidores individuales que, combinados, forman el servidor de pasarela de pagos.

Volviendo a la Figura 5, se muestran componentes de realización de ejemplo de un sistema para facilitar el pago usando la tarjeta virtual. El usuario 101 tiene una o más tarjetas de financiación 505 pre-registradas en su monedero en la nube (proceso no mostrado). Por ejemplo, el usuario tiene múltiples tarjetas de financiación. El usuario 101 también posee un dispositivo móvil habilitado para NFC 501, que incluye una aplicación de pagos. El dispositivo móvil 501 está configurado para interactuar, a través de NFC, con un dispositivo de terminal de POS de comerciante 502. El dispositivo terminal de POS de comerciante 502 está en comunicación de datos a través del sistema de pagos de comerciante con el adquirente de comerciante 103 (por ejemplo, un servidor), el adquirente de comerciante y el servidor de pasarela de pagos 506 están en comunicación con una red de pagos (por ejemplo, Visa, MasterCard, Discover, etc.), que está configurada para enviar datos relacionados con pagos y transacciones a partes relevantes, incluyendo el servidor de pasarela de pagos 506 y el emisor de tarjeta de financiación 104 (por ejemplo, un servidor). La comunicación entre el dispositivo terminal de POS de comerciante 502, el adquirente de comerciante 103, la red de pagos 504, el servidor de pasarela de pagos 505 y el emisor de tarjeta de financiación 104 puede tener lugar a través de redes de comunicación alámbricas o inalámbricas, o ambas.

El servidor de pasarela de pagos 506 también está en comunicación con el dispositivo móvil 501 a través de una red inalámbrica. Por ejemplo, la red inalámbrica se proporciona por un operador de telefonía móvil.

Los componentes de ejemplo del servidor de pasarela de pagos 506 se muestran en el bloque 507. El servidor 506 puede incluir el emisor de tarjeta virtual 401, el operador de tarjetas virtual 402 y el adquirente de tarjetas virtual 403. Durante un proceso de registro realizado por el usuario 101, el servidor de pasarela de pagos 506 almacena el número de identificación personal (PIN) seleccionado por el usuario, datos de tarjeta de financiación en asociación con el ID de dispositivo móvil del usuario (por ejemplo, en la base de datos 508). Por ejemplo, el PIN de usuario, la tarjeta de financiación 1 y la tarjeta de financiación 2 (y otras tarjetas de financiación) se almacenan en asociación con el ID de dispositivo móvil del dispositivo móvil 501. También, en la base de datos 509, se almacenan las asociaciones de datos temporales entre una tarjeta de financiación dada, una tarjeta virtual y un código de autorización cuando es aplicable. Por ejemplo, la tarjeta virtual 1, la tarjeta de financiación 1 y el código de autorización 1 se almacenan todos en asociación entre sí. Otro ejemplo es que la tarjeta virtual 2 y la tarjeta de financiación 2 que también están asociadas, pero no tienen código de autorización emitido todavía para el par de tarjetas. En una realización de ejemplo, aún no se ha emitido ningún código de autorización porque el usuario aún no ha tocado en el dispositivo móvil usando la tarjeta de financiación 2 (por ejemplo, tarjeta realmente virtual 2), o porque la autorización de pago del comerciante se interrumpió de tal manera que el servidor de pasarela de pagos nunca recibió el código de autorización.

Volviendo a la Figura 6, se muestran componentes de ejemplo del dispositivo móvil 501. El dispositivo móvil 501 incluye un procesador principal 601 que interactúa con un número de componentes que incluyen, entre otras cosas, entradas/salidas auxiliares 302, un puerto de datos 603, un teclado 604, un altavoz 605 (por ejemplo, un altavoz de audio), un micrófono 606, un receptor de GPS 607 y una cámara 608. El dispositivo móvil 501 también incluye un subsistema de NFC 609, un elemento seguro 622 que puede o no tener también conectividad directa a los subsistemas de NFC 609 y otros subsistemas de dispositivo 611.

El dispositivo móvil 501 usa un sistema de comunicación 613 para interactuar con una red inalámbrica 612. Los tipos de memoria incluyen la memoria flash 614 y la pantalla del dispositivo móvil de memoria de acceso aleatorio (RAM) 616 puede ser una pantalla de tipo pantalla táctil u otro tipo de pantalla.

Puede usarse un sistema operativo 617 para gestionar y ejecutar componentes de software 618. Los componentes o aplicaciones de software incluyen un navegador web o navegador de Internet 619 y la aplicación de pagos 620. Se incluyen otros componentes de software 621.

El elemento seguro 622 puede usarse para almacenar información tal como elementos de aplicación y datos, por ejemplo, una aplicación de pagos y un identificador móvil. En una realización de ejemplo, el elemento seguro está dentro de una tarjeta de módulo de identidad de abonado (SIM). Los ejemplos no limitantes de dispositivos móviles incluyen teléfonos celulares, teléfonos inteligentes, PDA, tabletas, portátiles y ordenadores portátiles.

Se apreciará que, cualquier módulo o componente ejemplificado en el presente documento que ejecuta instrucciones

u operaciones puede incluir o tener acceso de otro modo a medios legibles por ordenador tales como medios de almacenamiento, medios de almacenamiento informático o dispositivos de almacenamiento de datos (extraíbles y/o no extraíbles) tales como, por ejemplo, discos magnéticos, discos ópticos o cinta. Los medios de almacenamiento informático pueden incluir medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier método o tecnología para el almacenamiento de información, tal como instrucciones legibles por ordenador o procesador, estructuras de datos, módulos de programa u otros datos, excepto señales de propagación transitorias *per se*. Los ejemplos de medios de almacenamiento informático incluyen RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro almacenamiento óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar la información deseada y al que pueda accederse por una aplicación, módulo o ambos. Cualquier medio de almacenamiento informático de este tipo puede ser parte de uno cualquiera de los servidores 103, 504, 104, 506, 401, 402, 403, el dispositivo móvil 501, el terminal de POS 502, etc. o accesible o conectable a los mismos. Cualquier aplicación o módulo descrito en el presente documento puede implementarse usando instrucciones u operaciones legibles/ejecutables por ordenador o procesador que pueden almacenarse o mantenerse de otro modo por tales medios legibles por ordenador.

Volviendo a la Figura 7, se proporcionan instrucciones ejecutables por ordenador o implementadas por procesador de ejemplo para facilitar una transacción entre un dispositivo móvil 501 y un dispositivo terminal de POS 502.

Se supone que el usuario final tiene un dispositivo móvil de NFC compatible 501. Se supone que la aplicación de pagos 620 se ha instalado en el dispositivo móvil 501. Se supone que el usuario final se ha registrado para el servicio.

Después de que el comerciante capture los detalles de la transacción de compra en su sistema de punto de venta, el dispositivo terminal de POS habilitado para NFC 502 visualiza un mensaje al usuario final para "tocar" para pagar (bloque 701). Por ejemplo, el usuario puede tocar su dispositivo móvil 501 o una tarjeta de financiación sin contacto. Los ejemplos descritos en el presente documento se refieren a tocar el dispositivo móvil 501.

El usuario final 101 ve el mensaje desde el dispositivo terminal de POS 502 e inicia la aplicación de pagos 620 en el dispositivo móvil 501 (bloque 702). Por ejemplo, el usuario selecciona un icono para la aplicación de pagos 620 en la pantalla del dispositivo móvil 501, lanzando de esta manera la aplicación de pagos 620. La aplicación de pagos 620 determina si el usuario se ha registrado satisfactoriamente en el servicio (bloque 703), y, en caso afirmativo, muestra un menú (bloque 704) de acciones soportadas por la aplicación. Si el usuario no se ha registrado, el menú ofrece al usuario que se registre con el servicio (por ejemplo, registrar una o más tarjetas de financiación, proporcionar un PIN, vincular un identificador de dispositivo móvil al registro de registro).

Una interfaz gráfica de usuario (GUI) en el menú puede recibir una entrada del usuario para iniciar un pago con una tarjeta virtual con la aplicación de pagos (bloque 705). Ejemplo de otro elemento de menú incluye "añadir una tarjeta de financiación", "borrar una tarjeta de financiación", etc.

El dispositivo móvil 501 visualiza a continuación las tarjetas de financiación que se han pre-registrado por el usuario (bloque 706). Se proporciona una entrada de usuario para seleccionar una de las tarjetas de financiación (bloque 707). En una realización de ejemplo, la información de tarjeta de financiación visualizada se carga después de que el usuario final se registre satisfactoriamente en el servicio y haya registrado al menos una tarjeta de financiación. La lista se actualiza cuando el usuario añade una tarjeta de financiación adicional en la aplicación de pagos o cuando se borra una tarjeta de financiación. Para cada tarjeta de financiación registrada, hay un correspondiente registro almacenado en la aplicación de pagos 620 y en la base de datos de servidor de pasarela de pagos 508 que incluye un identificador para la red de pagos asociada con la tarjeta de financiación, un identificador de tarjeta de financiación, etc.

La aplicación de pagos 620 envía el identificador de dispositivo móvil al servidor de pasarela de pagos 506 (bloque 708). La aplicación de pagos 620 también envía el tipo de transacción (acción seleccionada en el menú de aplicación, en este caso, "Pagar con una tarjeta virtual") y el identificador para la tarjeta de financiación seleccionada al servidor de pasarela de pagos 506 (bloque 709). Basándose en la información recibida por el dispositivo móvil 501, el servidor de pasarela de pagos 506 crea y calcula los detalles con respecto a la tarjeta virtual (bloque 710). En particular, el servidor de pasarela de pagos 506 calcula un PAN virtual, una fecha de caducidad de la tarjeta virtual y todos o algunos de los elementos de datos que forman los datos de la pista dos. Se observa que, los datos de la pista dos incluyen, entre otras cosas: el PAN, un código de servicio, una fecha de caducidad, datos discrecionales y un LRC. En una realización de ejemplo, el servidor de pasarela de pagos 506 en este momento no calcula los datos discrecionales, que son de naturaleza dinámica (por ejemplo, los datos discrecionales son datos dinámicos). En una realización de ejemplo, la fecha de caducidad de la tarjeta virtual es idéntica a la fecha de caducidad de la tarjeta de financiación, de modo que, desde la perspectiva del comerciante y del usuario, la tarjeta virtual es idéntica a la tarjeta de financiación. De hecho, basándose en ciertas similitudes entre la tarjeta de financiación y la tarjeta virtual, el comerciante y el usuario no serán conscientes de que se está generando y usando una tarjeta virtual y, en su lugar, creerán que la tarjeta de financiación se está usando en el pago. Los detalles de la tarjeta virtual pueden incluir además una fecha de caducidad interna que es conocida únicamente por el servidor de pasarela de pagos, y tiene una línea de tiempo corta de aproximadamente unos pocos días desde la fecha en la que se crea la tarjeta virtual. La fecha de caducidad interna es diferente de la fecha de caducidad de la tarjeta virtual, y la función de la fecha de caducidad interna es proporcionar

un indicador adicional a la pasarela de pagos para determinar si una tarjeta virtual ha caducado o no. El servidor de pasarela de pagos 506 cifra los datos de tarjeta virtual, que no incluyen la fecha de caducidad interna, y envía la carga útil de tarjeta virtual cifrada a la aplicación de pagos del dispositivo móvil 620 (bloque 711).

Como una realización de ejemplo alternativa, en lugar de que el servidor de pasarela de pagos 506 envíe el PAN de tarjeta virtual como parte de la carga útil de tarjeta virtual cifrada al dispositivo móvil, el servidor de pasarela de pagos 506, en su lugar, envía un valor de clave (llamado Kpan) que el dispositivo móvil puede usar para generar un PAN de tarjeta virtual idéntico según lo calculado por el servidor de pasarela de pagos 506.

En una realización de ejemplo, los últimos cuatro dígitos del PAN de tarjeta virtual son los mismos que los últimos cuatro dígitos del PAN de tarjeta de financiación. Los últimos cuatro dígitos del PAN de tarjeta virtual son idénticos al PAN de tarjeta de financiación de modo que, después del truncamiento de PAN, parece como si el PAN de la tarjeta virtual fuera idéntico al PAN de la tarjeta de financiación. En otras palabras, el usuario no puede detectar que se está usando una tarjeta virtual en lugar de una tarjeta de financiación. A modo de antecedentes, el truncamiento de PAN se aplica por la industria de pago como parte del proceso de certificación de comerciante para aceptar pago de tarjeta. Un PAN truncado significa que el número de tarjeta, cuando se imprime en un recibo de cliente, se reemplaza con una impresión de únicamente los últimos cuatro dígitos, y el resto de los otros dígitos de PAN se reemplazan normalmente por asteriscos. Una realización de ejemplo de un PAN truncado es **** **** **** 7777. Esto oculta el número de tarjeta de cualquiera que obtenga el recibo cuando se descarta, o por otros medios, mientras aún permite que un titular de tarjeta con múltiples tarjetas identifique cuál se usó y, por lo tanto, registre la transacción.

En una realización de ejemplo, la primera porción de dígitos del PAN de la tarjeta virtual es estática y se refiere al servidor de pasarela de pagos 506. Por ejemplo, los primeros seis dígitos apuntan al servidor de pasarela de pagos 506; el adquiriente de comerciante 103 y la red de pagos asociada usan esta información para enviar los detalles de transacción y pago al servidor de pasarela de pagos 506.

En una realización de ejemplo, el PAN de la tarjeta virtual tiene una longitud de diecinueve dígitos y cumple con el algoritmo LUHN-10. El algoritmo, también conocido como el algoritmo de "módulo 10" o "mod 10", es una fórmula de suma de comprobación usada para validar una diversidad de números de identificación, tales como números de tarjeta. Como se ha descrito anteriormente, los primeros seis dígitos se usan para identificar el servidor de pasarela de pagos y los últimos cuatro dígitos son idénticos a los últimos cuatro dígitos del PAN de tarjeta de financiación. Los dígitos restantes se pueden calcular de varias maneras. En una realización de ejemplo, los dígitos restantes del PAN de tarjeta virtual se generan aleatoriamente. En otra realización de ejemplo, los dígitos restantes se calculan usando el valor de Kpan; en la Figura 11 se describen detalles adicionales a este respecto. Pueden usarse otros métodos para calcular el PAN de tarjeta virtual.

El dispositivo móvil 501 recibe la carga útil de tarjeta virtual cifrada, descifra la comunicación cifrada y extrae los detalles de tarjeta virtual (por ejemplo, el PAN de tarjeta virtual y otros detalles de tarjeta).

En otra realización de ejemplo, si la carga útil de tarjeta virtual incluye un Kpan (por ejemplo, un valor de clave) en lugar de un PAN de tarjeta virtual, el dispositivo móvil 501 usa el Kpan para calcular el PAN de tarjeta virtual.

La aplicación de pagos 620 en el dispositivo móvil 501 visualiza una GUI que solicita al usuario 101 que introduzca su PIN (por ejemplo, que debería ser el mismo PIN proporcionado cuando el usuario se registró para el servicio) (bloque 712). La aplicación 620 recibe el PIN del usuario 101 (por ejemplo, el usuario introduce el PIN) (bloque 713). La aplicación 620 usa el PIN para calcular los datos discrecionales de la tarjeta virtual (bloque 714). Con los datos discrecionales calculados, el conjunto de datos de la pista dos está completo. El conjunto de datos de tarjeta virtual (por ejemplo, los datos de la pista dos) se entrega al elemento seguro 622 del dispositivo móvil (bloque 715). En una realización de ejemplo, los datos a enviar a través del subsistema de NFC 609 necesitan proporcionarse por el elemento seguro 622 (bloque 716). En otra realización de ejemplo, aunque no se muestra, el sistema operativo del dispositivo móvil 501 puede transferir directamente información al subsistema de NFC 609 sin el uso del elemento seguro. El conjunto de datos de tarjeta virtual incluye el PAN de tarjeta virtual, la fecha de caducidad, los datos discrecionales y todos los otros elementos en un conjunto de datos de pista dos para completar una transacción de pago sin contacto convencional. La aplicación de pagos del móvil 620 visualiza un mensaje al usuario para "Tocar para pagar" (bloque 717).

En esta etapa, el usuario 101 toca o coloca el dispositivo móvil 501 muy cerca del dispositivo terminal de POS 502 (bloque 718). Cuando el dispositivo móvil 501 entra en el alcance de comunicación con el dispositivo terminal de POS 502, el dispositivo móvil 501 envía los datos de tarjeta virtual al dispositivo terminal de POS 502, usando el subsistema de NFC 609 del dispositivo móvil (bloque 719) siguiendo la norma de red de pagos para tal transacción de pago sin contacto. La transferencia de datos se produce usando medios de comunicación por radio. En una realización de ejemplo, el dispositivo terminal de POS 502 visualiza un mensaje al usuario 101 para "Retirar tarjeta" (bloque 720) una vez que el terminal ha recibido todos los datos de tarjeta que necesitaba. El usuario coloca el dispositivo móvil 501 lejos del dispositivo terminal de POS (bloque 721). Pueden tener lugar otros cálculos y procesos dentro del dispositivo móvil 501 que completa la participación del dispositivo móvil en el proceso de transacción (bloque 722).

Aunque no se muestra en la Figura 7, el dispositivo terminal de POS 502 enviará los detalles de tarjeta virtual al adquirente de comerciante, junto con otros datos de transacción (por ejemplo, coste por transacción, ID de comerciante, etc.). Esta información se enruta eventualmente al servidor de pasarela de pagos 506, como se identifica por la primera porción de dígitos del PAN de la tarjeta virtual. Véase la figura 8 para más detalles.

En una realización de ejemplo, puede usarse un PIN para todas las tarjetas de financiación asociadas con el dispositivo móvil. En otra realización de ejemplo, el proceso de registro puede solicitar un PIN específico para cada tarjeta de financiación. En otras palabras, si un usuario selecciona una tarjeta de financiación diferente, el usuario necesitará introducir un PIN diferente.

En una realización de ejemplo preferida, la aplicación de pagos del dispositivo móvil 620 no verifica el PIN. En su lugar, el PIN se verifica indirecta o implícitamente por el servidor de pasarela de pagos 506 cuando se verifica el conjunto de datos de tarjeta virtual. En otras palabras, el servidor de pasarela de pagos 506 usa el PIN que se almacenó en el momento de registro para calcular el conjunto de datos de tarjeta virtual. Si se proporcionó un PIN incorrecto por el usuario o un adversario durante la transacción, hará que los datos virtuales calculados den como resultado un valor diferente, incorrecto, en comparación con los datos de tarjeta virtual calculados por el servidor de pasarela de pagos. Una vez que el conjunto de datos de tarjeta virtual recibido se compara con el valor esperado por el servidor, puede detectarse una entrada de PIN no válida. Cuando el servidor de pasarela de pagos recibe y verifica el conjunto de datos de tarjeta virtual y detecta un conjunto de datos de tarjeta virtual inesperado (por ejemplo, debido al PIN incorrecto), a continuación, puede declinarse la autorización de pago.

Volviendo a la figura 8, se proporcionan instrucciones ejecutables por ordenador o implementadas por procesador de ejemplo para facilitar una transacción entre un dispositivo móvil 501 y un dispositivo terminal de POS 502, incluyendo detalles adicionales con respecto al procesamiento de datos por el adquiriente de comerciante 103, el servidor de pasarela de pagos 506 y servidor emisor de tarjeta de financiación 104.

Los bloques 701, 718, 719, 720 y 721 se muestran de nuevo para proporcionar contexto para el proceso. Después de que el dispositivo terminal de POS 502 recibe los datos de tarjeta virtual desde el dispositivo móvil 501 (bloque 719), el dispositivo terminal de POS 502 envía los datos de tarjeta virtual, la información de transacción (por ejemplo, cantidad de pago) y otra información (por ejemplo, ID de comerciante) al adquirente de comerciante 103 (bloque 801). En una realización de ejemplo, los datos enviados por el dispositivo terminal de POS 502 están en un formato de solicitud de autorización de pago convencional.

El adquiriente de comerciante 103 envía la solicitud de autorización de pago, que incluye al menos los datos de tarjeta virtual (por ejemplo, datos de pista dos de la tarjeta virtual) y la cantidad de pago, al servidor de pasarela de pagos 506 (bloque 802) a través de la red de pagos. El adquirente 103 y la red de pagos pueden identificar el servidor de pasarela de pagos 506 por la primera porción de dígitos en el PAN de la tarjeta virtual. Puede apreciarse que el PAN es parte de los datos de la pista dos.

El servidor de pasarela de pagos 506 valida los datos de tarjeta virtual (bloque 803). Para validar los datos de tarjeta virtual recibidos desde el dispositivo móvil (a través del adquirente de comerciante 103), el servidor de pasarela de pagos calcula el conjunto de datos de pista dos por sí mismo. El cálculo de datos de pista dos incluye que el servidor de pasarela de pagos calcule los datos discrecionales usando el PIN originalmente recibido y almacenado durante el registro por el usuario. En una realización de ejemplo, se precalcularon y almacenaron algunas de las porciones de datos de la pista dos (como el PAN y la fecha de caducidad); estas porciones de datos precalculadas pueden compararse con los datos de pista dos recibidos. Si los datos de tarjeta virtual se validan satisfactoriamente (el conjunto de datos de la pista dos de la tarjeta recibida coincide con el conjunto de datos de pista dos de la tarjeta calculados por el servidor de la pasarela de pagos), a continuación, el servidor de la pasarela de pagos recupera los datos de tarjeta de financiación que están asociados con la tarjeta de datos de la tarjeta virtual (bloque 804).

La validación de los datos de tarjeta virtual en el bloque 803 también puede incluir verificar si ha pasado o no la fecha de caducidad interna asociada con la tarjeta virtual. Si la fecha actual de la validación se produce antes o en la fecha de caducidad interna, a continuación, la tarjeta virtual puede considerarse validada y el procesamiento de la transacción puede continuar. De lo contrario, la tarjeta virtual se considera no válida y se deniega la solicitud de autorización de pago.

Si se valida la tarjeta virtual, el servidor de pasarela de pagos 506, que desempeña una función que es similar al de un comerciante en ese punto, envía una solicitud de autorización de pago a su propio adquirente, donde la autorización de pago incluye al menos los datos de la tarjeta de financiación y la misma cantidad de pago recibida en el bloque 802, al servidor emisor de tarjeta de financiación 104 (bloque 805) a través de la red de pagos. El emisor de tarjeta de financiación 104 recibe a continuación la solicitud de autorización de pago y procesa la transacción como norma. Una vez que se procesa la transacción, el emisor de tarjeta de financiación 104 envía un código de autorización de pago al servidor de pasarela de pagos (bloque 806) a través de la red de pagos. La respuesta de código de autorización incluye si se ha aceptado o denegado la autorización de pago, un número de identificación de transacción, etc.

El servidor de pasarela de pagos 506 envía a continuación una respuesta de autorización de pago correspondiente al

adquirente de comerciante 103 (bloque 807) a través de la red de pagos, y el adquirente 103 envía la respuesta de autorización de pago al dispositivo terminal de POS 502 (bloque 808) también a través de la red de pagos. Aunque no se muestra, el servidor de pasarela de pagos almacena el código de autorización de pago en la base de datos 509. Aunque no se muestra también, el dispositivo terminal de POS 502 puede visualizar un mensaje al usuario final de que el pago ha sido aceptado o denegado, de acuerdo con la respuesta.

En una realización de ejemplo, el servidor de pasarela de pagos 506 también puede enviar una confirmación al dispositivo móvil 501 que indica si el pago fue aceptado o denegado o no (bloque 809). La indicación puede enviarse como datos específicos a la aplicación de pagos 620 en el dispositivo móvil, o como un correo electrónico. Después de recibir tal indicación, el dispositivo móvil 501 puede visualizar un mensaje al usuario de acuerdo con la indicación.

En una realización de ejemplo, después de que el servidor de pasarela de pagos 506 recibe una respuesta de que se ha procesado el pago (bloque 806), el servidor de pasarela de pagos 506 marca la tarjeta virtual como en uso. De esta manera, si la misma tarjeta virtual se usa de nuevo en una transacción futura, el servidor de pasarela de pagos rechazará la transacción. Esto se debe a que la tarjeta virtual está destinada a usarse únicamente una vez.

En otra realización de ejemplo, la misma tarjeta virtual puede usarse para más de una transacción.

Volviendo a la Figura 9a, se proporciona una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para facilitar una transacción usando una tarjeta virtual. En una realización de ejemplo, las instrucciones de la Figura 9a son una implementación detallada de ejemplo de los bloques 710 y 711. En la realización de ejemplo, el número de tarjeta virtual (también denominado el PAN de la tarjeta virtual), la fecha de caducidad de la tarjeta virtual y los otros datos se calculan todos por el servidor de pasarela de pagos 506. También se proporcionan detalles que explican el flujo de datos entre el servidor emisor de tarjeta virtual 401, el operador de tarjeta virtual 402 y el adquirente de tarjeta virtual 403. Las entidades 401, 402, 403 pueden ser parte del servidor de pasarela de pagos 506. En otra realización de ejemplo, las entidades 401, 402, 403 son entidades separadas.

Las operaciones en los bloques 901 a 908 son parte del proceso global para que el dispositivo móvil obtenga una tarjeta virtual (bloque 909).

El proceso en la Figura 9a supone que el dispositivo móvil 501 tiene la aplicación de pagos 620 instalada, y que el dispositivo móvil y las tarjetas de financiación se han registrado con el servidor de pasarela de pagos 506. También se supone que ya se ha iniciado una transacción con el comerciante. Por ejemplo, el dispositivo terminal de POS 502 ha visualizado el mensaje "Tocar para pagar", y el usuario ya ha seleccionado una tarjeta de financiación a través de la aplicación de pagos 620. Estas condiciones se logran usando, por ejemplo, los bloques 701, 702, 703, 704, 705, 706 y 707.

Después de recibir una entrada de usuario para seleccionar una tarjeta de financiación, el dispositivo móvil 501 envía el tipo de transacción (acción seleccionada en el menú de aplicación, en este caso, "Pagar con una tarjeta virtual") y un identificador de tarjeta de financiación. En una realización de ejemplo preferida, el identificador de tarjeta de financiación se determina en el momento del registro.

El operador de tarjeta virtual 402 confirma que la tarjeta de financiación seleccionada es válida (bloque 902) garantizando, por ejemplo, que el identificador de tarjeta de financiación está vinculado con el usuario registrado y que la tarjeta de financiación seleccionada no ha expirado desde su registro.

El operador de tarjeta virtual 402 envía una solicitud para crear un PAN de tarjeta virtual al servidor de emisión de tarjeta virtual 401 (bloque 903). La solicitud para el PAN de tarjeta virtual incluye los últimos cuatro dígitos del PAN de tarjeta de financiación y la fecha de caducidad de la tarjeta de financiación. El servidor de emisión de tarjeta virtual crea un PAN de tarjeta virtual que tiene los últimos cuatro dígitos idénticos a los últimos cuatro dígitos del PAN de tarjeta de financiación. La tarjeta virtual también tiene la misma fecha de caducidad y la tarjeta de financiación. El PAN virtual se crea usando los primeros 6 dígitos asignados al emisor de tarjeta virtual, un número aleatorio de 8 dígitos de longitud único, nunca usado antes (para evitar colisiones), y el dígito mod10 de comprobación.

Después de que se calcula el PAN de tarjeta virtual, el servidor de emisión de tarjeta virtual 401 envía esta información, en una respuesta, al operador de tarjeta virtual 402 (bloque 904). El operador de tarjeta virtual generará porciones de los datos de la pista dos tales como el Pan, la caducidad de la tarjeta, el código de servicio, etc. (bloque 905). En una realización de ejemplo, los datos discrecionales (que son parte de los datos de pista dos) no se calculan por el servidor de pasarela de pagos 506 en este momento. El operador de tarjeta virtual 402 asocia el PAN de tarjeta virtual con la tarjeta de financiación (bloque 906) y lo almacena en la base de datos 509 (no mostrada). También añade una fecha de caducidad interna a los registros de tarjeta virtual en la base de datos. En una realización de ejemplo, la fecha de caducidad interna se calcula para ser algún periodo de tiempo predeterminado después del tiempo en el que se crea la tarjeta virtual. Por ejemplo, la fecha de caducidad interna es 48 horas desde la fecha y hora en que se crea la tarjeta virtual. El operador de tarjeta virtual 402 a continuación cifra y envía los datos de tarjeta virtual (por ejemplo, PAN de tarjeta virtual, fecha de caducidad externa, etc.) requeridos por la aplicación móvil para generar el conjunto de datos de tarjeta virtual final (bloque 907). El resultado forma una carga útil de tarjeta virtual cifrada que se envía al dispositivo

móvil 501 (bloque 908).

El dispositivo móvil 501 recibe el PIN del usuario (bloque 925). El dispositivo móvil 501 usa a continuación el PIN para calcular los datos discrecionales (que son una porción de los datos de pista dos de la tarjeta virtual). El cálculo de los datos discrecionales puede implicar un valor dinámico que cambia con el tiempo, o con cada transacción, haciendo de esta manera que los datos discrecionales sean los datos dinámicos. Los datos recibidos de la carga útil de tarjeta virtual (por ejemplo, PAN, fecha de caducidad y otros datos) y los datos discrecionales forman el conjunto de datos de pista dos completo de la tarjeta virtual (bloque 926).

Volviendo a la Figura 9b, se proporciona una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para validar y autorizar una transacción usando una tarjeta virtual. El proceso en la Figura 9b supone que ya se creó una tarjeta virtual (por ejemplo, según la Figura 9a) y se centra en el procesamiento para verificar la tarjeta virtual. En una realización de ejemplo, las instrucciones de la Figura 9a son una implementación detallada de ejemplo de los bloques 802 a 807. Las entidades 401, 402, 403 pueden ser parte del servidor de pasarela de pagos 506. En otra realización de ejemplo, las entidades 401, 402, 403 son entidades separadas.

Los procesos descritos con respecto a los bloques 910 a 923 son parte del proceso de autorización global de la tarjeta virtual (bloque 924).

El flujo comienza después de que el dispositivo móvil 501 haya recibido la carga útil de tarjeta virtual cifrada, descifrado la carga útil de tarjeta virtual, capturado a través de la GUI el PIN del usuario, y calculado el conjunto de datos de tarjeta virtual completo (por ejemplo, el conjunto de datos de pista dos completo). En ese punto, la aplicación móvil puede enviar el conjunto de datos de tarjeta virtual al dispositivo terminal de POS 502 a través del subsistema de NFC 609 (bloque 910). El dispositivo terminal de POS 502 envía los datos de tarjeta virtual, junto con datos de transacción, al adquirente de comerciante 103 (bloque 911). El adquiriente de comerciante 103 envía una solicitud de autorización de pago, que incluye los datos de tarjeta virtual y la cantidad de pago, al servidor de emisión de tarjeta virtual 401 (bloque 913) a través de la red de pagos.

El servidor de emisión de tarjeta virtual 401 envía los datos de tarjeta virtual al operador de tarjeta virtual 402 (bloque 914). El operador de tarjeta virtual 402 usa los datos de tarjeta virtual, tal como el PAN de tarjeta virtual, para recuperar el perfil de usuario asociado y datos de tarjeta de financiación (por ejemplo, PAN y fecha de caducidad) (bloque 915). El operador de tarjeta virtual 402 a continuación verifica los datos de tarjeta virtual recibidos, por ejemplo, comparando datos con la versión calculada de servidor de los datos de tarjeta esperados. El proceso de validación es similar a la operación del bloque 803.

Si los datos de tarjeta virtual se verifican satisfactoriamente, a continuación, el operador de tarjeta virtual 402 usa los detalles de tarjeta de financiación asociados con la transacción de tarjeta virtual y envía una solicitud de autorización de pago, que incluye los datos de tarjeta de financiación y la cantidad de pago correspondiente, al adquirente de tarjeta virtual 403. El adquirente de tarjeta virtual 403 reenvía los detalles al servidor de emisión de tarjetas de financiación 104 (bloque 917) a través de la red de pagos.

El servidor de emisión de tarjetas de financiación 104 recibe y verifica los datos de tarjeta de financiación. Si los datos de tarjeta de financiación se verifican satisfactoriamente, el servidor emisor de tarjeta de financiación envía una respuesta de código de autorización de pago al adquirente de tarjeta virtual 403, que reenvía la misma al operador de tarjeta virtual 402 (bloque 918), todo a través de la red de pagos. La respuesta de código de autorización de pago indica si se aceptan o deniegan los datos de tarjeta de financiación, y un número de identificación de transacción, etc.

El operador de tarjeta virtual 402 envía una correspondiente respuesta de código de autorización de validación al servidor de emisión de tarjeta virtual 401 (bloque 919). El operador de tarjeta virtual 402 y el servidor de emisión de tarjeta virtual 401 marcan la tarjeta virtual como en uso (bloque 920 y bloque 921). De esta manera, si la misma tarjeta virtual se usa de nuevo en un momento posterior, el operador de tarjeta virtual 402 o el servidor de emisión de tarjeta virtual 401 podrá detectar un posible fraude.

El servidor de emisión de tarjeta virtual 401 envía la respuesta de código de autorización de pago para la tarjeta virtual al operador de tarjeta virtual 402 (bloque 922). Esta respuesta de código de autorización de pago para la tarjeta virtual se reenvía a continuación al adquiriente de comerciante 103 (bloque 923) a través de la red de pagos.

Como se ha descrito anteriormente, en otras realizaciones de ejemplo, la tarjeta virtual no se calcula para cada transacción. Por ejemplo, después de que se calcula la tarjeta virtual de acuerdo con los bloques 708, 709, 710, 711, 712, 713 y 714, para una o más transacciones posteriores, puede usarse la misma tarjeta virtual para la transacción. En otras palabras, los bloques 708, 709, 710, 711, 712, 713 y 714 no se realizan para la una o más transacciones posteriores. Esto ahorra potencia de procesamiento y reduce el tiempo de cálculo cuando se realiza una transacción. Esto también puede ser ventajoso cuando el dispositivo móvil 501 no puede comunicarse con el servidor de pasarela de pagos 506. En otras palabras, incluso si el dispositivo móvil 501 no puede comunicarse con el servidor de pasarela de pagos 506, el dispositivo móvil puede usar la tarjeta virtual ya calculada para realizar la transacción.

En una realización de ejemplo donde se usa la misma tarjeta virtual para transacciones posteriores, ciertos eventos, o periodos de tiempo, o ambos pueden desencadenar que se calcule y cargue una nueva tarjeta virtual en el dispositivo móvil 501. En una realización de ejemplo, se calcula una nueva tarjeta virtual cuando se ha realizado un número dado de transacciones usando la tarjeta virtual anterior, y cuando el dispositivo móvil 501 puede comunicarse con el servidor de pasarela de pagos 506. El número dado de transacciones es, por ejemplo, un número generado aleatoriamente que se genera cada vez que se emite una nueva tarjeta virtual al dispositivo móvil 501. En otra realización de ejemplo, se calcula una nueva tarjeta virtual para una transacción cuando ha pasado un número dado de días desde que se calculó la tarjeta virtual anterior, y cuando el dispositivo móvil 501 puede comunicarse con el servidor de pasarela de pagos 506. El número de días dado es, por ejemplo, un número generado aleatoriamente que se genera cada vez que se emite una nueva tarjeta virtual al dispositivo móvil 501. Puede apreciarse que, los números generados aleatoriamente evitan que los atacantes predigan cuándo se calculará la siguiente tarjeta virtual nueva para el dispositivo móvil.

Volviendo a la Figura 10, se proporciona una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para registrar una tarjeta de financiación y un dispositivo móvil con un servidor de pasarela de pagos. Una realización de este tipo puede usarse en combinación con los principios descritos anteriormente, y se usa en la invención. El dispositivo móvil 501 envía una solicitud de registro al servidor de pasarela de pagos 506 (bloque 1001). La solicitud incluye el ID de dispositivo del dispositivo móvil, un PIN proporcionado por el usuario y detalles de la tarjeta de financiación. Después de recibir la solicitud, el servidor de pasarela de pagos envía una respuesta de registro al dispositivo móvil (bloque 1002). La respuesta incluye un certificado, un contador de transacciones de aplicación (ATC), un valor de clave (llamado Kpan) para generar un PAN, un valor de clave de elemento seguro (llamado Ksec) y un identificador de tarjeta de financiación que identifica cada tarjeta o tarjetas de financiación registradas. El certificado es un certificado de cliente para el dispositivo móvil 501 y, en una realización de ejemplo, está configurado de acuerdo con el algoritmo de RSA y tiene una longitud de 2048 bits. El ATC es un contador que se establece inicialmente a un valor aleatorio entre "0" o "1000" y se incrementa con cada transacción. El valor de ATC inicializado es un valor aleatorio para evitar que los adversarios predigan los valores de ATC. Se almacenan copias del ATC y se sincronizan tanto en el servidor de pasarela de pagos como en el dispositivo móvil. En una realización de ejemplo, el ATC es un valor de 10 dígitos. En una realización de ejemplo, el Kpan tiene una longitud de 128 bits y el Ksec tiene una longitud de 128 bits.

El servidor de pasarela de pagos 506 almacena los datos de la solicitud de registro y la respuesta de registro en asociación entre sí (bloque 1003). El dispositivo móvil 501 también almacena los datos de la respuesta de registro (bloque 1004).

Volviendo a la figura 11, se proporciona una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para calcular datos de tarjeta virtual. Una realización de este tipo puede usarse en combinación con los principios descritos anteriormente para calcular datos de tarjeta virtual, y se usa en la invención. El dispositivo móvil 501 envía una solicitud de tarjeta virtual para vincular el servidor de pasarela de pagos 506 (bloque 1101). Esto es similar al bloque 901 en la Figura 9a. La solicitud incluye el ID de dispositivo, el identificador de la tarjeta de financiación seleccionada, el certificado y el Kpan almacenado. El Kpan almacenado puede ser del registro o de la transacción anterior.

El servidor de pasarela de pagos 506 determina si el Kpan y el certificado recibidos coinciden con el Kpan y el certificado almacenados en el servidor de pasarela de pagos (bloque 1102) asociado con el ID de dispositivo almacenado en la base de datos de servidor de pasarela de pagos. En caso afirmativo, a continuación, el servidor de pasarela de pagos 506 envía una respuesta de tarjeta virtual al dispositivo móvil 501 que incluye un nuevo Kpan (bloque 1103). Se usa un nuevo Kpan para generar un PAN diferente de la transacción anterior, y para evitar también contra ataques de reproducción. El servidor de pasarela de pagos 506 calcula el PAN para la tarjeta virtual usando el nuevo Kpan (bloque 1104). Este nuevo Kpan y el PAN precalculado se almacenan por el servidor de pasarela de pagos 506 para su uso posterior (bloque 1105).

Después de que el dispositivo móvil recibe el nuevo Kpan, reemplaza el Kpan almacenado con el nuevo Kpan (bloque 1106). Usa el nuevo Kpan para calcular un PAN para la tarjeta virtual, de la misma manera que el servidor de pasarela de pagos calculó el PAN (bloque 1107). Si las condiciones y los datos son correctos, aunque el dispositivo móvil calcula el PAN independientemente del servidor de pasarela de pagos, el PAN calculado por el dispositivo móvil debería ser idéntico al PAN calculado por el servidor de pasarela de pagos.

A continuación, el dispositivo móvil calcula los datos discrecionales (que son parte de los datos de pista dos) usando el PIN, el Ksec, el PAN, el certificado y el ATC (bloque 1108). El ATC y el PAN siguen cambiando con cada transacción, lo que hace que los datos discrecionales sean datos dinámicos.

El dispositivo móvil incrementa el ATC en 1 (bloque 1109).

En particular, el PAN se calcula por el dispositivo móvil y el servidor de pasarela de pagos de acuerdo con lo siguiente:
PAN = BIN(6) + SHA256[Kpan](8)+Luhn(1)+ Reservado(4)
en donde

BIN(6) es un número binario de 6 dígitos para identificar el servidor de pasarela de pagos;
SHA256[Kpan](8) es un número de 8 dígitos generado tomando el sha256 del valor de Kpan, incluyendo además convertir el valor de sha256 a decimal y truncando a ocho dígitos del valor de función de troceo;
Luhn(1) es un único dígito usado para garantizar que la tarjeta virtual siempre pase el algoritmo de LUHN;
y
Reservado(4) es un número de 4 dígitos que es el mismo que los últimos 4 dígitos del PAN de tarjeta de financiación.

Los valores anteriores se concatenan juntos para formar el PAN. El símbolo "+" en el cálculo anterior se refiere a la operación de concatenación.

En una realización de ejemplo de cálculo del PAN, los otros valores pueden conocerse o calcularse en primer lugar, y el valor de LUHN se calcula en último lugar. Por ejemplo, una forma intermedia al PAN es 66666612345678X1111, de modo que X representa Luhn(1). En otras palabras, el BIN(6) = 666666; SHA256[Kpan](8) = 12345678; y Reservado(4) = 1111.

Se pueden usar diferentes algoritmos de LUHN para resolver X, para garantizar que el PAN satisface el algoritmo de LUHN. Por ejemplo, un algoritmo de realización de ejemplo incluye (etapa 1) duplicar el valor de cualquier otro dígito, empezando desde el dígito más a la derecha; (etapa 2) sumar todos los dígitos individuales que incluyen el dígito X de la etapa 1; y (etapa 3) resolver la expresión mod10(suma total de la etapa 2)=0 para el dígito X. En esta realización de ejemplo, la solución a la ecuación es X = 9. Se pueden usar otros algoritmos de LUHN.

En una realización de ejemplo, puede usarse cualquier dígito antes de los últimos 4 dígitos del PAN que satisface los criterios de LUHN.

Los datos discrecionales se calculan usando lo siguiente:
Datos discrecionales = HMAC_SHA256[Ksec+PIN,M](10)
donde M = concatenación de (PAN, ID de certificado, ATC)

El truncamiento se realiza codificando los resultados de SHA en decimal, tomando a continuación los dígitos más a la izquierda. Puede apreciarse que SHA256 es una función de troceo criptográfica conocida, y HMAC es un código de autenticación de mensaje basado en función de troceo que implica una función de troceo criptográfica en combinación con una clave criptográfica secreta. La clave criptográfica secreta de la función de HMAC son los valores concatenados de Ksec y PIN. El mensaje M son los valores concatenados de PAN, ID de certificado y ATC. El ID de certificado es del certificado.

Volviendo a la Figura 12, se proporciona una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para verificar datos de tarjeta virtual, y, en particular, la verificación por el servidor de pasarela de pagos de los datos discrecionales (por ejemplo, los datos dinámicos). Una realización de este tipo puede usarse en combinación con los principios descritos anteriormente para verificar los datos de tarjeta virtual, y se usa en la invención. Esto puede ser una continuación del proceso descrito en la Figura 11.

El dispositivo móvil 501 envía una tarjeta virtual al terminal de POS de comerciante 502, que, a continuación, crea y envía una solicitud de autorización de pago al adquiriente de comerciante 103 (bloque 1201). La solicitud de autorización de pago se recibe finalmente por el servidor de pasarela de pagos 506 (bloque 1202). La solicitud de autorización de pago incluye, entre otras cosas, el PAN y los datos discrecionales de la tarjeta virtual, según se calculan por el dispositivo móvil 501.

Después de recibir la solicitud, el servidor de pasarela de pagos 506 usa el PAN para encontrar los datos asociados almacenados relevantes (por ejemplo, Kpan, certificado, Ksec, identificador de tarjeta de financiación, ID de dispositivo y otros datos de usuario). Los datos asociados almacenados relevantes se identifican por el PAN precalculado, que actúa como un índice para buscar en la base de datos de servidor. En otras palabras, el PAN recibido se compara con un número de PAN precalculados, y si se encuentra una coincidencia con un PAN precalculado dado, a continuación, los datos almacenados asociados con ese PAN precalculado dado se consideran los datos asociados almacenados relevantes.

El servidor de pasarela de pagos 506 usa los datos asociados almacenados relevantes para calcular sus propios datos discrecionales. Esto puede incluir usar el PIN (recibido durante el proceso de registro de usuario), el Ksec almacenado, el ID de certificado del certificado almacenado y un valor incrementado del ATC (bloque 1203).

El cálculo de los propios datos discrecionales de la pasarela de pagos usa lo siguiente:
Datos discrecionales = HMAC_SHA256[Ksec+PIN,M](10)
donde M = concatenación de (PAN, ID de certificado, (ATC+1))

El ATC+1 representa el valor de ATC incrementado.

El servidor de pasarela de pagos 506 determina si sus propios datos discrecionales son iguales a los datos

discrecionales recibidos (bloque 1204). Si no son iguales, el servidor de pasarela de pagos incrementa además el ATC en "1" y recalcula sus propios datos discrecionales (bloque 1205). El proceso vuelve al bloque 1204 para comprobar si los conjuntos de datos discrecionales son iguales. El proceso que implica el bloque 1205 puede repetirse, de modo que cada vez el valor de ATC se incremente además en 1. Esto se puede hacer hasta un cierto número de veces (por ejemplo, 10 veces), después de lo cual se detendrá el proceso de transacción.

Si el intervalo de valores de ATC (por ejemplo, entre ATC+1 y ATC+10) no genera un conjunto de datos discrecional idéntico, a continuación, la verificación es infructuosa. El intervalo es para tener en cuenta la posibilidad de que el contador de ATC del dispositivo móvil pueda haberse incrementado sin el conocimiento del servidor de pasarela de pagos. Por lo tanto, se usa una memoria intermedia o intervalo o valores de ATC.

Si los propios datos discrecionales del servidor de pasarela de pagos son los mismos que los datos discrecionales recibidos, a continuación, el servidor de pasarela de pagos reemplaza el valor de ATC anterior con el valor de ATC actualmente incrementado que se usa en el cálculo de sus propios datos discrecionales. De esta manera, el valor de ATC almacenado en el servidor de pasarela de pagos debería ser ahora igual al valor de ATC almacenado en el dispositivo móvil.

Se observa que, si el PIN usado por el dispositivo móvil para calcular los datos discrecionales se introduce incorrectamente por el usuario (por ejemplo, no es el mismo que el PIN proporcionado en el registro), a continuación, los datos discrecionales del dispositivo móvil no igualarán los propios datos discrecionales del servidor de pasarela de pagos. Esto es debido a que sus propios datos discrecionales se calculan usando el PIN proporcionado en el registro. De esta manera, se verifica implícitamente el PIN proporcionado por el usuario en el dispositivo móvil durante cada transacción por el servidor de pasarela de pagos.

Continuando con la Figura 12, después de que los datos se verifiquen satisfactoriamente o no, el servidor de pasarela de pagos finalmente responde al comerciante enviando una respuesta de autorización al comerciante (103, 502) (bloque 1207). Para aclarar además, si la verificación de datos discrecionales no fue satisfactoria (según el bloque 1205 después de que se haya alcanzado unas ciertas iteraciones), a continuación se envía una respuesta de autorización de pago negativa al comerciante (bloque 1207).

Los métodos y sistemas descritos en el presente documento no se basan en tener una tarjeta de pago de software almacenada en el elemento seguro en el dispositivo móvil para facilitar la transacción de pago sin contacto. Esto es debido a que el PAN y los otros elementos de datos de tarjeta de la tarjeta de financiación no se almacenan en el dispositivo móvil. En su lugar, se almacena el PAN y la fecha de caducidad de la tarjeta de financiación en un servidor seguro (por ejemplo, el servidor de pasarela de pagos). Además, los datos de tarjeta virtual se crean en un servidor seguro y se cifran para un dispositivo móvil particular. Además, los datos discrecionales en los datos de la pista dos son una función del PIN que se volvió a introducir con cada pago. Los datos de tarjeta virtual únicamente se envían en el momento de realizar el pago, y únicamente pueden usarse una vez. Además, únicamente el servidor puede validar los datos de tarjeta virtual. En otras palabras, no hay nada para que un adversario acceda a través de la fuerza bruta en el dispositivo móvil sin ser detectado.

Además, la carga útil cifrada de tarjeta virtual no es reutilizable. Esto se debe a que tan pronto como la tarjeta se usa una vez, ninguna otra parte puede usarla de nuevo.

También se observa que, algunas realizaciones de ejemplo, la tarjeta virtual de un solo uso se crea justo a tiempo, antes de la autorización de pago del comerciante.

Además, los detalles de la tarjeta de financiación nunca se proporcionan al comerciante, ya que, en su lugar, se proporcionan los detalles de la tarjeta virtual.

Los métodos y sistemas descritos en el presente documento son totalmente compatibles con el modelo y sistemas de pago de tarjeta de 4 partes convencional. No hay cambio de sistema requerido por el emisor de la tarjeta de financiación, comerciante, adquirente o red de pagos.

Los métodos y sistemas descritos en el presente documento también permiten el uso de una "aplicación única" para soportar una o muchas tarjetas virtuales, así como una o muchas tarjetas de financiación. Esto reduce el almacenamiento requerido en el elemento seguro (y, generalmente, el almacenamiento en el dispositivo móvil) para no limitar el número de tarjetas que un cliente puede cargar en un elemento seguro.

Se puede apreciar que, los métodos y sistemas descritos en el presente documento permiten que el titular de la tarjeta (por ejemplo, el usuario final) registre cualquier tarjeta de financiación que desee en su dispositivo móvil habilitado para NFC, independientemente de que el emisor de la tarjeta tenga la infraestructura o una relación comercial con un operador móvil particular.

Los métodos y sistemas descritos en el presente documento pueden usarse con cualquier tipo de tarjeta de financiación. Las tarjetas de financiación y el dispositivo móvil se pre-registran con el servidor de pasarela de pagos

506. Este registro es independiente de cualquier operador de telefonía móvil particular y cualquier emisor de tarjeta de financiación particular. Como resultado, no se requiere ningún acuerdo comercial ni infraestructura informática adicional por un operador de telefonía móvil y un emisor de tarjeta de financiación para facilitar el pago sin contacto usando un dispositivo móvil. Esto, a su vez, reduce el coste incurrido por el emisor de tarjeta de financiación para emitir tarjetas de pago de software a dispositivos móviles.

En una realización de ejemplo, se proporciona un método realizado por un servidor para facilitar el pago. El método incluye: recibir un mensaje desde un dispositivo móvil que identifica una tarjeta de financiación; buscar en una base de datos de múltiples tarjetas asociadas con el dispositivo móvil un número de tarjeta de financiación asociado con la tarjeta de financiación identificada; calcular datos para una tarjeta virtual, comprendiendo los datos un número de tarjeta y una fecha de caducidad; almacenar los datos para el número de tarjeta virtual en asociación con el número de tarjeta de financiación; enviar los datos para la tarjeta virtual al dispositivo móvil; calcular los detalles de la tarjeta usando el PIN de usuario como entrada; recibir una primera solicitud de autorización de pago de un adquirente de comerciante, comprendiendo la solicitud los datos para la tarjeta virtual y una cantidad de pago solicitada; recuperar el número de tarjeta de financiación basándose en los datos para la tarjeta virtual; enviar una segunda solicitud de autorización de pago a un emisor de tarjeta de financiación, comprendiendo la solicitud el número de tarjeta de financiación y la cantidad de pago solicitada; recibir una respuesta de autorización de pago del emisor de la tarjeta de financiación; y enviar la respuesta de autorización de pago al adquirente de comerciante.

Comercio electrónico y transacciones basadas en Internet

En otra realización de ejemplo de los sistemas y métodos propuestos, los principios anteriormente descritos de la tarjeta virtual también se aplican a comercio electrónico o transacciones basadas en Internet. En otras palabras, mientras que los ejemplos anteriores incluyen el uso de un dispositivo terminal de POS físico 502 que interactúa con el dispositivo móvil 501, el comercio electrónico o las transacciones basadas en Internet no usan el dispositivo terminal de POS 502. En su lugar, un dispositivo móvil 501 puede comunicarse con el adquirente de comerciante 103 o el servidor de pasarela de pagos 506 (por ejemplo, a través de una página web de comercio electrónico o aplicación de pagos). En otras palabras, para ejecutar una transacción, el dispositivo móvil envía los datos de tarjeta virtual al adquiriente de comerciante 103 o al servidor de pasarela de pagos 506 (por ejemplo, a través de una página web de comercio electrónico o aplicación de pagos) usando una conexión a Internet.

Por ejemplo, las operaciones anteriores que implican el dispositivo terminal de POS 502 pueden realizarse, pero usando una página web de comercio electrónico o aplicación de pagos en lugar del dispositivo terminal de POS 502. Como se muestra en la Figura 13, se proporciona una vista de diagrama esquemática de las entidades implicadas en una realización de ejemplo de una transacción de pago que usa una tarjeta virtual para facilitar un pago, que es similar a la Figura 5. Sin embargo, a diferencia de la Figura 5, que muestra un dispositivo terminal de POS 502, en la Figura 13, se muestra una interfaz de Internet y comercio electrónico 1301 interactuando con el dispositivo móvil 501 y el adquirente de comerciante 103. En otra realización de ejemplo, además, o como alternativa, el dispositivo móvil 501 interactúa con la red de pagos 504 directamente a través de la interfaz de Internet y comercio electrónico como se muestra por la conexión 1302. Se aprecia que, el dispositivo móvil 501 no requiere un subsistema de NFC 609 para realizar transacciones usando la interfaz de Internet y comercio electrónico 1301. En otras palabras, el dispositivo móvil 501 puede tener o no el subsistema de NFC 609, sin afectar al almacenamiento y recuperación de información en el elemento seguro 622, y sin afectar a una transacción de Internet o de comercio electrónico. El dispositivo móvil se conecta a la interfaz de Internet y comercio electrónico 1301 a través de una página web que puede verse a través de una aplicación de explorador de Internet 619 en el dispositivo móvil. En otra realización de ejemplo, el dispositivo móvil se conecta a la interfaz de internet y comercio electrónico 1301 a través de una GUI de aplicación de pagos.

En general, los ejemplos anteriores descritos con respecto a las Figuras 7, 8, 9a, 9b, 10, 11 y 12 también se usan para transacciones de comercio electrónico, pero con el terminal de POS 502 reemplazado por la interfaz de Internet y comercio electrónico 1301 según la Figura 13.

En la Figura 14, se muestra una interfaz gráfica de usuario (GUI) 1401 de ejemplo como se visualiza por una página web de comercio electrónico o GUI de aplicación de pagos. Esto se visualiza por el dispositivo móvil 501, por ejemplo, cuando un usuario ha seleccionado un producto, un artículo o un servicio para comprar. Se muestran los detalles de transacción 1402, que incluyen, por ejemplo, la cantidad a pagar por el usuario y el nombre del usuario. Puede mostrarse otra información, por ejemplo, el ID de producto o el ID de usuario. La información de tarjeta de financiación 1403 también se muestra y, en el caso de una tarjeta de crédito, puede mostrar los últimos cuatro dígitos de la tarjeta de financiación 1404. En una realización de ejemplo, se visualiza una tarjeta de financiación por defecto, pero puede seleccionarse una tarjeta de financiación diferente usando el control 1407. En el ejemplo de la Figura 14, el dispositivo móvil 501 realizará un pago usando una tarjeta virtual asociada con la tarjeta de financiación Visa que termina en los dígitos '4242' (1404). En otra realización de ejemplo, los últimos cuatro dígitos no se visualizan para evitar que atacantes visualicen esta información.

Cuando se visualiza la GUI 1401, para completar la transacción, el usuario introduce un PIN en el campo 1405 y selecciona el botón "pagar ahora" 1406. Cuando la GUI 1401 detecta estos eventos, el dispositivo móvil 501 envía datos de tarjeta de financiación virtual al adquiriente de comerciante 103 o al servidor de pasarela de pagos 506, a

través de la interfaz de Internet y comercio electrónico 1301.

En otra GUI de realización de ejemplo (no mostrada), no se visualiza el botón de "pagar ahora" 1406. Por ejemplo, la GUI puede detectar la longitud de cuántos caracteres se introdujeron en el campo de entrada 1405. Después de que la GUI detecta que se ha introducido el número requerido de caracteres en el campo de entrada 1405, el PIN se envía automáticamente.

En una realización de ejemplo, el PIN es el valor de verificación de tarjeta (CVV), valor de seguridad de tarjeta (CSV), código de seguridad de tarjeta (CSC), verificación de código de tarjeta (CCV), código de verificación de tarjeta (CVC o CVC2), etc., de la tarjeta de financiación y este valor se determina por el emisor de la tarjeta de financiación 104. En otra realización de ejemplo, el PIN se determina por el usuario. En otra realización de ejemplo, el PIN es una contraseña. En otra realización de ejemplo, el PIN es una contraseña usada por el sistema "Verificado por Visa", que es una verificación complementaria.

En otra realización de ejemplo, como se muestra en la Figura 15, se proporciona otra GUI 1501 de ejemplo y visualiza detalles de transacción 1402, información de tarjeta de financiación 1403 y un botón de "pagar ahora" 1406. En otras palabras, cuando se visualiza la GUI 1501, el usuario únicamente necesita seleccionar el botón "pagar ahora" 1406 para ejecutar la transacción. Esto hará que el dispositivo móvil 501 envíe datos de tarjeta de financiación virtual al adquiriente de comerciante 103 o al servidor de pasarela de pagos 506, a través de la interfaz de Internet y comercio electrónico 1301. Se aprecia que no se requiere un PIN usando la GUI de la Figura 15.

Volviendo a la Figura 16, se proporciona un conjunto de ejemplo de instrucciones implementadas por procesador para realizar un pago usando una interfaz de Internet y comercio electrónico 1301. La Figura 16 es similar a la Figura 7, por lo que no se repiten operaciones similares en detalle. En el bloque 1601, la interfaz de Internet y comercio electrónico invoca el dispositivo móvil para visualizar datos en una GUI de comercio electrónico (por ejemplo, 1401 y 1501). El dispositivo móvil 501 visualiza la GUI de comercio electrónico en el bloque 1602. Opcionalmente, aunque no necesariamente, se realizan los bloques 703 y 704 por el dispositivo móvil 501. Además, el dispositivo móvil, a través de la GUI de comercio electrónico, muestra opcionalmente tarjetas de financiación pre-registradas en el bloque 706, y el usuario selecciona una tarjeta de financiación 707. En otras realizaciones, únicamente hay una tarjeta de financiación, o hay una tarjeta de financiación predeterminada que se usa, a menos que se cambie por el usuario. Se realizan las operaciones en los bloques 708, 709, 710 y 711. Como se ha descrito anteriormente, en algunas realizaciones de ejemplo, se puede usar una tarjeta virtual previamente calculada y, por lo tanto, no es necesario calcular una nueva tarjeta virtual para todas y cada una de las transacciones.

Continuando con la Figura 16, en una realización de ejemplo, la GUI de comercio electrónico solicita autenticación de PIN (bloque 712) y el usuario proporciona el PIN (713). Sin embargo, en otras realizaciones, no se requiere proporcionar el PIN. También se realizan las operaciones en los bloques 714 y 715. Sin embargo, en otras realizaciones, si se está usando la tarjeta virtual previamente calculada, no se realizan los bloques 714 y 715.

En una realización de ejemplo, el usuario introduce un comando, a través de la GUI de comercio electrónico, para ejecutar la transacción (bloque 1603). Por ejemplo, el usuario puede seleccionar el botón de "pagar ahora" 1406, o proporcionar alguna otra entrada que se entienda que ejecuta la transacción.

El dispositivo móvil envía los datos de tarjeta virtual a la interfaz de Internet y comercio electrónico (bloque 1604), y la interfaz de Internet y comercio electrónico envía los mismos al adquiriente de comerciante 103 o al servidor de pasarela de pagos 506 (véase la Figura 17), cuando se completa la transacción (ya sea aceptada o denegada), se envía un mensaje de confirmación a través de la interfaz de Internet y comercio electrónico al dispositivo móvil (bloque 1605). A continuación, puede realizarse el bloque 722.

La Figura 17 muestra instrucciones implementadas de procesador de ejemplo, que es una continuación de la Figura 16. Los bloques 1601, 1603 y 1604 se incluyen para mostrar contexto, y se implementaron en la Figura 16 anterior. La Figura 17 es similar a la Figura 8, pero, en su lugar, incluye la interfaz de Internet y comercio electrónico 1301. Las operaciones de los bloques 801, 802, 803, 804, 805, 806, 807, 808 y 809 se aplican a la Figura 17 y no se describen en detalle de nuevo, ya que estos bloques se describieron en detalle con respecto a la Figura 8.

Transferencia de valor de parte a parte

En otras realizaciones de ejemplo de los sistemas y métodos propuestos, lo siguiente se refiere en general a facilitar una transferencia de valor de parte a parte usando una tarjeta virtual en un dispositivo móvil.

Los dispositivos móviles se pueden usar para transferir valor, por ejemplo, entre dos personas. Un dispositivo móvil puede estar equipado con un sistema de comunicación de campo cercano (NFC) que puede usarse para transferir credenciales de pago, tal como información de tarjeta de pago, a otro dispositivo móvil que también está equipado con un sistema de NFC.

Se reconoce que es difícil transferir dinero desde el dispositivo móvil de una persona al dispositivo de otra persona, o,

más en general, de una parte a otra parte usando dispositivos móviles. En muchos casos, los operadores de telefonía móvil y los emisores de tarjetas de financiación no tienen sistemas informáticos para soportar la transferencia de dinero desde un dispositivo móvil a otro dispositivo móvil, o es de coste prohibitivo para las partes. También se reconoce que es difícil transferir dinero entre dispositivos móviles de una manera segura, manteniendo aún la comodidad.

También se reconoce que hay situaciones en las que un usuario emisor desea transferir valor a un usuario receptor, pero el usuario emisor no conoce o no confía en el usuario receptor. Por ejemplo, un usuario emisor debe dinero a un usuario receptor, pero no conoce o no confía en el usuario receptor. Transferir valor (por ejemplo, dinero) usando una tarjeta de financiación al usuario receptor, sin proporcionar ningún dato o información acerca de la tarjeta de financiación, puede ser difícil. Además, la elección y la manera conveniente también dificultan la transferencia de valor.

También se reconoce que hay situaciones en las que el usuario receptor no tiene una cuenta bancaria. En otras palabras, el usuario receptor no tiene una cuenta establecida para recibir y almacenar el valor (o fondos) del usuario emisor. Por lo tanto, en muchos casos, el usuario receptor no puede aceptar o recibir el valor (o fondos) del usuario emisor.

Transferir valor de parte a parte usando un ID de transferencia

Los métodos y sistemas descritos en el presente documento permiten que un emisor (por ejemplo, una primera persona) envíe valor, por ejemplo, dinero, a un receptor (por ejemplo, una segunda persona). En particular, el dispositivo móvil habilitado para NFC del emisor se "toca" contra el dispositivo móvil habilitado para NFC del receptor, y se produce la transferencia de valor. El valor transferido se almacena en asociación con el dispositivo móvil del receptor como una tarjeta virtual de prepago. El receptor puede usar a continuación su teléfono habilitado para NFC para realizar pagos con la tarjeta virtual de prepago, o bien a través de NFC (por ejemplo, con un terminal de punto de venta habilitado para NFC de un comerciante) o a través de Internet (por ejemplo, comercio móvil o comercio electrónico).

Como una realización de ejemplo alternativa, en lugar de enviar una tarjeta virtual, el servidor de pasarela de pagos 506 envía un ID de transferencia al usuario dador para que se comparta con el usuario receptor. El ID de transferencia se usa por el servidor de pasarela de pagos para identificar la tarjeta de financiación seleccionada y la cantidad especificada por el usuario emisor. En otras palabras, el ID de transferencia se considera un puntero que apunta a la información almacenada en el servidor de pasarela de pagos para identificar la tarjeta de financiación seleccionada y la cantidad especificada por el usuario emisor. Ejemplos no limitantes de un ID de transferencia pueden ser números, una colección de caracteres (incluyendo números) y un URL.

Los sistemas y métodos descritos en el presente documento también permiten que un servidor de pasarela de pagos de monedero basado en la nube se sincronice con un dispositivo móvil habilitado para NFC del receptor y una aplicación para facilitar transferencias de valor sin contacto desde un dispositivo móvil habilitado para NFC del emisor. Un usuario emisor selecciona una tarjeta de financiación y proporciona la cantidad para realizar la transferencia de valor de parte a parte sin contacto, a través de su dispositivo móvil. Se genera un ID de transferencia por el servidor de pasarela de pagos para completar la transacción de pago de parte a parte. El ID de transferencia se usa por el servidor de pasarela de pagos para identificar la tarjeta de financiación seleccionada y la cantidad a transferir por el usuario emisor. En el servidor de pasarela de pagos, el ID de transferencia se asocia temporalmente con la tarjeta de financiación y la cantidad permitida de valor a transferir.

Cuando se inicia una transferencia de valor de parte a parte, los datos que incluyen los datos de ID de transferencia se envían a través del sistema de NFC en el dispositivo móvil del emisor al dispositivo móvil habilitado para NFC del receptor. Esta información se envía desde el dispositivo móvil del receptor al servidor de pasarela de pagos de cartera basada en la nube (también denominado el "servidor de pasarela de pagos"). El servidor de pasarela de pagos de cartera basada en la nube verifica el ID de transferencia. Si se verifica satisfactoriamente, se recuperan los detalles de la tarjeta de financiación del usuario emisor asociados con el ID de transferencia y se envían al servidor emisor de tarjeta de pago a través del servidor de pasarela de pagos para completar la autorización de transferencia de valor. El servidor emisor de tarjeta de financiación verifica la tarjeta de financiación y devuelve un código de autorización al servidor de pasarela de pagos. El servidor de pasarela de pagos actúa a continuación como un servidor emisor de tarjeta virtual y genera una tarjeta virtual de prepago para el usuario receptor, que puede usarse por el dispositivo móvil del receptor.

La transferencia de valor para la tarjeta virtual de prepago puede liquidarse cuando el servidor de pasarela de pagos inicia una solicitud de liquidación, típicamente una vez al final de cada día laboral, usando el método convencional. Esto incluye recuperar todos los números de tarjeta de financiación y los correspondientes códigos de autorización recibidos durante el periodo y enviar esta información al emisor de tarjeta de financiación para su liquidación. El emisor de la tarjeta de financiación verifica los números de tarjeta de financiación y los códigos de autorización, y si se verifica satisfactoriamente, envía el dinero de vuelta a la cuenta bancaria asociada con el servidor de pasarela de pagos a través de un método de transferencia de fondos electrónica convencional. El dinero se almacena en asociación con la cuenta de tarjeta virtual de prepago. En una realización de ejemplo, el emisor de tarjeta virtual es el servidor de pasarela de pagos, o un módulo dentro del servidor de pasarela de pagos.

En otra realización de ejemplo, antes de que el dispositivo móvil del emisor envíe el ID de transferencia al dispositivo móvil del receptor, el dispositivo móvil del emisor solicita autorización al emisor de tarjeta de financiación a través del servidor de pasarela de pagos. Después de que se completa la autorización, se crea un ID de transferencia y a continuación se envía al dispositivo móvil del receptor. El dispositivo móvil del receptor verifica el ID de transferencia con el servidor de pasarela de pagos. El servidor de pasarela de pagos realiza a continuación una solicitud de liquidación asociada con la solicitud de autorización desde el ID de transferencia. El servidor de pasarela de pagos genera a continuación una tarjeta virtual de prepago para el usuario receptor, que puede usarse por el dispositivo móvil del receptor.

En otra realización de ejemplo, antes de que el dispositivo móvil del emisor envíe el ID de transferencia al dispositivo móvil del receptor, tienen lugar tanto la autorización como la liquidación. Después de que el servidor emisor de tarjeta de financiación completa la autorización, y después de que se haya realizado la liquidación para la transferencia de valor y se haya creado una tarjeta virtual de prepago, a continuación, se transfiere el ID de transferencia al dispositivo móvil del receptor.

En una realización de ejemplo, los sistemas y métodos descritos en el presente documento permiten que un dispositivo habilitado para NFC con la aplicación de transferencia de parte a parte transfiera una cantidad de valor definida por el usuario a otro dispositivo habilitado para NFC, que también tiene la aplicación de transferencia de parte a parte, sin revelar nunca los detalles de la tarjeta de financiación del emisor al receptor. Además, el emisor puede establecer o determinar el valor a dar al receptor. Una transferencia satisfactoria da como resultado que se emita al usuario receptor una tarjeta virtual de prepago por la misma cantidad de valor que la enviada por el usuario emisor. Por lo tanto, incluso si el usuario receptor no tiene una cuenta bancaria para recibir el valor, al usuario receptor todavía se le puede dar una tarjeta virtual de prepago que puede usarse por el usuario receptor para realizar pagos y transacciones.

Puede apreciarse que, puede usarse cualquier tarjeta de financiación, y no está limitada o depende de que el operador de telefonía móvil tenga acuerdo con el emisor de la tarjeta de financiación. Para que se use una tarjeta, en primer lugar necesita registrarse con el servicio. También puede apreciarse que puede registrarse cualquier número de tarjetas de financiación en asociación con el dispositivo móvil. El dispositivo móvil del titular de la tarjeta incluye una aplicación de pagos (también denominada aplicación de transferencia de valor) que puede interactuar con el servidor de pasarela de pagos.

En una realización de ejemplo del registro, para cada tarjeta de financiación que el usuario desea registrar, el usuario escribe detalles de la tarjeta en el dispositivo móvil (por ejemplo, el nombre impreso en la tarjeta de financiación, el PAN impreso en la tarjeta de financiación, la fecha de caducidad impresa en la tarjeta de financiación y el código de seguridad estático impreso en la tarjeta de financiación). Como se ha mencionado anteriormente, el emisor de la tarjeta de financiación no necesita tener un acuerdo existente con ningún operador de telefonía móvil. El dispositivo móvil envía estos datos y un ID de dispositivo móvil al servidor de pasarela de pagos. El servidor de pasarela de pagos calcula un identificador de tarjeta de financiación que identifica la tarjeta de financiación dada. El servidor de pasarela de pagos almacena el identificador de tarjeta de financiación en asociación con los detalles de tarjeta de financiación y envía el identificador de tarjeta de financiación al dispositivo móvil para su almacenamiento. En otra realización de ejemplo, el usuario simplemente toca y toca una tarjeta sin contacto en el dispositivo móvil de modo que la aplicación móvil puede capturar los detalles de la tarjeta y enviarlos al servidor de pasarela de pagos para su registro. En una realización de ejemplo, el identificador de tarjeta de financiación es un valor que es diferente del PAN, fecha de caducidad o código de seguridad estático de la tarjeta de financiación. Por ejemplo, el identificador de tarjeta de financiación es un valor aleatorio de modo que, si es interceptado por un adversario, no sería capaz de reconocer ningún detalle de tarjeta de financiación. En una realización de ejemplo, el dispositivo móvil no almacena ningún detalle de tarjeta de financiación o almacena detalles de tarjeta de financiación limitados (por ejemplo, el nombre del emisor de tarjeta de financiación y los últimos 4 dígitos del PAN). El dispositivo móvil almacena el identificador de tarjeta de financiación, que envía al servidor de pasarela de pagos para indicar una tarjeta de financiación específica. Puede apreciarse que, hay otros métodos para capturar los detalles de la tarjeta de crédito de financiación (por ejemplo, además de que el usuario escriba los datos), que pueden usarse con los principios descritos en el presente documento.

Puede apreciarse que, se requiere una única aplicación de pagos en el dispositivo móvil, que puede gestionar múltiples tarjetas de financiación. Si se registran múltiples tarjetas de financiación, se almacena cada uno de los identificadores de tarjeta de financiación asociados en el dispositivo móvil, dentro de la aplicación de pagos única. Los detalles de cada tarjeta de financiación individual se almacenan en el servidor de pasarela de pagos. De esta manera, el servidor de pasarela de pagos actúa como un servidor basado en la nube que almacena los detalles de múltiples tarjetas de financiación.

Volviendo a la Figura 18, se proporciona un ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para facilitar una transferencia de valor desde un usuario emisor 101 a un usuario receptor 1807. En el bloque 1801, el usuario emisor especifica una tarjeta de financiación y una cantidad para transferir al usuario receptor. En el bloque 1802, el usuario emisor recibe, desde el servidor de pasarela de pagos, un ID de transferencia que se basa en la cantidad y la tarjeta de financiación. En el bloque 1803, el usuario emisor envía el ID de transferencia al usuario receptor. En el bloque 1804, el usuario receptor valida el ID de transferencia y la cantidad, por ejemplo, a

través del servidor de pasarela de pagos. En el bloque 1805, si es válido, se emite al usuario receptor una tarjeta virtual de prepago por la cantidad especificada por el usuario emisor.

Con respecto al bloque 1803, aunque muchas de las realizaciones de ejemplo descritas en el presente documento usan tecnología de NFC para transmitir datos entre los dispositivos móviles, puede apreciarse que pueden usarse otros métodos de transmisión de datos. Por ejemplo, puede enviarse el ID de transferencia al dispositivo móvil del usuario receptor a través de Bluetooth, infrarrojos y otras tecnologías de comunicación entre pares (P2P). En otras realizaciones de ejemplo, el ID de transferencia puede transmitirse a través de otros medios que pueden no ser necesariamente P2P, incluyendo mensajería instantánea, mensajería de texto, códigos de barras, códigos de barras 2D, código QR, correo electrónico, etc. En una realización de ejemplo, se transmiten datos adicionales o datos alternativos desde el dispositivo móvil del usuario emisor al dispositivo móvil del usuario receptor para facilitar la transferencia de valor, tarjeta virtual resultado disponible para su uso por el usuario receptor. En una realización de ejemplo, se transmite de forma segura el ID de transferencia, por ejemplo, cuando se transfiere entre cualquiera del servidor, el dispositivo móvil del usuario emisor y el dispositivo móvil del usuario receptor.

Volviendo a la Figura 19, se muestran componentes de realización de ejemplo de un sistema para facilitar una transferencia de fondos de parte a parte usando el ID de transferencia. Se muestra el usuario emisor 101. El usuario tiene una o más tarjetas de financiación 505. Por ejemplo, el usuario tiene múltiples tarjetas de financiación. El usuario 101 también posee un dispositivo móvil habilitado para NFC 501, que incluye una aplicación de pagos (también denominada una aplicación de transferencia de valor). El dispositivo móvil del emisor 1901 está configurado para interactuar, a través de NFC, con el dispositivo móvil habilitado para NFC del receptor 1901. Se aprecia que, el dispositivo móvil del receptor 1901 puede tener componentes de hardware y software similares al dispositivo móvil del emisor, como se muestra, el dispositivo móvil del emisor 501 y el dispositivo móvil del receptor 1901 interactúan con el servidor de pasarela de pagos 506. El servidor de pasarela de pagos 506 también está en comunicación de datos con un servidor de emisión de tarjetas de financiación 104.

El servidor de pasarela de pagos 506 almacena componentes de datos específicos del usuario emisor (bloque 1903) y componentes de datos específicos del usuario receptor (bloque 1902). Por ejemplo, los componentes de datos específicos para el usuario emisor (bloque 1903) incluyen asociaciones de datos registrados 1904 que asocian una o más tarjetas de financiación con el ID de dispositivo móvil del emisor. Por ejemplo, la tarjeta de financiación 1 y la tarjeta de financiación 2 (y otras tarjetas de financiación) se almacenan en asociación con el ID de dispositivo móvil del dispositivo móvil del emisor 501. También hay asociaciones de datos temporales 1905, que incluyen un ID de transferencia 1907 que se asocia temporalmente con una de las tarjetas de financiación del usuario 1906. El ID de transferencia 1907 puede usarse por el usuario emisor 101 para realizar una transferencia de valor de parte a parte.

Los componentes de datos relacionados con el usuario receptor (bloque 1902) incluyen asociaciones de datos registradas 1908 que especifican que cero o más tarjetas de financiación están asociadas con el ID de dispositivo móvil del receptor. Por ejemplo, las tarjetas de financiación asociadas con el ID de dispositivo móvil del receptor pueden incluir dos tarjetas de financiación y la tarjeta virtual de prepago 1909 emitida por el servidor de pasarela de pagos 506. Puede apreciarse que, puede usarse la tarjeta virtual de prepago 1909 para el usuario receptor 1807 para realizar un pago a un comerciante o a otra transferencia de valor de parte a parte más a otro usuario.

El servidor de pasarela de pagos 506 está en comunicación con los dispositivos móviles 501, 1901 a través de una red inalámbrica. Por ejemplo, la red inalámbrica se proporciona por un operador de telefonía móvil. El servidor de pasarela de pagos 506 está en comunicación de datos con el servidor de emisión de tarjetas de financiación 104 a través de medios alámbricos o inalámbricos, o ambos.

Volviendo a las Figuras 20, 21 y 22, se muestra un dispositivo móvil emisor 501 y un dispositivo móvil receptor 1901 interactuando entre sí cuando se envían fondos a través de NFC.

Volviendo a la figura 20, el dispositivo móvil del receptor 1901 muestra una realización de ejemplo de una interfaz gráfica de usuario (GUI) que permite a un usuario enviar o recibir fondos. Aunque no se muestra, el dispositivo móvil del emisor 501 podría haber visualizado una GUI similar y, a continuación, basándose en una selección de usuario para enviar fondos, el dispositivo móvil 501 se coloca en un modo para enviar fondos. En el modo de "enviar fondos", el dispositivo móvil del emisor 501 muestra una GUI para facilitar el envío de fondos. La GUI visualizada en la Figura 20 en el dispositivo móvil del emisor 501 es una realización de ejemplo de una GUI de este tipo para facilitar el envío de fondos.

Continuando con la Figura 20, la GUI en el dispositivo móvil del emisor 501 incluye un campo de entrada 2001 que permite al emisor especificar cuánto dinero enviar en una transferencia de parte a parte. Por ejemplo, se pueden especificar 100 $. También incluye un menú de tarjetas de financiación que pueden seleccionarse para realizar la transferencia de parte a parte. Existe una opción, por ejemplo, para usar la tarjeta de crédito Visa de CIBC (por ejemplo, un nombre de un primer banco emisor) 2002; existe otra opción para usar la tarjeta de crédito Mastercard del Banco de Montreal o BMO (por ejemplo, un nombre de un segundo banco emisor) 2003. El usuario selecciona 2004 la tarjeta de crédito Visa 2002 como la tarjeta de financiación.

El dispositivo móvil del receptor 1901 también tiene una aplicación de pagos que visualiza una GUI con un control para recibir fondos 2006 y un control para enviar fondos 2005. El usuario receptor proporciona una entrada de selección 2007, seleccionando el control 2006, que coloca el dispositivo móvil 1091 en un modo para recibir fondos.

Volviendo a la Figura 21, después de que se haya introducido la información requerida en las aplicaciones de pago de los respectivos dispositivos móviles 501, 1901, los fondos están listos para transferirse. El dispositivo móvil emisor 501 muestra un mensaje "Tocar teléfonos para enviar fondos de 100 $ usando CIBC Visa". El dispositivo móvil del receptor 1901 muestra un mensaje "Tocar teléfonos para recibir fondos". En esta etapa, los dos dispositivos móviles 501, 1901 se colocan lo suficientemente cerca entre sí (por ejemplo, tocándose) para permitir la transferencia satisfactoria de datos a través de NFC.

Volviendo a la Figura 22, después de que el dinero se haya transferido del emisor al receptor, el dispositivo móvil del emisor 501 visualiza un mensaje que "Usted ha enviado 100 $ a Bob (647-667-1234)". El mensaje incluye, por ejemplo, la cantidad transferida, el nombre del usuario receptor y un número de teléfono del dispositivo móvil del receptor. El dispositivo móvil del receptor 1901 visualiza un mensaje que "Usted ha recibido una tarjeta virtual de prepago de 100 $ de Alicia (416-333-4321)". El mensaje, por ejemplo, incluye la cantidad recibida, el nombre del usuario emisor y un número de teléfono del dispositivo móvil del emisor.

Volviendo a la Figura 23, se proporcionan instrucciones ejecutables por ordenador o implementadas por procesador de ejemplo para facilitar una transferencia de fondos de parte a parte entre un usuario emisor y un usuario receptor.

En una realización de ejemplo, se supone que tanto los usuarios emisores como receptores tienen cada uno un dispositivo habilitado para NFC. También se supone que ambos dispositivos móviles han instalado una aplicación de pagos. También se supone que ambos usuarios han registrado sus dispositivos móviles con un servidor de pasarela de pagos. También se supone que el usuario emisor también ha pre-registrado una o más tarjetas de financiación con el servidor de pasarela de pagos, que se identifican cada una por un identificador de tarjeta de financiación. En otras palabras, el servidor de pasarela de pagos tiene detalles de tarjeta de financiación almacenados en asociación con el ID de dispositivo móvil del emisor.

El usuario emisor 101 inicia la aplicación de pagos 620 en su dispositivo móvil 501 (bloque 2301). La aplicación de pagos 620 determina si el usuario se ha registrado satisfactoriamente en el servicio (bloque 2302), y, en caso afirmativo, se muestra un menú de aplicación, y visualiza la opción para dar usando la aplicación de pagos (bloque 2303). El usuario 101 selecciona la opción para dar dinero usando la aplicación de pagos. Se observa que, pueden usarse diversas experiencias de usuario con los principios descritos en el presente documento.

Por ejemplo, una GUI en el menú puede recibir una entrada del usuario para iniciar una transferencia de fondos de parte a parte con una tarjeta virtual con la aplicación de pagos. Ejemplos de otros elementos de menú incluyen "añadir una tarjeta de financiación", "borrar una tarjeta de financiación", etc.

El dispositivo móvil 501 visualiza a continuación las tarjetas de financiación que se han pre-registrado por el usuario (bloque 2305). Se recibe una entrada de usuario para especificar una cantidad a transferir (por ejemplo, dada) y se recibe una entrada para seleccionar una de las tarjetas de financiación (bloque 2306). En una realización de ejemplo, la información de tarjeta de financiación visualizada se carga después de que el usuario final se registre satisfactoriamente en el servicio y haya registrado al menos una tarjeta de financiación. La lista se actualiza cuando el usuario añade una tarjeta de financiación adicional en la aplicación de pagos o cuando se borra una tarjeta de financiación. Para cada tarjeta de financiación registrada, hay un correspondiente registro almacenado en la aplicación de pagos 620 y en la base de datos de servidor de pasarela de pagos 506 que incluye un identificador para la red de pagos asociada con la tarjeta de financiación, un identificador de tarjeta de financiación, etc.

La aplicación de pagos 620 envía el identificador de dispositivo móvil al servidor de pasarela de pagos 506 para autenticación de dispositivo (bloque 2307). La aplicación de pagos 620 también envía el tipo de transacción (acción seleccionada en el menú de la aplicación, en este caso, "Hacer una transferencia de parte a parte"), la cantidad a transferir (por ejemplo, dada) y el identificador de tarjeta de financiación para la tarjeta de financiación seleccionada al servidor de pasarela de pagos 506 (bloque 2308). El servidor de pasarela de pagos 506 almacena la información enviada por el dispositivo móvil 501, y también calcula los detalles con respecto a un ID de transferencia (bloque 2309). El ID de transferencia está asociado con la tarjeta de financiación y la cantidad especificada. También puede asociarse una fecha de caducidad con el ID de transferencia, de manera que el ID de transferencia ya no es válido después de un cierto periodo de tiempo. Por ejemplo, después de unos pocos minutos, o unas pocas horas, o un día, o algún otro período de tiempo a partir de la creación del ID de transferencia, el ID de transferencia ya no es válido. En otras palabras, si el usuario emisor va a transferir valor al usuario receptor, ha de hacerse antes de que expire el periodo de tiempo. El servidor de pasarela de pagos 506 envía el ID de transferencia al dispositivo móvil del usuario emisor 501 (bloque 2310). En una realización de ejemplo, el ID de transferencia está cifrado y puede descifrarse por la aplicación de dispositivo móvil del usuario emisor 620.

Como una realización de ejemplo alternativa, en lugar de que el servidor de pasarela de pagos 506 envíe el ID de transferencia al dispositivo móvil, el servidor de pasarela de pagos 506 envía en su lugar un valor de clave que el

dispositivo móvil puede usar para generar un ID de transferencia idéntico al generado por la pasarela de pagos servidor 506. Enviar un valor de clave puede ser más seguro, en caso de que un atacante intercepte el valor de clave. Se aprecia que, el dispositivo móvil 501 obtiene finalmente el ID de transferencia.

La aplicación de pagos del móvil 620 visualiza a continuación un mensaje que solicita al usuario que toque el dispositivo móvil del emisor 501 con el dispositivo móvil del receptor 1901 (bloque 2311). El usuario emisor 101 le dice al usuario receptor 1807 que se prepare para recibir los fondos, por ejemplo, "tocando" los dispositivos móviles entre sí (bloque 2312). En otras realizaciones de ejemplo, además de, o, como alternativa, el usuario emisor envía el ID de transferencia al usuario receptor a través de otros medios de comunicación, incluyendo Bluetooth, infrarrojos, correo electrónico, mensajería instantánea, mensajería de texto y otros medios inalámbricos y alámbricos.

En una realización de ejemplo, antes de transferir el ID de transferencia a la aplicación de pagos 620 en el dispositivo móvil 501 visualiza una GUI que solicita al usuario emisor que introduzca su PIN (por ejemplo, que debería ser el mismo PIN proporcionado cuando el usuario emisor se registró para el servicio). En una realización de ejemplo, el PIN se verifica en primer lugar. En otra realización de ejemplo, el servidor de pasarela de pagos 506, en su lugar, envía un valor de clave para generar un ID de transferencia, el PIN proporcionado de nuevo por el usuario emisor se usa con el valor de clave para generar un ID de transferencia. Si el PIN proporcionado por el usuario emisor es correcto, a continuación, el ID de transferencia generado por el dispositivo móvil 501 debería ser idéntico al ID de transferencia generado por el servidor de pasarela de pagos 506.

Volviendo a la Figura 24, después de que el usuario emisor le dice al usuario receptor que se prepare, el usuario receptor inicia la aplicación de pagos en el dispositivo móvil del receptor 1901 (bloque 2401). El dispositivo móvil del receptor 1901 determina si el usuario se ha registrado satisfactoriamente en el servicio (bloque 2402), y, en caso afirmativo, muestra un menú (bloque 2403). El usuario receptor proporciona una entrada para iniciar la recepción de fondos de parte a parte usando la aplicación de pagos (bloque 2404). A continuación, tanto el usuario receptor 1807 como el usuario emisor 101 tocan juntos sus dispositivos móviles 501, 1901 (bloques 2405 y 2406).

Este toque (o más específicamente la proximidad cercana de los dispositivos móviles) desencadena que el dispositivo móvil del emisor 501 envíe el ID de transferencia, a través de NFC (bloque 2407). En otra realización de ejemplo, se transfiere el ID de transferencia al dispositivo móvil del receptor 1901 a través de otras formas (por ejemplo, códigos de barras, códigos de barras 2D, código QR, mensajería, correo electrónico, etc.). En una realización de ejemplo, se envía el ID de transferencia desde el elemento seguro del dispositivo móvil 622. En otra realización de ejemplo, el envío del ID de transferencia no implica el elemento seguro del dispositivo móvil 622.

Continuando con la Figura 24, después de que el dispositivo móvil del receptor 1901 recibe el ID de transferencia desde el dispositivo móvil del emisor 501, el dispositivo móvil 1901 envía el mismo al servidor de pasarela de pagos 506 (bloque 2408). La pasarela de pagos 506 valida el ID de transferencia (bloque 2409), y si el ID de transferencia se valida satisfactoriamente, a continuación, el servidor de pasarela de pagos 506 recupera los detalles de la tarjeta de financiación del usuario emisor y la cantidad especificada asociada con el ID de transferencia (bloque 2410).

Para validar el ID de transferencia, el servidor de pasarela de pagos puede confirmar si el propio ID de transferencia es correcto (por ejemplo, coincide con un ID de transferencia almacenado en el servidor de pasarela de pagos). También puede comprobar para ver si el ID de transferencia ha expirado, y, en caso afirmativo, declinará la transferencia. También puede comprobar para ver si el ID de transferencia se ha usado previamente, y, en caso afirmativo, declinará la transferencia.

El servidor de pasarela de pagos 506 genera a continuación una solicitud de autorización de pago de transferencia de valor, que incluye los detalles de la tarjeta de financiación y la cantidad a transferir al usuario receptor 1807 (bloque 2411). Aunque no se muestra, el servidor de pasarela de pagos 506 a continuación envía esta solicitud de autorización de pago convencional al servidor de emisión de tarjetas de financiación 104. El servidor de emisión de tarjetas de financiación 104 verifica la solicitud de autorización de pago (por ejemplo, verifica que hay suficientes fondos disponibles, verifica datos de tarjeta de financiación, etc.) y proporciona una respuesta de autorización de pago al servidor de pasarela de pagos 506. La respuesta indica si se acepta o deniega la transferencia de valor.

Suponiendo que se acepta el pago usando la tarjeta de financiación, el servidor de pasarela de pagos 506 marca el ID de transferencia como usado (bloque 2412). Se observa que el ID de transferencia es un solo uso. En otras palabras, cuando el emisor desea realizar otra transferencia de parte a parte, se creará un nuevo ID de transferencia (por ejemplo, diferente) para la otra transferencia de parte a parte, incluso si se están utilizando la misma tarjeta de financiación y cantidad. De esta manera, hay mayor seguridad, y el usuario receptor nunca obtendrá los detalles de la tarjeta de financiación del usuario emisor.

El servidor de pasarela de pagos 506 calcula una tarjeta virtual de prepago que va a emitirse al usuario receptor, y los detalles asociados con la misma (bloque 2413). La tarjeta virtual de prepago se almacena en asociación con el ID de dispositivo móvil del receptor. La cantidad de dinero transferida (desde el usuario emisor) es la cantidad de dinero asociada (por ejemplo, disponible) en la tarjeta virtual de prepago. El servidor de pasarela de pagos 506 a continuación envía detalles acerca de la tarjeta virtual de prepago (por ejemplo, un identificador de tarjeta virtual de prepago) al

dispositivo móvil del receptor (bloque 2414).

En particular, el servidor de pasarela de pagos calcula un identificador de tarjeta virtual de prepago que identifica la cuenta de tarjeta virtual de prepago. El servidor de pasarela de pagos almacena el identificador de tarjeta virtual de prepago en asociación con los detalles de tarjeta virtual de prepago, y envía el identificador de tarjeta virtual de prepago al dispositivo móvil del usuario receptor para su almacenamiento. En una realización de ejemplo, el identificador de tarjeta virtual de prepago es un valor que es diferente del PAN, fecha de caducidad o código de seguridad estático de la tarjeta virtual de prepago. Por ejemplo, el identificador de tarjeta virtual de prepago es un valor aleatorio de modo que, si es interceptado por un adversario, no sería capaz de reconocer ningún detalle de tarjeta virtual de prepago. En una realización de ejemplo, el dispositivo móvil del usuario receptor no almacena ningún detalle de tarjeta virtual de prepago o almacena detalles de tarjeta virtual de prepago limitados (por ejemplo, el nombre del emisor de tarjeta virtual de prepago y los últimos 4 dígitos del PAN). En una realización de ejemplo, el dispositivo móvil del usuario receptor almacena al menos el identificador de tarjeta virtual de prepago, que envía al servidor de pasarela de pagos para indicar la tarjeta virtual de prepago asociada.

Después de la recepción del identificador de tarjeta virtual de prepago, el dispositivo móvil del receptor almacena esta información (bloque 2415) y visualiza un mensaje al usuario receptor de que la nueva tarjeta virtual de prepago está disponible (bloque 2416).

El servidor de pasarela de pagos 506 también puede enviar un mensaje de confirmación al dispositivo móvil del emisor 501 que indica que se ha emitido la nueva tarjeta virtual de prepago al receptor (bloque 2417).

Después de que el receptor 1807 tenga la tarjeta virtual de prepago, el receptor puede usar la tarjeta virtual de prepago para realizar una compra con un comerciante.

Transferir valor de parte a parte usando una tarjeta virtual

En otra realización de ejemplo, en lugar de usar un ID de transferencia, se envía una tarjeta virtual, en lugar del ID de transferencia, para facilitar la transferencia de valor desde el usuario emisor al usuario receptor. La tarjeta virtual está asociada con la tarjeta de financiación. Cuando se usa la tarjeta virtual, el usuario receptor no puede obtener información acerca de la tarjeta de financiación del usuario emisor. Esto aumenta la seguridad. Los resultados de la transferencia son que el usuario receptor tiene una tarjeta virtual de prepago que puede usarse para pago u otra transferencia de parte a parte. La tarjeta virtual en ocasiones se denomina en las Figuras como "Vcard".

A modo de antecedentes, el elemento seguro se gestiona típicamente por un operador de telefonía móvil que distribuye el elemento seguro con el dispositivo móvil. Se usa en parte para mantener la seguridad de las diversas aplicaciones que se ejecutan dentro del elemento seguro. Parte del servicio gestionado incluye entregar aplicaciones en el elemento seguro directamente, o dar permiso a una organización de terceros para desplegar su aplicación en un elemento seguro particular. El servicio gestionado se entrega típicamente usando lo que la industria denomina como un gestor de servicios de confianza (TSM).

Todas las aplicaciones almacenadas y que se ejecutan dentro del elemento seguro, tal como la "tarjeta de pago de software" individual, necesitan su propio espacio de almacenamiento. Las tarjetas de pago se emiten a los consumidores por el emisor de la tarjeta. El despliegue de tarjetas de pago de software en teléfonos móviles requiere un alto nivel de coordinación entre el operador de telefonía móvil y el emisor de tarjeta donde el operador de telefonía móvil proporciona acceso a elementos seguros individuales, uno cada vez, al emisor. Únicamente las tarjetas de emisores de tarjetas de financiación que tienen la infraestructura y el acuerdo con el operador de telefonía móvil pueden entregarse y usarse en el teléfono móvil para pago sin contacto. Esto es limitante tanto para los emisores de tarjetas como para los titulares de tarjetas.

También se reconoce que, desde la perspectiva del usuario, el proceso de asociar su dispositivo móvil con su tarjeta de financiación que va a usarse para pago sin contacto depende mucho de relaciones preestablecidas entre el operador de telefonía móvil y los emisores de tarjetas. Por lo tanto, un usuario tiene opciones limitadas o ninguna opción cuando determina si su tarjeta de financiación actual puede asociarse con su teléfono móvil para pagos sin contacto. Por ejemplo, un usuario tiene una tarjeta de financiación del emisor de tarjeta de pago A. El usuario también tiene un teléfono móvil habilitado para NFC del operador de teléfono móvil B. Sin embargo, el operador de teléfono móvil B únicamente tiene un acuerdo e infraestructura preestablecidos para facilitar los pagos sin contacto con el emisor de tarjeta de financiación B. Por lo tanto, incluso si el usuario quisiera usar su teléfono móvil para realizar un pago sin contacto, el usuario no podría hacerlo porque no existe un acuerdo preestablecido e infraestructura entre el operador de teléfono móvil B y el emisor de tarjeta de financiación A para emitir una tarjeta de pago de software en el teléfono del usuario. Esto limita la capacidad del usuario para realizar pagos de tipo NFC con su dispositivo móvil.

En otra realización de ejemplo, los datos dinámicos de tarjeta de pago son un valor de verificación de tarjeta rotatoria (CVV, también denominado en algún momento CVV dinámico o dCVV). Este CVV rotatorio puede calcularse basándose en información cambiante proporcionada por el circuito integrado dentro de la tarjeta. En otra realización de ejemplo, los datos dinámicos son datos de EMV dinámicos que se calculan usando datos aleatorios de la tarjeta

de financiación, o datos aleatorios del terminal de punto de venta de un comerciante, o ambos. Una implementación común de datos dinámicos usa un contador de transacciones de aplicación (ATC) en la tarjeta para que cada transacción produzca un flujo de datos diferente. Esto se logra a medida que el ATC se incrementa en 1 para cada transacción realizada.

También se reconoce que la aplicación específica para una tarjeta de financiación dada puede instalarse en el dispositivo móvil y usarse para interactuar con el terminal de POS como se ha descrito anteriormente. También se reconoce que la aplicación de tarjeta se instala típicamente en el elemento seguro del dispositivo móvil. Típicamente, cada tarjeta de financiación tiene su propia aplicación de tarjeta correspondiente que reside en el elemento seguro del dispositivo móvil. Puede apreciarse que, como cada aplicación de tarjeta ocupa espacio de almacenamiento en el elemento seguro, y que el elemento seguro típicamente tiene un espacio de almacenamiento muy limitado, tener múltiples aplicaciones de tarjeta en el elemento seguro en algunos casos no es posible debido a espacio de almacenamiento insuficiente. A modo de antecedentes, el elemento seguro puede tener un sistema operativo nativo que se programe para realizar diversas tareas y actividades, incluyendo, por ejemplo, una aplicación de tarjeta que emula los datos de banda magnética de una tarjeta de financiación o una aplicación de tarjeta que emula los datos usados en un pago sin contacto EMV. También, a modo de antecedentes, y a modo de ejemplo, un elemento seguro típico tiene memoria de 256 kB, y cada aplicación de tarjeta puede consumir memoria de 40-80 kB. Por lo tanto, puede apreciarse que asociar múltiples tarjetas de financiación (y cada una de sus aplicaciones de tarjeta) con un dispositivo móvil para pagos de NFC puede estar limitado.

Por lo tanto, es deseable reducir la cantidad de espacio de almacenamiento requerido que necesitan las aplicaciones de tarjeta en el elemento seguro para no limitar el número de tarjetas de pago de software que un usuario puede cargar en un elemento seguro. En la misma línea, es deseable que los operadores de telefonía móvil reduzcan la cantidad de datos usados por la "aplicación de tarjeta" en el elemento seguro de modo que puedan cargarse otros tipos de aplicaciones en el mismo. También es deseable reducir costes incurridos por el emisor de tarjeta de financiación para emitir y operar tarjetas de pago de software en elementos seguros. A modo de antecedentes, un operador de telefonía móvil típicamente cobra a los proveedores de aplicaciones, tales como emisores de tarjetas de financiación, por la cantidad de espacio de almacenamiento usado en el elemento seguro. También es deseable reducir la cantidad de infraestructura requerida por el emisor de tarjeta de financiación para emitir una tarjeta de pago de software para el teléfono móvil. También es deseable reducir la cantidad de coordinación requerida entre el emisor de la tarjeta de financiación y el operador de telefonía móvil para emitir una tarjeta de pago de software en un teléfono móvil particular. También es deseable permitir que el usuario (por ejemplo, el titular de la tarjeta) cargue cualquiera, y tantas, tarjetas de financiación que desee en su teléfono móvil habilitado para NFC, independientemente del emisor de la tarjeta de financiación que tenga la infraestructura o una relación comercial o acuerdo con un operador de telefonía móvil particular. También es deseable permitir que el usuario (por ejemplo, el titular de la tarjeta) cargue cualquiera, y tantas, tarjetas de financiación que desee en su teléfono móvil habilitado para NFC, independientemente del emisor de la tarjeta de financiación que tenga la infraestructura o una relación comercial o acuerdo con un operador de telefonía móvil particular. También es deseable facilitar la transferencia de dinero entre dos usuarios de una manera de parte a parte usando sus dispositivos móviles habilitados para NFC.

Los sistemas y métodos descritos en el presente documento también permiten que un servidor de pasarela de pagos de monedero basado en la nube se sincronice con un dispositivo móvil habilitado para NFC del receptor y una aplicación para facilitar transferencias de valor sin contacto desde un dispositivo móvil habilitado para NFC del emisor. Un usuario emisor selecciona una tarjeta de financiación y proporciona la cantidad para realizar la transferencia de valor de parte a parte sin contacto, a través de su dispositivo móvil. Se genera una segunda tarjeta, denominada en el presente documento como una tarjeta virtual, junto con todos los datos de tarjeta requeridos (por ejemplo, PAN, fecha de caducidad, datos dinámicos, datos discrecionales, etc.) para facilitar la transacción de pago de parte a parte. En el servidor de pasarela de pagos, la tarjeta virtual se asocia temporalmente con la tarjeta de financiación y la cantidad permitida de valor a transferir. El usuario emisor envía los datos de tarjeta virtual y la cantidad a transferir al usuario receptor (por ejemplo, a través de NFC u otros medios de comunicación). El usuario receptor envía estos datos al servidor de pasarela de pagos y valida los datos de tarjeta virtual. Si se valida, el servidor de pasarela de pagos recupera los detalles de la tarjeta de financiación y usa los mismos para transferir la cantidad especificada desde la tarjeta de financiación a una nueva tarjeta virtual de prepago. La tarjeta virtual de prepago puede usarse por el usuario receptor para realizar pagos, transacciones, transferencias de parte a parte, etc.

Volviendo a la Figura 25, se muestran componentes de realización de ejemplo de un sistema para facilitar una transferencia de fondos de parte a parte usando la tarjeta virtual. La Figura 25 es similar a la Figura 19, sin embargo, difiere en que las asociaciones de datos temporales 1905 incluyen una tarjeta virtual (por ejemplo, la tarjeta virtual 1) 2501 que está asociada temporalmente con una de las tarjetas de financiación del usuario 505. La tarjeta virtual 1101 puede usarse por el usuario emisor 101 para realizar una transferencia de valor de parte a parte.

Volviendo a las Figuras 26 y 27, se proporcionan instrucciones ejecutables por ordenador o implementadas por procesador de ejemplo para facilitar una transferencia de fondos de parte a parte entre un usuario emisor y un usuario receptor. Los ejemplos de las Figuras 26 y 27 son similares a las Figuras 23 y 24, pero usan una tarjeta virtual en lugar de un ID de transferencia. Por lo tanto, elementos o etapas similares no se repiten en el análisis de las Figuras 26 y 27.

Se supone que el dispositivo móvil del emisor ha experimentado un proceso de registro, que incluye proporcionar el PIN. Un ejemplo de un proceso de este tipo se describe más adelante con respecto a la Figura 28.

Volviendo a la Figura 26, se realizan los bloques 2301 a 2308. Después de recibir la solicitud 2308, basándose en la información enviada por el dispositivo móvil 501, el servidor de pasarela de pagos 404 crea y calcula los detalles con respecto a la tarjeta virtual (bloque 2601). En particular, el servidor de pasarela de pagos 506 calcula un PAN virtual, una fecha de caducidad de la tarjeta virtual y otros datos que forman los datos de pista dos. Se observa que los datos de pista dos incluyen, entre otras cosas; el PAN, un código de servicio, una fecha de caducidad, datos discrecionales y un LRC. En una realización de ejemplo, el servidor de pasarela de pagos 506 en este momento no calcula los datos discrecionales, que son de naturaleza dinámica (por ejemplo, los datos discrecionales son datos dinámicos). Los detalles de la tarjeta virtual pueden incluir además una fecha de caducidad interna que es conocida únicamente por el servidor de pasarela de pagos, y tiene una línea de tiempo corta de aproximadamente unos pocos días desde la fecha en la que se crea la tarjeta virtual. La fecha de caducidad interna es diferente de la fecha de caducidad de la tarjeta virtual, y la función de la fecha de caducidad interna es proporcionar un indicador adicional a la pasarela de pagos para determinar si una tarjeta virtual ha caducado o no. El servidor de pasarela de pagos 506 cifra los datos de tarjeta virtual, que no incluyen la fecha de caducidad interna, y envía la carga útil de tarjeta virtual cifrada a la aplicación de pagos del dispositivo móvil 620 (bloque 2602).

Como una realización de ejemplo alternativa, en lugar de que el servidor de pasarela de pagos 506 envíe el PAN de tarjeta virtual como parte de la carga útil de tarjeta virtual cifrada al dispositivo móvil, el servidor de pasarela de pagos 506, en su lugar, envía un valor de clave (llamado Kpan) que el dispositivo móvil puede usar para generar un PAN de tarjeta virtual idéntico según lo calculado por el servidor de pasarela de pagos 506. Este ejemplo se describe en la Figura 29.

En una realización de ejemplo, la primera porción de dígitos del PAN de la tarjeta virtual es estática y se refiere al servidor de pasarela de pagos 506. Por ejemplo, los primeros seis dígitos apuntan al servidor de pasarela de pagos 506; un comerciante o red de pagos, o cualquier otra entidad, puede usar esta información para enviar los detalles de transacción y pago al servidor de pasarela de pagos 506.

En una realización de ejemplo, el PAN de la tarjeta virtual tiene una longitud de diecinueve dígitos y cumple con el algoritmo LUHN-10. El algoritmo, también conocido como el algoritmo de "módulo 10" o "mod 10", es una fórmula de suma de comprobación usada para validar una diversidad de números de identificación, tales como números de tarjeta. Como se ha descrito anteriormente, los primeros seis dígitos se usan para identificar el servidor de pasarela de pagos. Los dígitos restantes se pueden calcular de varias maneras. En una realización de ejemplo, los dígitos restantes del PAN de tarjeta virtual se generan aleatoriamente. En otra realización de ejemplo, los dígitos restantes se calculan usando el valor de Kpan; se describen detalles adicionales a este respecto con respecto a la Figura 29. Pueden usarse otros métodos para calcular el PAN de tarjeta virtual. El dispositivo móvil 501 recibe la carga útil de tarjeta virtual cifrada, descifra la comunicación cifrada y extrae los detalles de tarjeta virtual (por ejemplo, el PAN de tarjeta virtual y otros detalles de tarjeta).

En otra realización de ejemplo, si la carga útil de tarjeta virtual incluye un Kpan (por ejemplo, un valor de clave) en lugar de un PAN de tarjeta virtual, el dispositivo móvil 501 usa el Kpan para calcular el PAN de tarjeta virtual.

Continuando con la Figura 26, la aplicación de pagos 620 en el dispositivo móvil 501 visualiza una GUI que solicita al usuario emisor que introduzca su PIN (por ejemplo, que debería ser el mismo PIN proporcionado cuando el usuario emisor se registró para el servicio) (bloque 2603). La aplicación 620 recibe el PIN del usuario emisor (por ejemplo, el usuario emisor introduce el PIN) (bloque 2604). La aplicación 620 usa el PIN para calcular los datos discrecionales de la tarjeta virtual (bloque 2605). Una realización de ejemplo de cálculo de los datos discrecionales se describe a continuación con respecto a la Figura 30. Con los datos discrecionales calculados, el conjunto de datos de la pista dos está completo. La aplicación de pagos del móvil 620 visualiza a continuación un mensaje que solicita al usuario que toque el dispositivo móvil del emisor 402 con el dispositivo móvil del receptor 1901 (bloque 2311). El usuario emisor 101 le dice al usuario receptor 1807 que se prepare para recibir los fondos (bloque 2312).

En una realización de ejemplo, puede usarse un PIN para todas las tarjetas de financiación asociadas con el dispositivo móvil. En otra realización de ejemplo, el proceso de registro puede solicitar un PIN específico para cada tarjeta de financiación. En otras palabras, si un usuario selecciona una tarjeta de financiación diferente, el usuario necesitará introducir un PIN diferente.

En una realización de ejemplo, la aplicación de pagos del dispositivo móvil 620 no verifica el PIN. En su lugar, el PIN se verifica indirecta o implícitamente por el servidor de pasarela de pagos 506 cuando se verifica el conjunto de datos de tarjeta virtual. En otras palabras, el servidor de pasarela de pagos 506 usa el PIN que se almacenó en el momento del registro para calcular el conjunto de datos de tarjeta virtual, y si el usuario o un adversario proporcionó un PIN incorrecto durante la transacción, hará que los datos virtuales calculados den como resultado un valor diferente, incorrecto, en comparación con los datos de tarjeta virtual calculados por el servidor de pasarela de pagos. Una vez que el conjunto de datos de tarjeta virtual recibido se compara con el valor esperado por el servidor de pasarela de

pagos, puede detectarse una entrada de PIN no válida. Cuando el servidor de pasarela de pagos recibe y verifica el conjunto de datos de tarjeta virtual y detecta un conjunto de datos de tarjeta virtual inesperado (por ejemplo, debido al PIN incorrecto), a continuación, puede declinarse la autorización de transferencia de valor.

Volviendo a la Figura 27, después de que el usuario emisor le dice al usuario receptor que se prepare, el usuario receptor inicia la aplicación de pagos en el dispositivo móvil del receptor 1901 (bloque 2401). Se realizan los bloques 2401 a 2406, conduciendo a los dispositivos móviles de ambos usuarios a que toquen juntos sus teléfonos para transferir datos a través de NFC.

Este toque (o más específicamente la proximidad cercana de los dispositivos móviles) desencadena que el dispositivo móvil del emisor 501 envíe la cantidad autorizada y los datos de la pista dos para la tarjeta virtual en el elemento seguro del dispositivo móvil 622 (bloque 2701). El dispositivo móvil 501 configura los datos de la pista dos para emular una tarjeta virtual, y estos datos de tarjeta virtual emulados y la cantidad autorizada se proporcionan al subsistema de NFC 609 del dispositivo móvil (bloque 2702). Los datos de tarjeta virtual emulados incluyen el conjunto de datos de pista dos completo. La cantidad a transferir y los datos de tarjeta virtual se transfieren a continuación, a través de NFC, al dispositivo móvil del usuario de recepción 1901 (bloque 2703). En otra realización de ejemplo, aunque no se muestra, el sistema operativo del dispositivo móvil 501 puede transferir directamente información al subsistema de NFC 609 sin el uso del elemento seguro. El conjunto de datos de tarjeta virtual incluye el PAN de tarjeta virtual, la fecha de caducidad, los datos discrecionales y todos los otros elementos en un conjunto de datos de pista dos para completar una transferencia de valor sin contacto convencional.

Continuando con la Figura 27, después de que el dispositivo móvil del receptor 1901 recibe los datos de tarjeta virtual y la cantidad autorizada desde el dispositivo móvil del emisor 501, el dispositivo móvil 1901 envía los mismos al servidor de pasarela de pagos 506 (bloque 2704). La pasarela de pagos 506 valida los datos de tarjeta virtual y la cantidad autorizada (bloque 2705), y si los datos se validan satisfactoriamente, a continuación, el servidor de pasarela de pagos 506 recupera la asociación de detalles de tarjeta de financiación con la tarjeta virtual del emisor (bloque 2706).

Para validar los datos de tarjeta virtual recibidos desde el dispositivo móvil del emisor, el servidor de pasarela de pagos calcula el conjunto de datos de pista dos por sí mismo. El cálculo de datos de pista dos incluye que el servidor de pasarela de pagos calcule los datos discrecionales usando el PIN originalmente recibido y almacenado durante el registro por el usuario emisor. En una realización de ejemplo, se precalcularon y almacenaron algunas de las porciones de datos de la pista dos (como el PAN y la fecha de caducidad); estas porciones de datos precalculadas pueden compararse con los datos de pista dos recibidos. Si los datos de tarjeta virtual se validan satisfactoriamente (el conjunto de datos de la pista dos de la tarjeta recibida coincide con el conjunto de datos de pista dos de la tarjeta calculados por el servidor de la pasarela de pagos), a continuación, el servidor de la pasarela de pagos recupera los datos de tarjeta de financiación que están asociados con la tarjeta de datos de la tarjeta virtual.

La validación de los datos de tarjeta virtual en el bloque 2705 también puede incluir verificar si ha pasado o no la fecha de caducidad interna asociada con la tarjeta virtual. Si la fecha actual de la validación se produce antes o en la fecha de caducidad interna, a continuación, la tarjeta virtual puede considerarse validada y el procesamiento de la transacción puede continuar. Si se valida, el servidor de pasarela de pagos 506 recupera detalles de la tarjeta de financiación 2706. De lo contrario, la tarjeta virtual se considera no válida y se deniega la solicitud de autorización de transferencia de valor.

Cuando se valida, el servidor de pasarela de pagos 506 genera a continuación una solicitud de pago de autorización de transferencia de valor, que incluye los detalles de la tarjeta de financiación y la cantidad a transferir al usuario receptor 1807 (bloque 2707). Aunque no se muestra, el servidor de pasarela de pagos 506 a continuación envía esta solicitud de autorización de pago convencional al servidor de emisión de tarjetas de financiación 104. El servidor de emisión de tarjetas de financiación 104 verifica la solicitud de autorización de pago (por ejemplo, verifica que hay suficientes fondos disponibles, verifica datos de tarjeta de financiación, etc.) y proporciona una respuesta de autorización de pago al servidor de pasarela de pagos 506. La respuesta indica si se acepta o deniega la transferencia de valor.

Suponiendo que se acepta el pago usando la tarjeta de financiación, el servidor de pasarela de pagos 506 marca la tarjeta virtual del emisor como en uso (bloque 2708). Se observa que la tarjeta virtual es de un solo uso. En otras palabras, cuando el emisor desea realizar otra transferencia de parte a parte, se creará una nueva tarjeta virtual (por ejemplo, diferente) para la otra transferencia de parte a parte, incluso si se están utilizando la misma tarjeta de financiación y cantidad. De esta manera, hay mayor seguridad, y el usuario receptor nunca obtendrá los detalles de la tarjeta de financiación del usuario emisor.

El servidor de pasarela de pagos 506 calcula una tarjeta virtual de prepago que va a emitirse al usuario receptor, y los detalles asociados con la misma (bloque 2709).

Después de generar la tarjeta virtual de prepago, se realizan los bloques 2414, 2415, 2416 y 2417. Estos se describieron previamente con respecto a la Figura 24.

Volviendo a la Figura 28, se proporciona una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para registrar una tarjeta de financiación y un dispositivo móvil con un servidor de pasarela de pagos. Una realización de este tipo puede combinarse con los principios descritos anteriormente. El dispositivo móvil del emisor envía una solicitud de registro al servidor de pasarela de pagos (bloque 2801). La solicitud incluye el ID de dispositivo del dispositivo móvil, un PIN proporcionado por el usuario y detalles de la tarjeta de financiación. Después de recibir la solicitud, el servidor de pasarela de pagos envía una respuesta de registro al dispositivo móvil del emisor (bloque 2802). La respuesta incluye un certificado, un contador de transacciones de aplicación (ATC), un valor de clave (llamado Kpan) para generar un PAN, un valor de clave de elemento seguro (llamado Ksec) y un identificador de tarjeta de financiación que identifica la tarjeta de financiación. El certificado es un certificado de cliente para el dispositivo móvil del emisor y, en una realización de ejemplo, está configurado de acuerdo con el algoritmo de RSA y tiene una longitud de 2048 bits. El ATC es un contador que se establece inicialmente a un valor aleatorio entre "0" o "1000" y se incrementa con cada transacción. El valor de ATC inicializado es un valor aleatorio para evitar que los adversarios predigan los valores de ATC. Se almacenan copias del ATC y se sincronizan tanto en el servidor de pasarela de pagos como en el dispositivo móvil. En una realización de ejemplo, el ATC es un valor de 10 dígitos. En una realización de ejemplo, el Kpan tiene una longitud de 128 bits y el Ksec tiene una longitud de 128 bits.

El servidor de pasarela de pagos 404 almacena los datos de la solicitud de registro y la respuesta de registro en asociación entre sí (bloque 2803). El dispositivo móvil del emisor 402 también almacena los datos de la respuesta de registro (bloque 2804).

Volviendo a la figura 29, se proporciona una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para calcular datos de tarjeta virtual. Una realización de este tipo puede usarse en combinación con los principios descritos anteriormente para calcular datos de tarjeta virtual. El dispositivo móvil del emisor envía una solicitud de tarjeta virtual al servidor de pasarela de pagos (bloque 2901). La solicitud incluye el ID de dispositivo, el identificador de tarjeta de financiación, el certificado y el Kpan almacenado. El Kpan almacenado puede ser del registro o de la transacción anterior.

El servidor de pasarela de pagos determina si el Kpan y el certificado recibidos coinciden con el Kpan y el certificado almacenados en el servidor de pasarela de pagos (bloque 2902) asociado con el ID de dispositivo almacenado en la base de datos de servidor de pasarela de pagos. En caso afirmativo, a continuación, el servidor de pasarela de pagos envía una respuesta de tarjeta virtual al dispositivo móvil del emisor que incluye un nuevo Kpan (bloque 2903). Se usa un nuevo Kpan para generar un PAN nuevo o diferente para cada transacción, y para evitar también contra ataques de reproducción. El servidor de pasarela de pagos calcula el PAN para la tarjeta virtual usando el nuevo Kpan (bloque 2904). Este nuevo Kpan y el PAN precalculado se almacenan por el servidor de pasarela de pagos para su uso posterior (bloque 2905).

Después de que el dispositivo móvil recibe el nuevo Kpan, reemplaza el Kpan almacenado con el nuevo Kpan (bloque 2906). Usa el nuevo Kpan para calcular un PAN para la tarjeta virtual, de la misma manera que el servidor de pasarela de pagos calculó el PAN (bloque 2907), si las condiciones y los datos son correctos, aunque el dispositivo móvil calcula el PAN independientemente del servidor de pasarela de pagos, el PAN calculado por el dispositivo móvil debe ser idéntico al PAN calculado por el servidor de pasarela de pagos.

El dispositivo móvil a continuación calcula los datos discrecionales (que son parte de los datos de pista dos) usando el PIN, el Ksec, el PAN, el certificado y el ATC (bloque 2908). El PAN sigue cambiando con cada transacción, lo que hace que los datos discrecionales sean datos dinámicos.

El dispositivo móvil incrementa el ATC en 1 (bloque 2909).

En particular, el PAN se calcula por el dispositivo móvil y el servidor de pasarela de pagos de acuerdo con lo siguiente:
PAN = BIN(6) + SHA256[Kpan](12) + Luhn(1)
en donde
BIN(6) es un número binario de 6 dígitos para identificar el servidor de pasarela de pagos;
SHA256[Kpan](12) es un número de 12 dígitos generado tomando el sha256 del valor de Kpan, incluyendo además convertir el valor de sha256 a decimal y truncando a doce dígitos del valor de función de troceo;
y
Luhn(1) es un único dígito usado para garantizar que la tarjeta virtual siempre pase el algoritmo de LUHN.

Los valores anteriores se concatenan juntos para formar el PAN. El símbolo "+" en el cálculo anterior se refiere a la operación de concatenación.

Los datos discrecionales se calculan usando lo siguiente:
Datos discrecionales = HMAC_SHA256[Ksec+PIN,M](10)
donde M = concatenación de (PAN, ID de certificado, ATC)

El truncamiento se realiza codificando los resultados de SHA en decimal, tomando a continuación los dígitos más a la izquierda. Puede apreciarse que SHA256 es una función de troceo criptográfica conocida, y HMAC es un código de autenticación de mensaje basado en función de troceo que implica una función de troceo criptográfica en combinación con una clave criptográfica secreta. La clave criptográfica secreta de la función de HMAC son los valores concatenados de Ksec y PIN. El mensaje M son los valores concatenados de PAN, ID de certificado y ATC. El ID de certificado es del certificado.

Volviendo a la Figura 30, se proporciona una realización de ejemplo de instrucciones ejecutables por ordenador o implementadas por procesador para verificar datos de tarjeta virtual, y, en particular, la verificación por el servidor de pasarela de pagos de los datos discrecionales (por ejemplo, los datos dinámicos). Una realización de este tipo puede usarse en combinación con los principios descritos anteriormente para verificar los datos de tarjeta virtual. Esto puede ser una continuación del proceso descrito en la Figura 26.

El dispositivo móvil del emisor 501 envía una tarjeta virtual al dispositivo móvil del receptor 1901 (bloque 3001). El dispositivo móvil del receptor 1901 a continuación crea y envía una solicitud de autorización de transferencia de valor al servidor de pasarela de pagos 506 (bloque 3002). La solicitud de autorización de transferencia de valor incluye, entre otras cosas, el PAN y los datos discrecionales de la tarjeta virtual, según se calculan por el dispositivo móvil del emisor. También incluye la cantidad de dinero o fondos a transferir desde el emisor al receptor.

Después de recibir la solicitud, el servidor de pasarela de pagos 506 usa el PAN para encontrar los datos asociados almacenados relevantes (por ejemplo, Kpan, certificado, Ksec, identificador de tarjeta de financiación, ID de dispositivo y otros datos de usuario). Los datos asociados almacenados relevantes se identifican por el PAN precalculado, que actúa como un índice. En otras palabras, el PAN recibido se compara con un número de PAN precalculados, y si se encuentra una coincidencia con un PAN precalculado dado, a continuación, los datos almacenados asociados con ese PAN precalculado dado se consideran los datos asociados almacenados relevantes.

El servidor de pasarela de pagos 506 usa los datos asociados almacenados relevantes para calcular sus propios datos discrecionales. Esto puede incluir usar el PIN (recibido durante el proceso de registro de usuario), el Ksec almacenado, el ID de certificado del certificado almacenado y un valor incrementado del ATC (bloque 3003).

El cálculo de los propios datos discrecionales de la pasarela de pagos usa lo siguiente:
Datos discrecionales = HMAC_SHA256[Ksec+PIN,M](10)
donde M = concatenación de (PAN, ID de certificado, (ATC +1))

El ATC+1 representa el valor de ATC incrementado.

El servidor de pasarela de pagos 506 determina si sus propios datos discrecionales son iguales a los datos discrecionales recibidos (bloque 3004). Si no son iguales, el servidor de pasarela de pagos incrementa además el ATC en "1" y recalcula sus propios datos discrecionales (bloque 3005). El proceso vuelve al bloque 3004 para comprobar si los conjuntos de datos discrecionales son iguales. El proceso que implica el bloque 3005 puede repetirse, de modo que cada vez el valor de ATC se incremente además en 1. Esto se puede hacer hasta un cierto número de veces (por ejemplo, 10 veces), después de lo cual se detendrá el proceso de transacción.

Si el intervalo de valores de ATC (por ejemplo, entre ATC+1 y ATC+10) no genera un conjunto de datos discrecional idéntico, a continuación, la verificación es infructuosa. El intervalo es para tener en cuenta la posibilidad de que el contador de ATC del dispositivo móvil pueda haberse incrementado sin el conocimiento del servidor de pasarela de pagos. Por lo tanto, se usa una memoria intermedia o intervalo o valores de ATC.

Si los propios datos discrecionales del servidor de pasarela de pagos son los mismos que los datos discrecionales recibidos, a continuación, el servidor de pasarela de pagos reemplaza el valor de ATC anterior con el valor de ATC actualmente incrementado que se usa en el cálculo de sus propios datos discrecionales (bloque 3006). De esta manera, el valor de ATC almacenado en el servidor de pasarela de pagos debería ser ahora igual al valor de ATC almacenado en el dispositivo móvil. Esto conduce a que se acepte la solicitud de autorización y, en consecuencia, el servidor de pasarela de pagos emite una tarjeta de prepago virtual para el dispositivo móvil del receptor (bloque 1607).

Se observa que, si el PIN usado por el dispositivo móvil para calcular los datos discrecionales se introduce incorrectamente por el usuario (por ejemplo, no es el mismo que el PIN proporcionado en el registro), a continuación, los datos discrecionales del dispositivo móvil no igualarán los propios datos discrecionales del servidor de pasarela de pagos. Esto es debido a que los propios datos discrecionales del servidor de pasarela de pagos se calculan usando el PIN proporcionado en el registro. De esta manera, se verifica implícitamente el PIN proporcionado por el usuario en el dispositivo móvil durante cada transacción por el servidor de pasarela de pagos.

Continuando con la Figura 30, después de que los datos se verifiquen de manera satisfactoria o no, el servidor de pasarela de pagos finalmente responde al dispositivo móvil del receptor enviando una respuesta al dispositivo móvil del receptor. La respuesta puede indicar que se declina la transferencia, o puede indicar que se ha emitido una tarjeta de prepago virtual.

En particular, según el bloque 3005, hay un límite superior de iteraciones que, cuando se alcanza, significa que la verificación de datos discrecional no es satisfactoria. Si la verificación no es satisfactoria, a continuación, se envía una respuesta de transferencia declinada al dispositivo móvil del receptor 1901 (bloque 3008). Si la verificación es satisfactoria, como se ha descrito anteriormente, se inicia el proceso para emitir una tarjeta de prepago virtual y se entrega al dispositivo móvil del receptor 1901 (bloque 3007).

Por lo tanto, puede apreciarse que un usuario emisor puede transferir valor a un usuario receptor de diversas formas, incluyendo usar un ID de transferencia o una tarjeta virtual. El resultado de una transferencia satisfactoria es que el usuario receptor tiene una tarjeta virtual de prepago.

En una realización de ejemplo, después de que el usuario receptor recibe la tarjeta virtual de prepago, el usuario receptor puede usar la tarjeta virtual de prepago para realizar un pago con un comerciante. Por ejemplo, la tarjeta virtual de prepago puede usarse para hacer un pago usando un terminal de POS 502 o una interfaz base de comercio electrónico e Internet 1301.

Los métodos y sistemas descritos en el presente documento pueden usarse con cualquier tipo de tarjeta de financiación. Las tarjetas de financiación del emisor y el dispositivo móvil se pre-registran con el servidor de pasarela de pagos 506. Este registro es independiente de cualquier operador de telefonía móvil particular y cualquier emisor de tarjeta de crédito de financiación particular. Como resultado, no se requiere ningún acuerdo comercial e infraestructura adicional entre un operador de telefonía móvil y un emisor de tarjeta de financiación para facilitar el pago sin contacto (por ejemplo, NFC) usando un dispositivo móvil. Esto, a su vez, reduce el coste incurrido por el emisor de tarjeta de financiación para emitir tarjetas de pago a dispositivos móviles.

En una realización de ejemplo, se proporciona un método realizado por un servidor para facilitar una transferencia de valor de parte a parte. El método incluye: recibir un mensaje desde el dispositivo móvil de un emisor para transferir una cantidad especificada usando un identificador de tarjeta de financiación; buscar en una base de datos de múltiples tarjetas asociadas con el dispositivo móvil del emisor detalles de tarjeta de financiación asociados con el identificador de tarjeta de financiación y cantidad; generar un ID de transferencia y asociar el ID de transferencia con el número de tarjeta de financiación y la cantidad especificada; enviar el ID de transferencia al dispositivo móvil del emisor; recibir una solicitud de autorización de transferencia de valor desde un dispositivo móvil del receptor, comprendiendo la solicitud el ID de transferencia; identificar el número de tarjeta de financiación y la cantidad autorizada basándose en el ID de transferencia; enviar una solicitud de autorización de pago a un emisor de tarjeta de financiación, comprendiendo la solicitud el número de tarjeta de financiación y la cantidad especificada; recibir una respuesta de autorización de pago del emisor de la tarjeta de financiación; y enviar una respuesta de autorización de transferencia de valor al dispositivo móvil del receptor.

En un aspecto de ejemplo, el método incluye, además: si la respuesta de autorización de transferencia de valor es positiva, crear una tarjeta virtual de prepago asociada con el dispositivo móvil del receptor y que tiene la cantidad especificada.

En otra realización de ejemplo, se proporciona un método realizado por un servidor para facilitar una transferencia de valor de parte a parte. El método incluye: recibir un mensaje desde un dispositivo móvil del emisor que identifica una tarjeta de financiación y cantidad; buscar en una base de datos de múltiples tarjetas asociadas con el dispositivo móvil del emisor detalles de tarjeta de financiación asociados con la tarjeta de financiación y la cantidad identificadas; calcular datos para una tarjeta virtual, comprendiendo los datos un número de tarjeta y una fecha de caducidad; almacenar los datos para el número de tarjeta virtual en asociación con el número de tarjeta de financiación; enviar los datos para la tarjeta virtual al dispositivo móvil del emisor; calcular los detalles de la tarjeta usando un PIN como entrada; recibir una solicitud de autorización de transferencia de valor desde un dispositivo móvil del receptor, comprendiendo la solicitud los datos para la tarjeta virtual y una cantidad de transferencia de valor solicitada; recuperar los detalles de la tarjeta de financiación basándose en los datos para la tarjeta virtual y cantidad; enviar una solicitud de autorización de pago a un emisor de tarjeta de financiación, comprendiendo la solicitud el número de tarjeta de financiación y la cantidad de pago solicitada; recibir una respuesta de autorización de pago del emisor de la tarjeta de financiación; y enviar una respuesta de autorización de transferencia de valor al dispositivo móvil del receptor.

Las etapas u operaciones en los diagramas de flujo descritos en el presente documento son solo a modo de ejemplo. Puede haber muchas variaciones en estas etapas u operaciones sin apartarse del espíritu de la invención. Por ejemplo, las etapas pueden realizarse en un orden diferente, o pueden añadirse, eliminarse o modificarse etapas.

REIVINDICACIONES

1. Un método en un servidor de pasarela de pagos (506), comprendiendo el método:
recibir una solicitud de registro de tarjeta desde un dispositivo móvil (501), basándose la solicitud de registro de tarjeta en entradas introducidas por un usuario en el dispositivo móvil (501), incluyendo la solicitud de registro de tarjeta:
a. un identificador, ID, de dispositivo del dispositivo móvil,
b. un PIN proporcionado por un usuario del dispositivo móvil (501), y
c. detalles de la tarjeta de financiación de una tarjeta de pago a registrar, que incluyen:
i. un nombre impreso en la tarjeta de financiación,
ii. un número de cuenta primario, PAN, impreso en la tarjeta de financiación,
iii. una fecha de caducidad impresa en la tarjeta de financiación, y
iv. un código de seguridad estático impreso en la tarjeta de financiación;
en donde
el servidor de pasarela de pagos (506) calcula un identificador de tarjeta de financiación que identifica la tarjeta de financiación y es distinto del PAN;
en respuesta a la solicitud de registro de tarjeta, el servidor de pasarela de pagos (506) envía una respuesta de registro de tarjeta al dispositivo móvil (501) para su almacenamiento en el dispositivo móvil (501), conteniendo la respuesta de registro de tarjeta
a. un certificado
b. un contador de transacciones de aplicación, ATC, que se establece inicialmente a un valor aleatorio entre "0" y "1000" y se incrementa con cada transacción
c. un primer valor de clave, Kpan
d. un valor de clave de elemento seguro, Ksec, y
e. el identificador de tarjeta de financiación;
el servidor de pasarela de pagos (506) almacena, en una base de datos (508) del servidor de pasarela de pagos (506), el certificado, el ATC, el primer Kpan, el Ksec, el identificador de tarjeta de financiación, el PIN y los detalles de la tarjeta de financiación en asociación con el ID de dispositivo;
después de enviar la respuesta de registro de tarjeta, el servidor de pasarela de pagos (506) recibe una solicitud de tarjeta virtual desde el dispositivo móvil (501), incluyendo la solicitud de tarjeta virtual
a. el ID de dispositivo
b. un identificador de tarjeta de financiación
c. un certificado, y
d. un Kpan;
el servidor de pasarela de pagos (506) determina que el Kpan y el certificado incluidos en la solicitud de tarjeta virtual coinciden respectivamente con el primer Kpan y el certificado almacenados en la base de datos en asociación con el ID de dispositivo que corresponde al ID de dispositivo en la solicitud de tarjeta virtual;
el servidor de pasarela de pagos (506) envía un segundo Kpan al dispositivo móvil para su uso en la generación de un PAN virtual, en donde después de que el dispositivo móvil recibe el segundo Kpan, el dispositivo móvil reemplaza el primer Kpan almacenado con el segundo Kpan;
el servidor de pasarela de pagos (506) calcula, usando el segundo Kpan, el PAN virtual de acuerdo con:
PAN virtual = BIN(6) + SHA256[Kpan](8)+Luhn(1)+Reservado(4);
el servidor de pasarela de pagos (506) almacena el segundo Kpan y el PAN virtual calculado en la base de datos (509) en asociación con el identificador de tarjeta de financiación;
el servidor de pasarela de pagos (506) recibe, desde el dispositivo móvil (501) a través de un sistema de adquiriente de comerciante (103), una solicitud de autorización de pago que incluye
a. una cantidad de transacción
b. un PAN virtual, y
c. datos discrecionales;
en donde se calcula el PAN virtual en la solicitud de autorización de pago por el dispositivo móvil cuando el dispositivo móvil reemplazó el primer Kpan con el segundo Kpan, usando el segundo Kpan de acuerdo con:
PAN virtual = BIN(6) + SHA256[Kpan](8)+Luhn(1)+Reservado(4);
y en donde se calculan los datos discrecionales en la solicitud de autorización de pago por el dispositivo móvil usando un PIN introducido por el usuario, el Ksec, el PAN virtual calculado, el certificado y el ATC de acuerdo con:
datos discrecionales = HMAC_SHA256[Ksec+PIN,M](10) donde M es una concatenación del PAN,
el ID del certificado y el ATC;
el servidor de pasarela de pagos (506), después de recibir la solicitud de autorización de pago, usa el PAN virtual incluido en la solicitud de autorización de pago como un índice para buscar en la base de datos (509) el PAN virtual calculado almacenado y los datos relevantes asociados, siendo los datos relevantes asociados el segundo Kpan almacenado, el certificado almacenado, el Ksec almacenado, el identificador de tarjeta de financiación almacenado, el ID de dispositivo almacenado, el ATC almacenado y el PIN almacenado y genera datos discrecionales de referencia basándose en el PAN virtual calculado almacenado y los datos relevantes asociados de acuerdo con:
datos discrecionales = HMAC_SHA256[Ksec+PIN,M](10) donde M es una concatenación del PAN,
el ID del certificado y el ATC;
el servidor de pasarela de pagos (506) determina que los datos discrecionales de referencia generados coinciden

con los datos discrecionales de la solicitud de autorización de pago;
el servidor de pasarela de pagos (506) recupera los detalles de la tarjeta de financiación y reenvía los detalles de la tarjeta de financiación a un emisor de la tarjeta de pago; y
el servidor de pasarela de pagos (506) marca el PAN virtual calculado almacenado en la base de datos como usado.

2. Un medio legible por ordenador que almacena instrucciones ejecutables por ordenador ejecutables por un servidor de pasarela de pagos (506) para:
recibir una solicitud de registro de tarjeta desde un dispositivo móvil (501), basándose la solicitud de registro de tarjeta en entradas introducidas por un usuario en el dispositivo móvil, incluyendo la solicitud de registro de tarjeta:
a. un identificador de dispositivo del dispositivo móvil (501)
b. un PIN proporcionado por un usuario del dispositivo móvil (501), y
c. detalles de la tarjeta de financiación de una tarjeta de pago a registrar, que incluyen:
i. un nombre impreso en la tarjeta de financiación,
ii. un número de cuenta primario, PAN, impreso en la tarjeta de financiación,
iii. una fecha de caducidad impresa en la tarjeta de financiación, y
iv. un código de seguridad estático impreso en la tarjeta de financiación;
en donde
el servidor de pasarela de pagos (506) calcula un identificador de tarjeta de financiación que identifica la tarjeta de financiación y es distinto del PAN;
en respuesta a la solicitud de registro de tarjeta, el servidor de pasarela de pagos (506) envía una respuesta de registro de tarjeta al dispositivo móvil (501) para su almacenamiento en el dispositivo móvil (501), conteniendo la respuesta de registro de tarjeta
a. un certificado
b. un contador de transacciones de aplicación, ATC, que se establece inicialmente a un valor aleatorio entre "0" y "1000" y se incrementa con cada transacción
c. un primer valor de clave, Kpan
d. un valor de clave de elemento seguro, Ksec, y
e. el identificador de tarjeta de financiación;
el servidor de pasarela de pagos (506) almacena, en una base de datos (508) del servidor de pasarela de pagos (506), el certificado, el ATC, el primer Kpan, el Ksec, el identificador de tarjeta de financiación, el PIN y los detalles de la tarjeta de financiación en asociación con el ID de dispositivo;
después de enviar la respuesta de registro de tarjeta, el servidor de pasarela de pagos (506) recibe una solicitud de tarjeta virtual desde el dispositivo móvil, incluyendo la solicitud de tarjeta virtual
a. el ID de dispositivo
b. un identificador de tarjeta de financiación
c. un certificado, y
d. un Kpan;
el servidor de pasarela de pagos (506) determina que el Kpan y el certificado incluidos en la solicitud de tarjeta virtual coinciden respectivamente con el primer Kpan y el certificado almacenados en la base de datos en asociación con el ID de dispositivo que corresponde al ID de dispositivo en la solicitud de tarjeta virtual;
el servidor de pasarela de pagos (506) envía un segundo Kpan al dispositivo móvil para su uso en la generación de un PAN virtual, en donde después de que el dispositivo móvil recibe el segundo Kpan, el dispositivo móvil reemplaza el primer Kpan almacenado con el segundo Kpan;
el servidor de pasarela de pagos (506) calcula, usando el segundo Kpan, el PAN virtual de acuerdo con:
PAN virtual = BIN(6) + SHA256[Kpan](8)+Luhn(1)+Reservado(4);
el servidor de pasarela de pagos (506) almacena el segundo Kpan y el PAN virtual calculado en la base de datos (509) en asociación con el identificador de tarjeta de financiación;
el servidor de pasarela de pagos (506) recibe, desde el dispositivo móvil (501) a través de un sistema de adquiriente de comerciante (103), una solicitud de autorización de pago que incluye
a. una cantidad de transacción
b. un PAN virtual, y
c. datos discrecionales;
en donde se calcula el PAN virtual en la solicitud de autorización de pago por el dispositivo móvil cuando el dispositivo móvil reemplazó el primer Kpan con el segundo Kpan, usando el segundo Kpan de acuerdo con:
PAN virtual = BIN(6) + SHA256[Kpan](8)+Luhn(1)+Reservado(4);
y en donde se calculan los datos discrecionales en la solicitud de autorización de pago por el dispositivo móvil usando un PIN introducido por el usuario, el Ksec, el PAN virtual calculado, el certificado y el ATC de acuerdo con:
datos discrecionales = HMAC_SHA256[Ksec+PIN,M](10) donde M es una concatenación del PAN,
el ID del certificado y el ATC;
el servidor de pasarela de pagos (506), después de recibir la solicitud de autorización de pago, usa el PAN virtual incluido en la solicitud de autorización de pago como un índice para buscar en la base de datos (509) el PAN virtual calculado almacenado y los datos relevantes asociados, siendo los datos relevantes asociados el segundo Kpan almacenado, el certificado almacenado, el Ksec almacenado, el identificador de tarjeta de financiación almacenado, el ID de dispositivo almacenado, el ATC almacenado y el PIN almacenado y genera datos discrecionales de referencia basándose en el PAN virtual calculado almacenado y los datos relevantes asociados

de acuerdo con:

datos discrecionales = HMAC_SHA256[Ksec+PIN,M](10) donde M es una concatenación del PAN, el ID del certificado y el ATC;

el servidor de pasarela de pagos (506) determina que los datos discrecionales de referencia generados coinciden con los datos discrecionales de la solicitud de autorización de pago;

el servidor de pasarela de pagos (506) recupera los detalles de la tarjeta de financiación y reenvía los detalles de la tarjeta de financiación a un emisor de la tarjeta de pago; y

el servidor de pasarela de pagos (506) marca el PAN virtual calculado almacenado en la base de datos como usado.

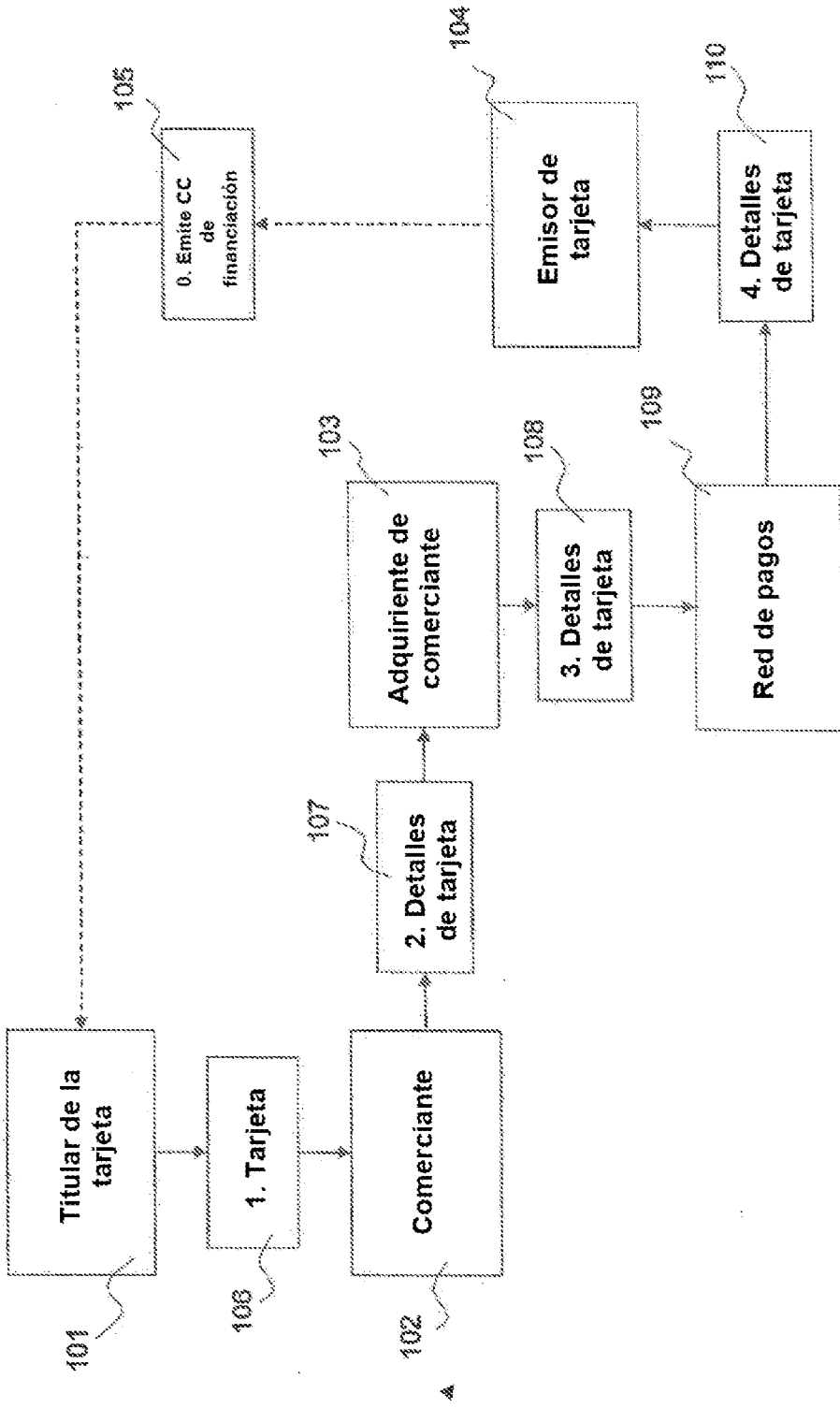

FIG. 1 *(Técnica anterior)*

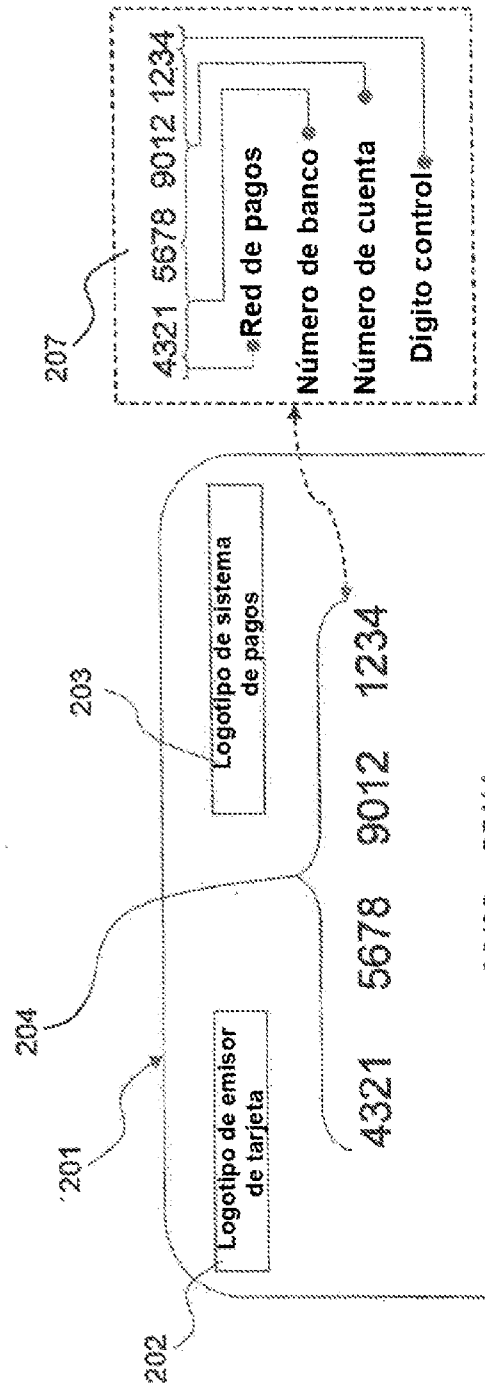

FIG. 2 *(Técnica anterior)*

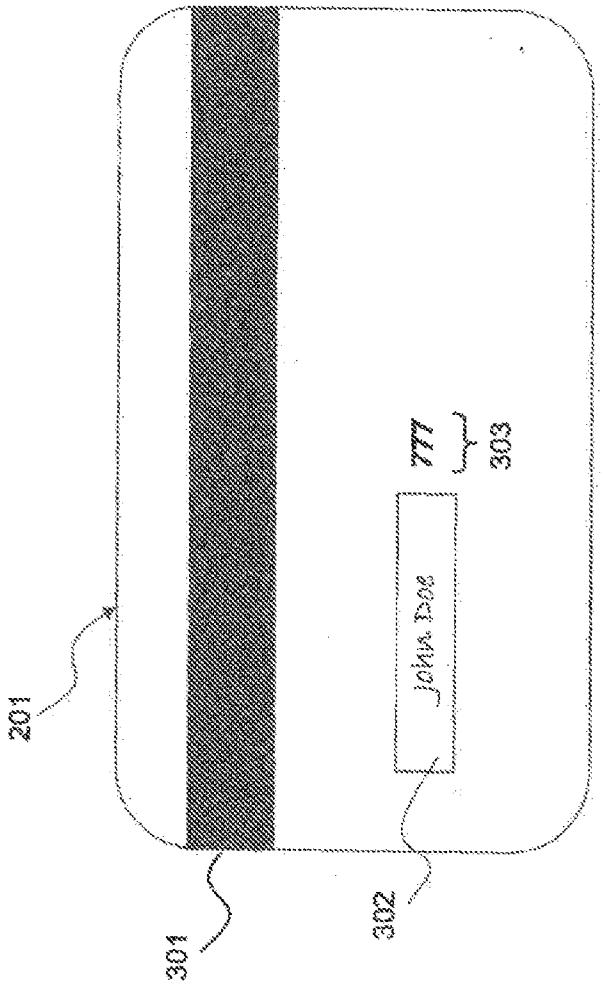

FIG. 3 *(Técnica anterior)*

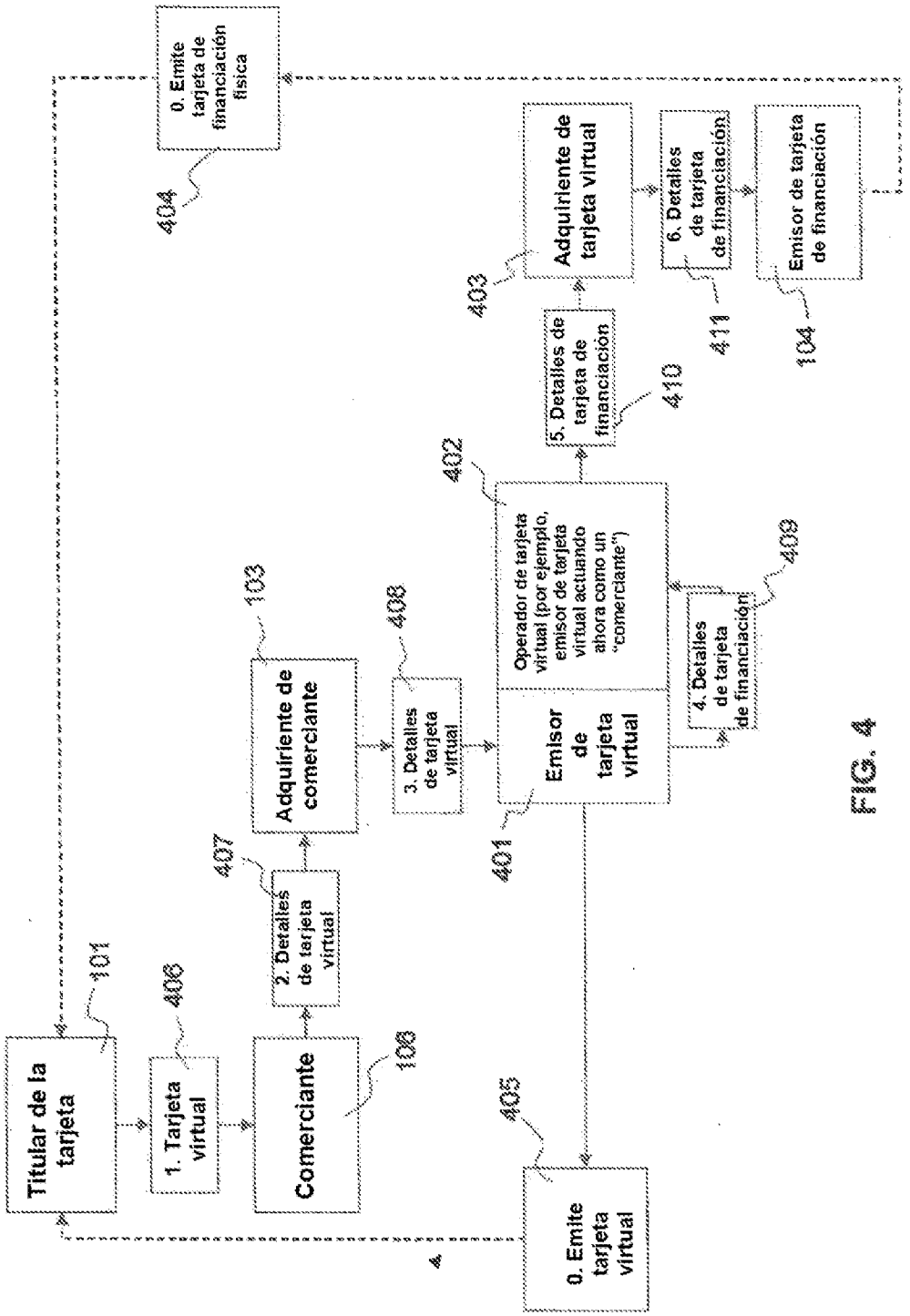
Titular de la tarjeta
101
1. Tarjeta virtual
406
Comerciante
106
2. Detalles de tarjeta virtual
407
Adquiriente de comerciante
103
3. Detalles de tarjeta virtual
408
Emisor de tarjeta virtual
401
Operador de tarjeta virtual (por ejemplo, emisor de tarjeta virtual actuando ahora como un "comerciante")
402
4. Detalles de tarjeta de financiación
409
5. Detalles de tarjeta de financiación
410
Adquiriente de tarjeta virtual
403
6. Detalles de tarjeta de financiación
411
Emisor de tarjeta de financiación
104
0. Emite tarjeta de financiación física
404
0. Emite tarjeta virtual
405

FIG. 4

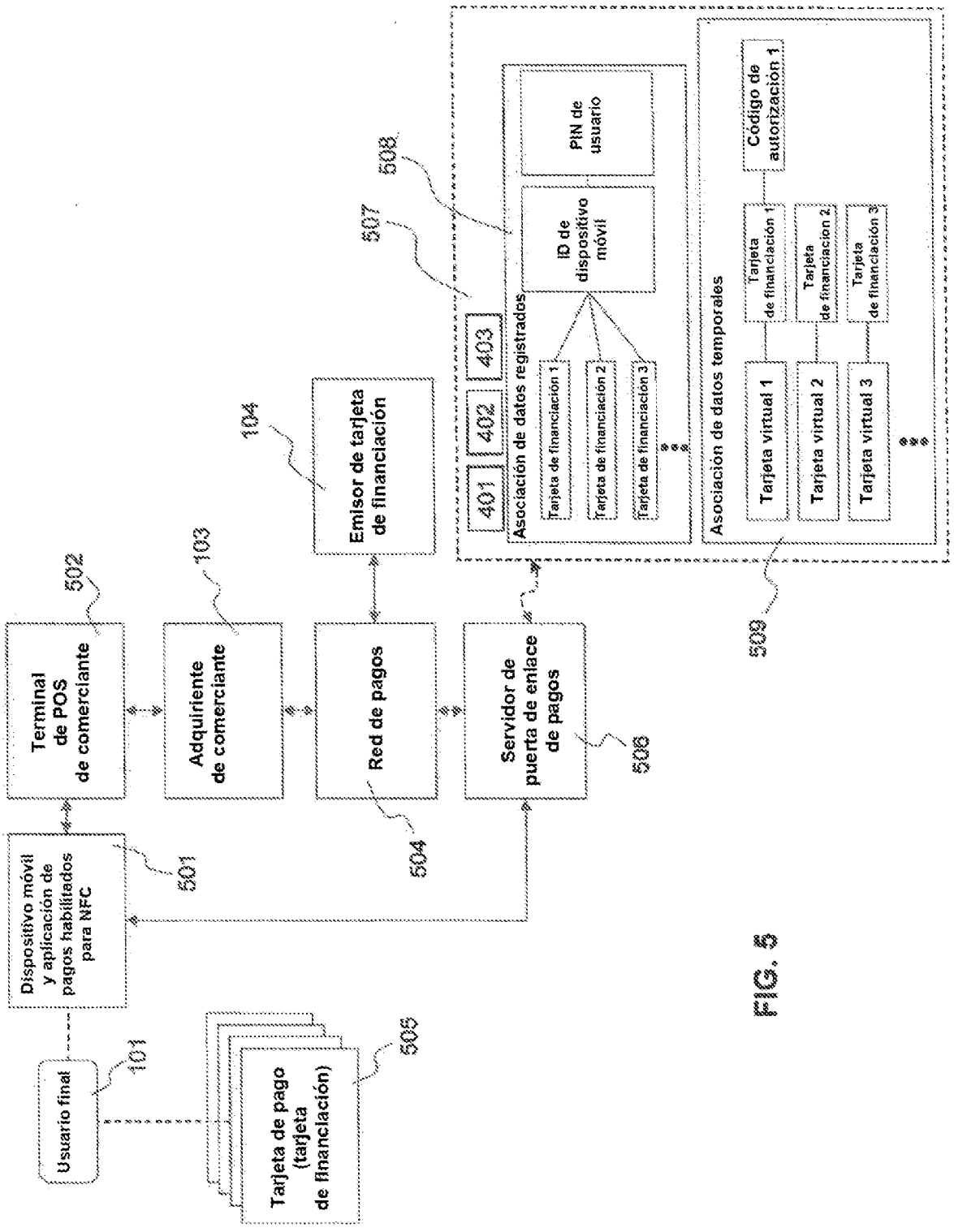
Usuario final
101
Tarjeta de pago (tarjeta de financiación)
505
Dispositivo móvil y aplicación de pagos habilitados para NFC
501
Terminal de POS de comerciante
502
Adquiriente de comerciante
103
Red de pagos
504
Emisor de tarjeta de financiación
104
Servidor de puerta de enlace de pagos
506
507
508
509
401
402
403
Asociación de datos registrados
Tarjeta de financiación 1
Tarjeta de financiación 2
Tarjeta de financiación 3
ID de dispositivo móvil
PIN de usuario
Asociación de datos temporales
Tarjeta virtual 1
Tarjeta virtual 2
Tarjeta virtual 3
Tarjeta de financiación 1
Tarjeta de financiación 2
Tarjeta de financiación 3
Código de autorización 1

FIG. 5

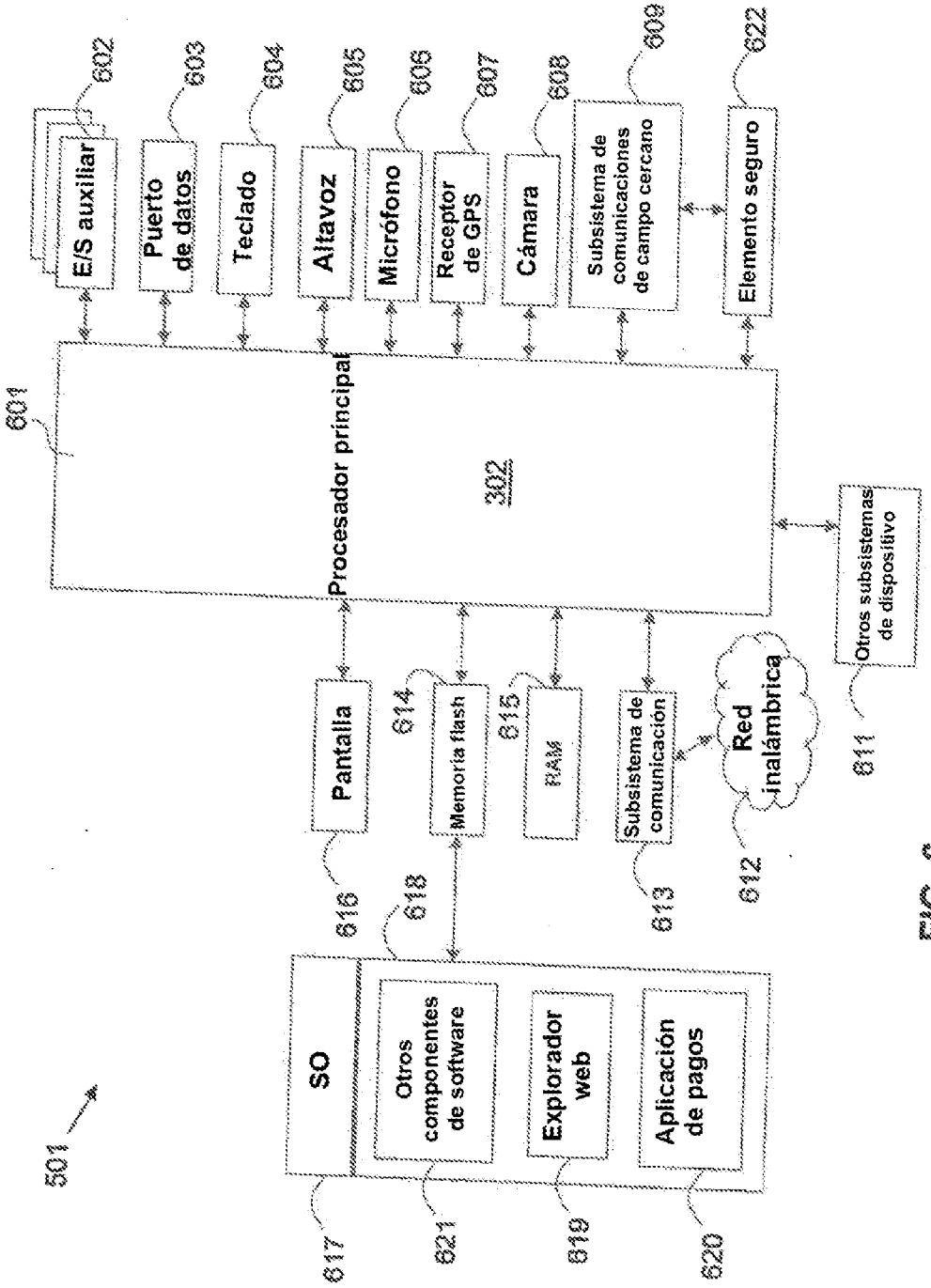
501
601
Procesador principal
302
E/S auxiliar
602
Puerto de datos
603
Teclado
604
Altavoz
605
Micrófono
606
Receptor de GPS
607
Cámara
608
Subsistema de comunicaciones de campo cercano
609
Elemento seguro
622
Otros subsistemas de dispositivo
611
Pantalla
616
Memoria flash
614
RAM
615
Subsistema de comunicación
613
Red inalámbrica
612
SO
617
Otros componentes de software
621
Explorador web
619
Aplicación de pagos
620
618

FIG. 6

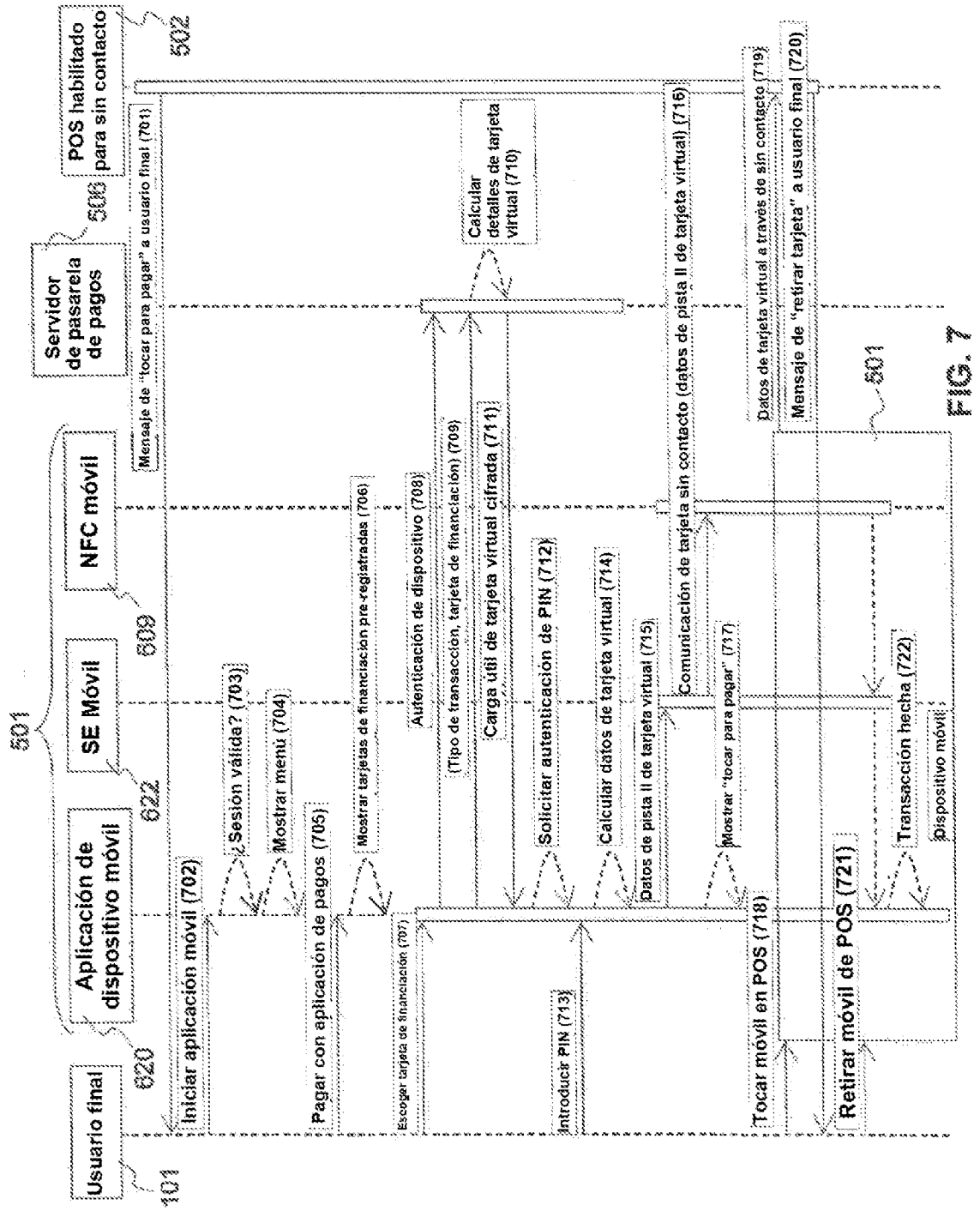
501
Usuario final
Aplicación de dispositivo móvil
SE Móvil
NFC móvil
Servidor de pasarela de pagos
POS habilitado para sin contacto
620
622
609
608
502
101
Iniciar aplicación móvil (702)
Sesión válida? (703)
Mostrar menú (704)
Pagar con aplicación de pagos (705)
Mostrar tarjetas de financiación pre-registradas (706)
Escoger tarjeta de financiación (707)
Autenticación de dispositivo (708)
Tipo de transacción, tarjeta de financiación) (709)
Mensaje de "tocar para pagar" a usuario final (701)
Calcular detalles de tarjeta virtual (710)
Carga útil de tarjeta virtual cifrada (711)
Solicitar autenticación de PIN (712)
Introducir PIN (713)
Calcular datos de tarjeta virtual (714)
Datos de pista II de tarjeta virtual (715)
Comunicación de tarjeta sin contacto (datos de pista II de tarjeta virtual) (716)
Mostrar "tocar para pagar" (717)
Tocar móvil en POS (718)
Datos de tarjeta virtual a través de sin contacto (719)
Mensaje de "retirar tarjeta" a usuario final (720)
Retirar móvil de POS (721)
Transacción hecha (722)
Dispositivo móvil
501

FIG. 7

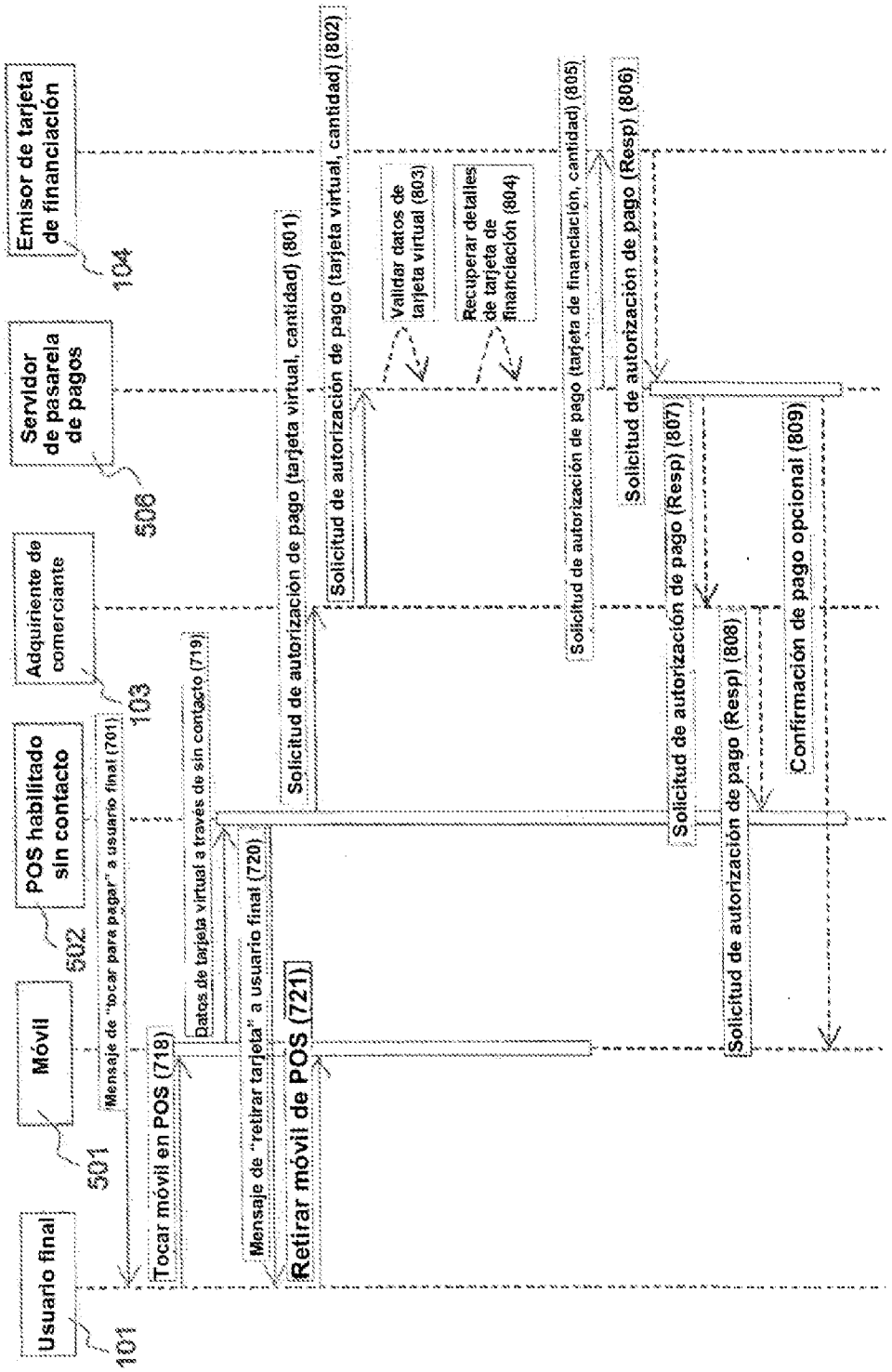
Usuario final
101
Móvil
501
POS habilitado sin contacto
502
Adquiriente de comerciante
103
Servidor de pasarela de pagos
108
Emisor de tarjeta de financiación
104
Mensaje de "tocar para pagar" a usuario final (701)
Tocar móvil en POS (718)
Datos de tarjeta virtual a través de sin contacto (719)
Mensaje de "retirar tarjeta" a usuario final (720)
Retirar móvil de POS (721)
Solicitud de autorización de pago (tarjeta virtual, cantidad) (801)
Solicitud de autorización de pago (tarjeta virtual, cantidad) (802)
Validar datos de tarjeta virtual (803)
Recuperar detalles de tarjeta de financiación (804)
Solicitud de autorización de pago (tarjeta de financiación, cantidad) (805)
Solicitud de autorización de pago (Resp) (806)
Solicitud de autorización de pago (807)
Solicitud de autorización de pago (Resp) (808)
Confirmación de pago opcional (809)

FIG. 8

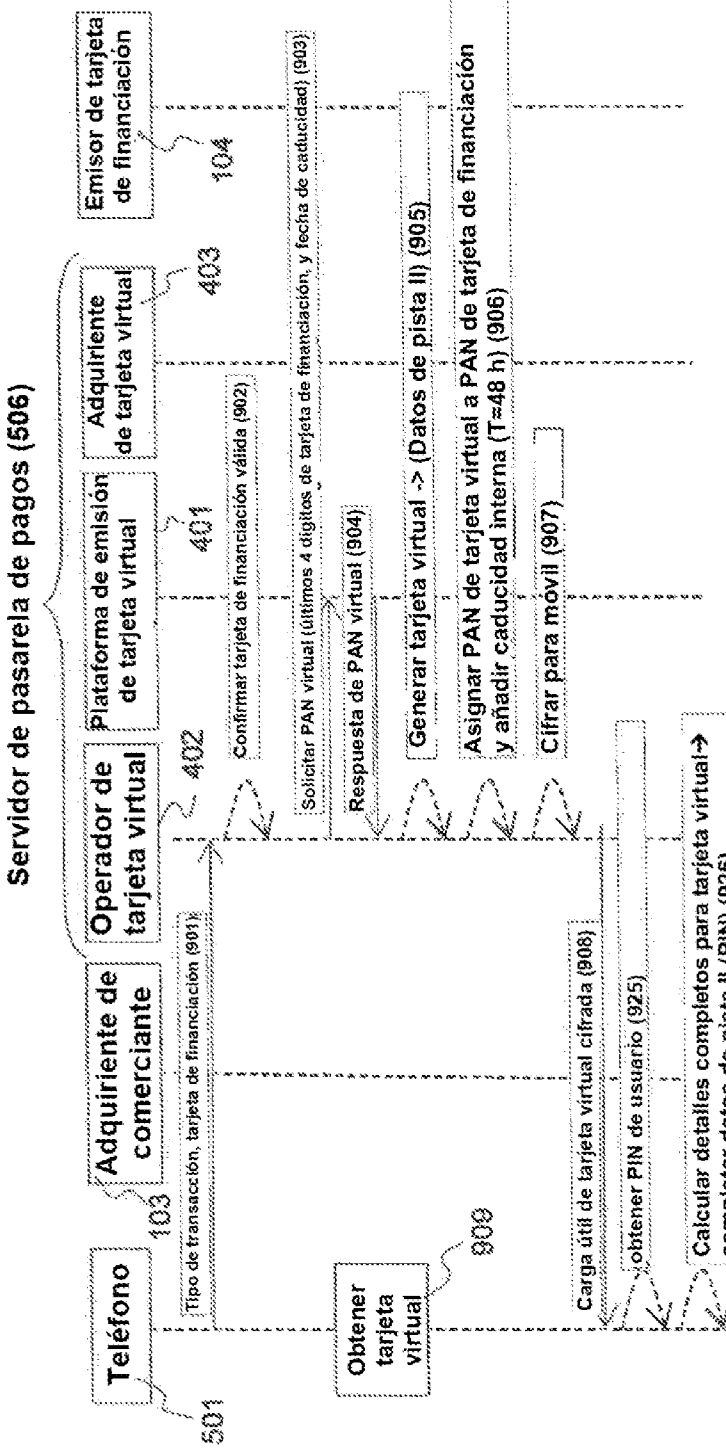
Servidor de pasarela de pagos (506)
Teléfono
501
Adquiriente de comerciante
103
Operador de tarjeta virtual
402
Plataforma de emisión de tarjeta virtual
401
Adquiriente de tarjeta virtual
403
Emisor de tarjeta de financiación
104
Tipo de transacción, tarjeta de financiación (901)
Confirmar tarjeta de financiación válida (902)
Solicitar PAN virtual (últimos 4 dígitos de tarjeta de financiación, y fecha de caducidad) (903)
Respuesta de PAN virtual (904)
Generar tarjeta virtual -> (Datos de pista II) (905)
Asignar PAN de tarjeta virtual a PAN de tarjeta de financiación y añadir caducidad interna (T=48 h) (906)
Cifrar para móvil (907)
Obtener tarjeta virtual
906
Carga útil de tarjeta virtual cifrada (908)
obtener PIN de usuario (925)
Calcular detalles completos para tarjeta virtual→ completar datos de pista II (PIN) (926)

FIG. 9a

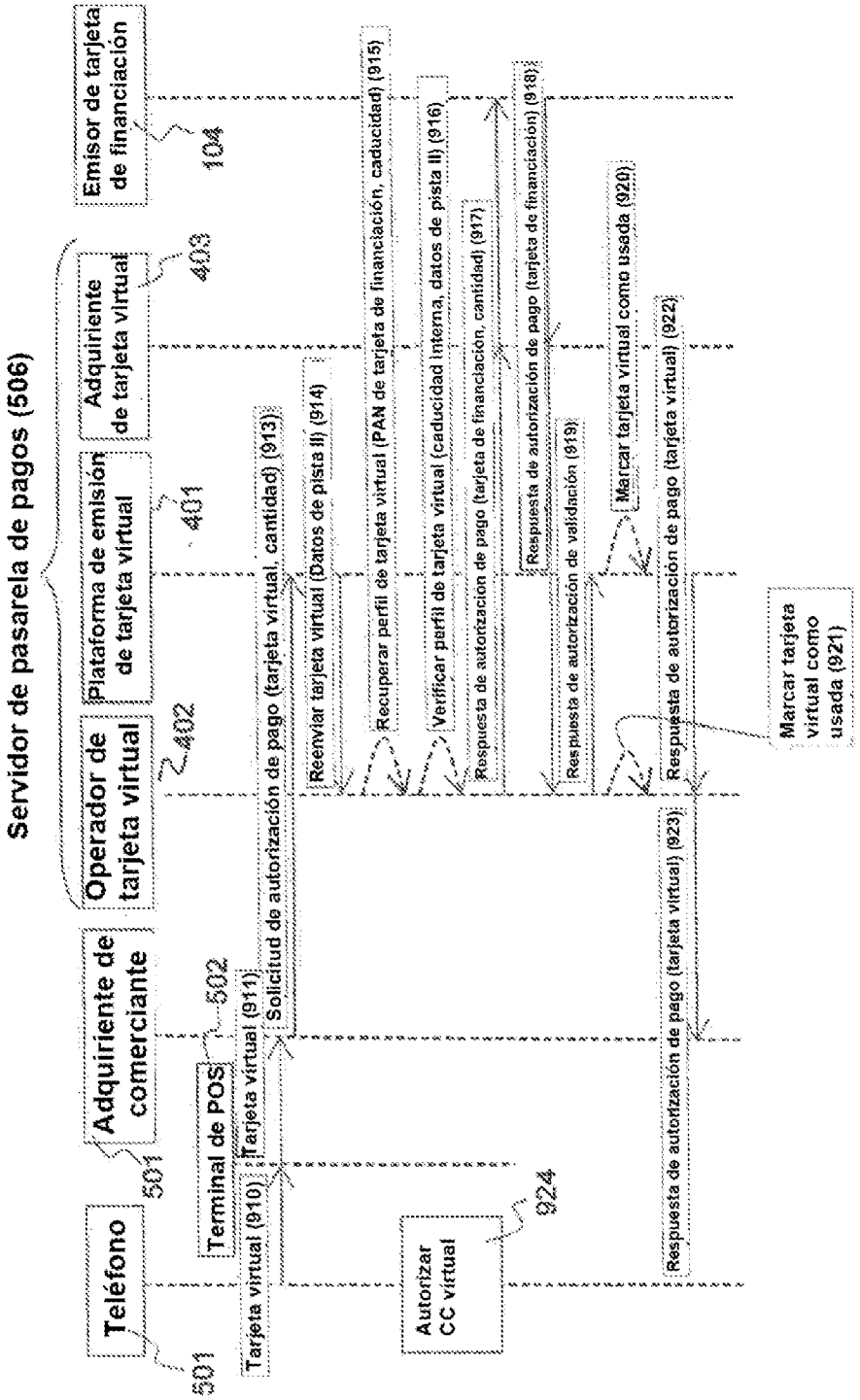
Servidor de pasarela de pagos (506)
Teléfono
501
Adquiriente de comerciante
501
Operador de tarjeta virtual
Plataforma de emisión de tarjeta virtual
401
Adquiriente de tarjeta virtual
403
Emisor de tarjeta de financiación
104
Terminal de POS
502
Tarjeta virtual (910)
Tarjeta virtual (911)
Solicitud de autorización de pago (tarjeta virtual, cantidad) (913)
Reenviar tarjeta virtual (Datos de pista II) (914)
Recuperar perfil de tarjeta virtual (PAN de tarjeta de financiación, caducidad) (915)
Verificar perfil de tarjeta virtual (caducidad interna, datos de pista II) (916)
Respuesta de autorización de pago (tarjeta de financiación, cantidad) (917)
Respuesta de autorización de pago (tarjeta de financiación) (918)
Respuesta de autorización de validación (919)
Marcar tarjeta virtual como usada (920)
Autorizar CC virtual
924
Respuesta de autorización de pago (tarjeta virtual) (923)
Respuesta de autorización de pago (tarjeta virtual) (922)
Marcar tarjeta virtual como usada (921)

FIG. 9b

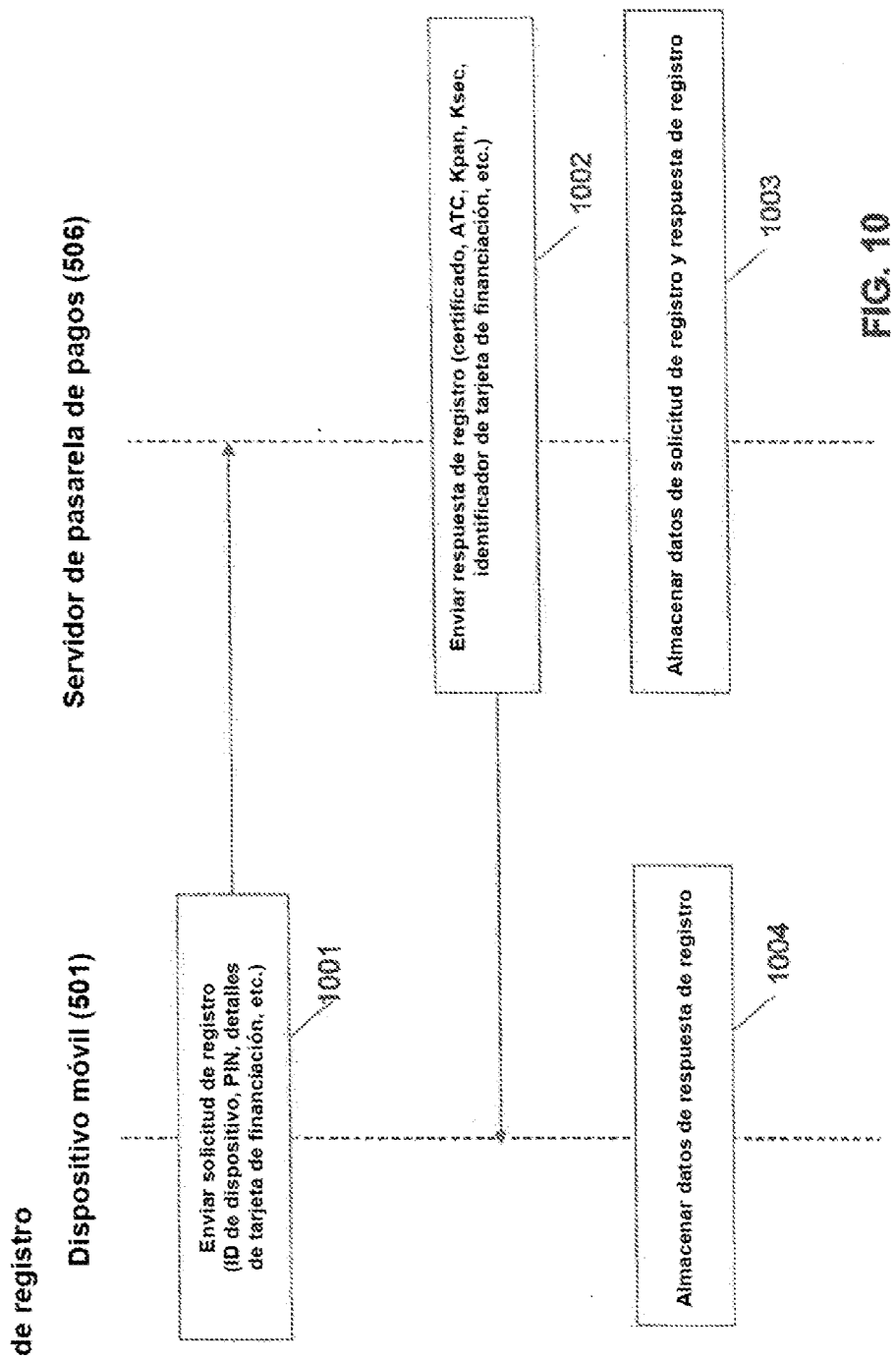
Proceso de registro
Dispositivo móvil (501)
Servidor de pasarela de pagos (506)
Enviar solicitud de registro (ID de dispositivo, PIN, detalles de tarjeta de financiación, etc.)
1001
Enviar respuesta de registro (certificado, ATC, Kpan, Ksec, identificador de tarjeta de financiación, etc.)
1002
Almacenar datos de solicitud de registro y respuesta de registro
1003
Almacenar datos de respuesta de registro
1004

FIG. 10

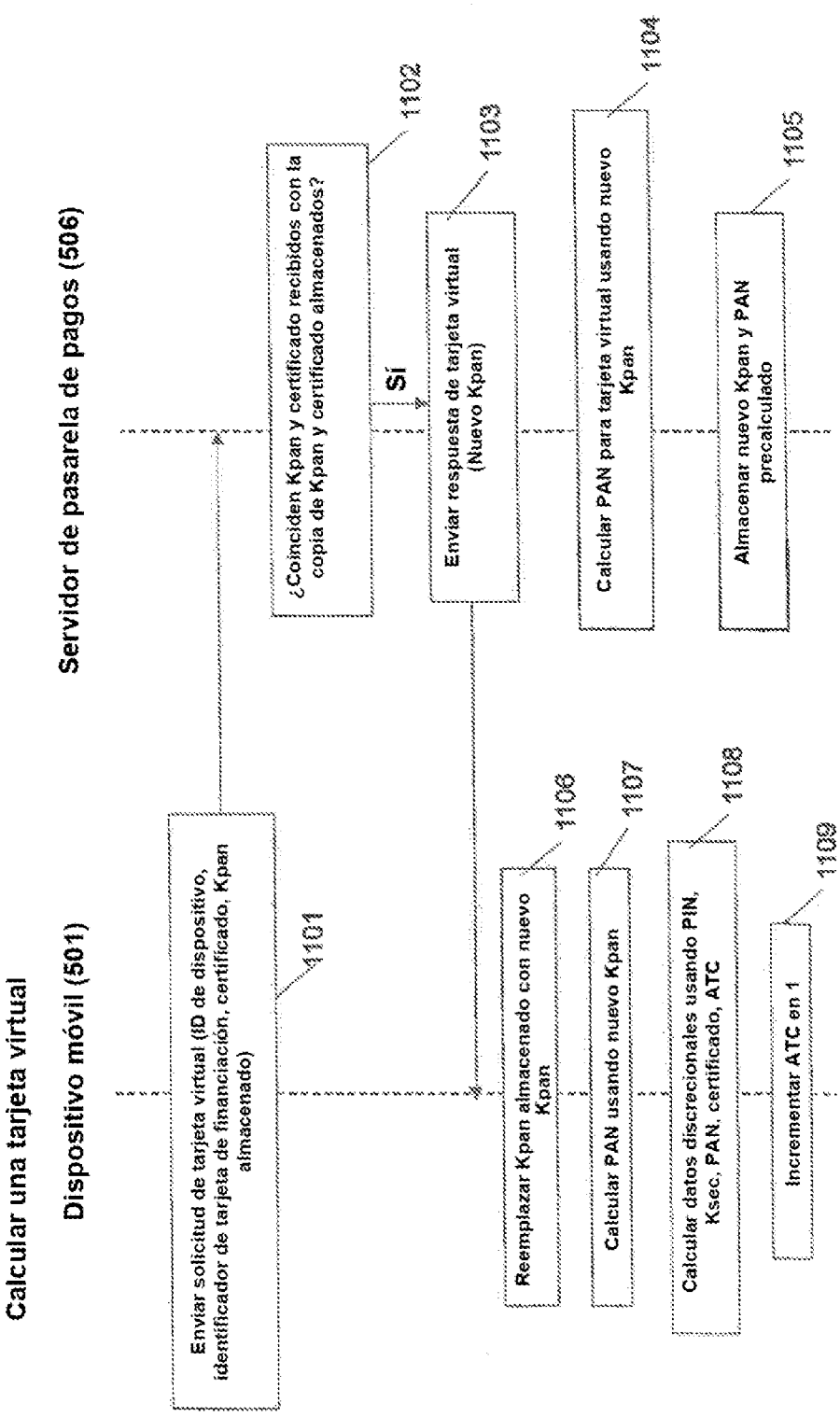
Calcular una tarjeta virtual
Dispositivo móvil (501)
Servidor de pasarela de pagos (506)
Enviar solicitud de tarjeta virtual (ID de dispositivo, identificador de tarjeta de financiación, certificado, Kpan almacenado)
1101
¿Coinciden Kpan y certificado recibidos con la copia de Kpan y certificado almacenados?
1102
Sí
Enviar respuesta de tarjeta virtual (Nuevo Kpan)
1103
Calcular PAN para tarjeta virtual usando nuevo Kpan
1104
Almacenar nuevo Kpan y PAN precalculado
1105
Reemplazar Kpan almacenado con nuevo Kpan
1106
Calcular PAN usando nuevo Kpan
1107
Calcular datos discrecionales usando PIN, Ksec, PAN, certificado, ATC
1108
Incrementar ATC en 1
1109

FIG. 11

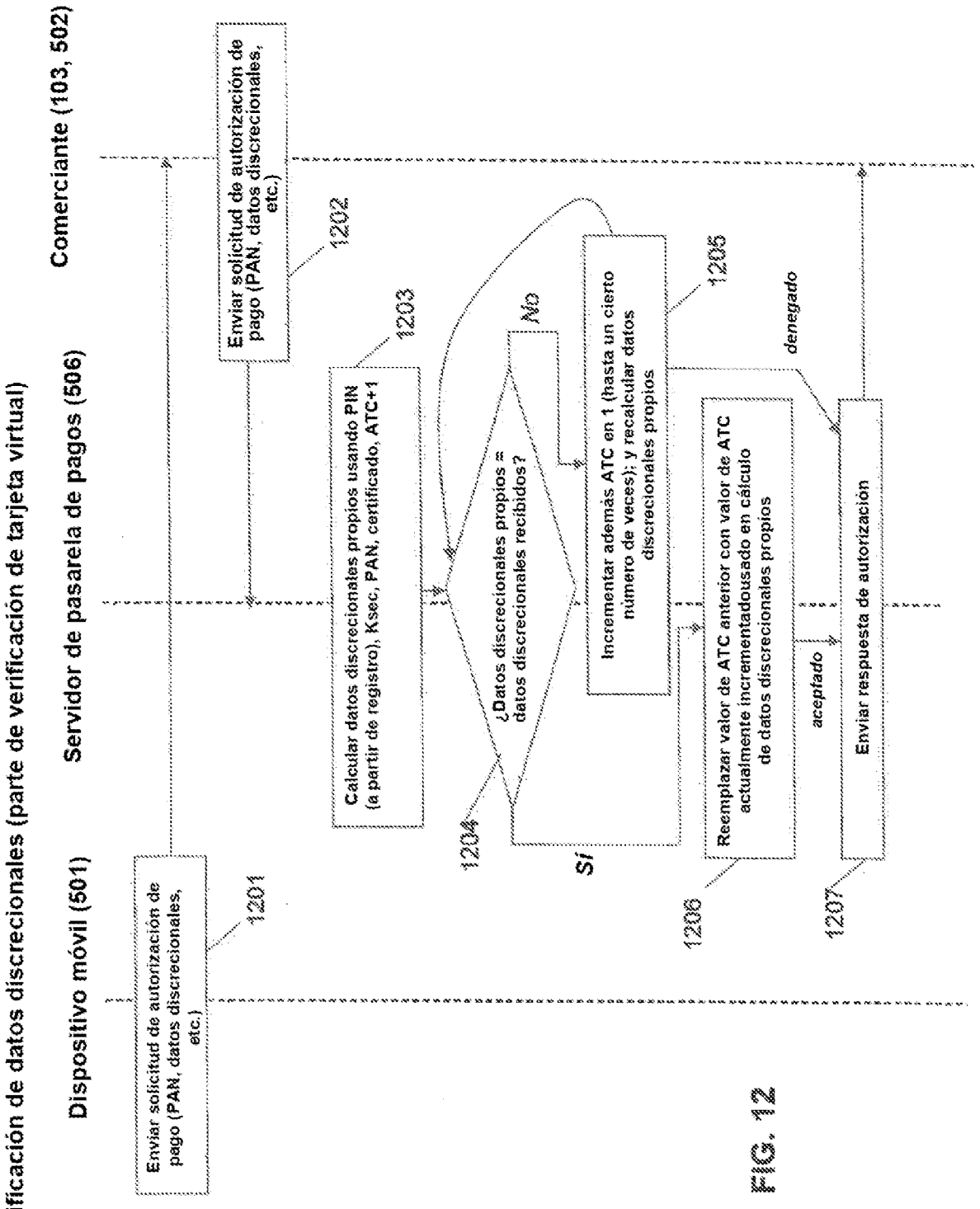
Verificación de datos discrecionales (parte de verificación de tarjeta virtual)
Dispositivo móvil (501)
Servidor de pasarela de pagos (506)
Comerciante (103, 502)
Enviar solicitud de autorización de pago (PAN, datos discrecionales, etc.)
1201
Enviar solicitud de autorización de pago (PAN, datos discrecionales, etc.)
1202
Calcular datos discrecionales propios usando PIN (a partir de registro), Ksec, PAN, certificado, ATC+1
1203
¿Datos discrecionales propios = datos discrecionales recibidos?
1204
No
Sí
Incrementar además ATC en 1 (hasta un cierto número de veces); y recalcular datos discrecionales propios
1205
Reemplazar valor de ATC anterior con valor de ATC actualmente incrementadousado en cálculo de datos discrecionales propios
1206
denegado
aceptado
Enviar respuesta de autorización
1207

FIG. 12

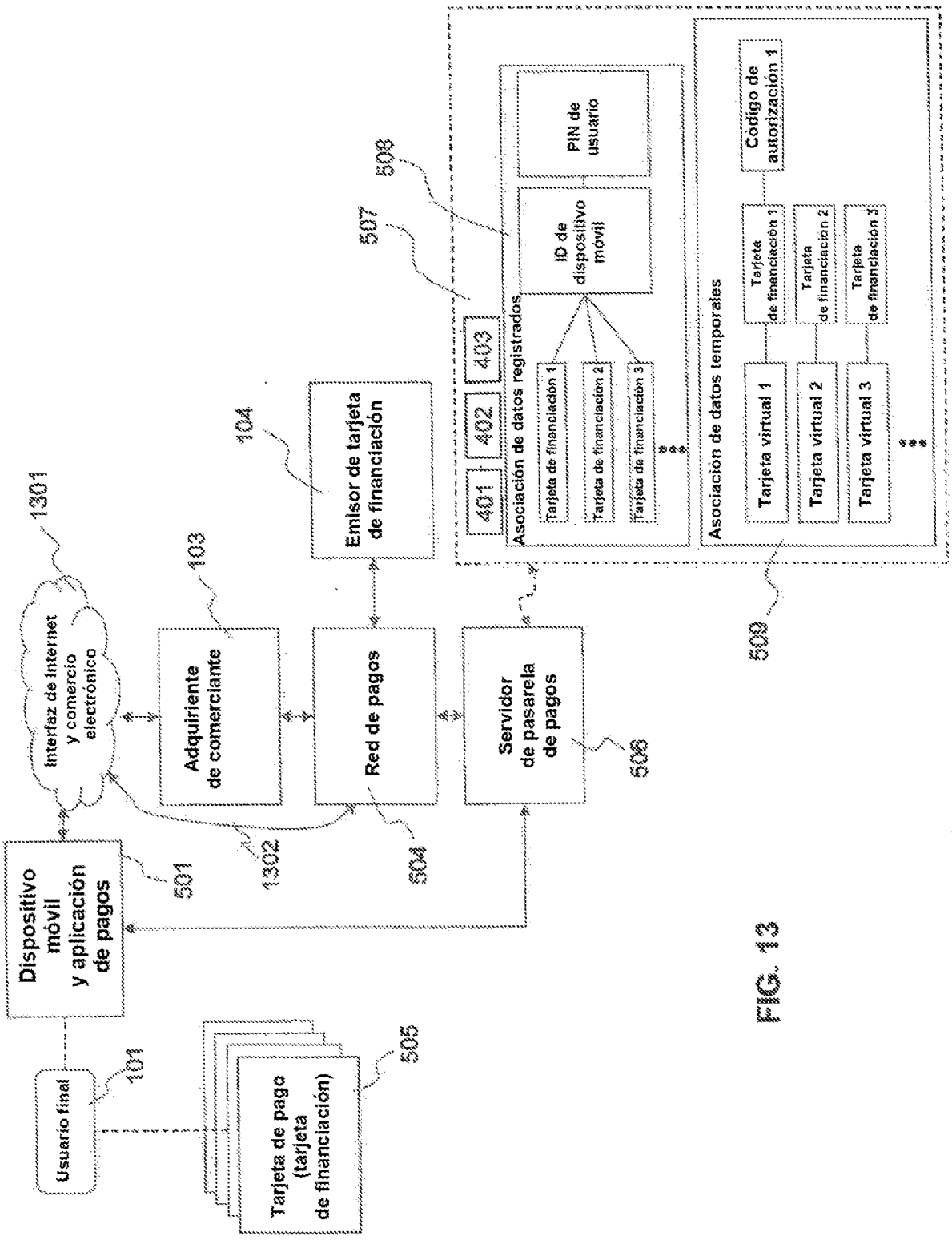
Usuario final
101
Tarjeta de pago (tarjeta de financiación)
505
Dispositivo móvil y aplicación de pagos
501
1301
Interfaz de Internet y comercio electrónico
1302
103
Adquiriente de comerciante
104
Emisor de tarjeta de financiación
Red de pagos
504
Servidor de pasarela de pagos
508
507
508
401
402
403
Asociación de datos registrados
Tarjeta de financiación 1
Tarjeta de financiación 2
Tarjeta de financiación 3
ID de dispositivo móvil
PIN de usuario
Asociación de datos temporales
Tarjeta virtual 1
Tarjeta virtual 2
Tarjeta virtual 3
Tarjeta de financiación 1
Tarjeta de financiación 2
Tarjeta de financiación 3
Código de autorización 1
509

FIG. 13

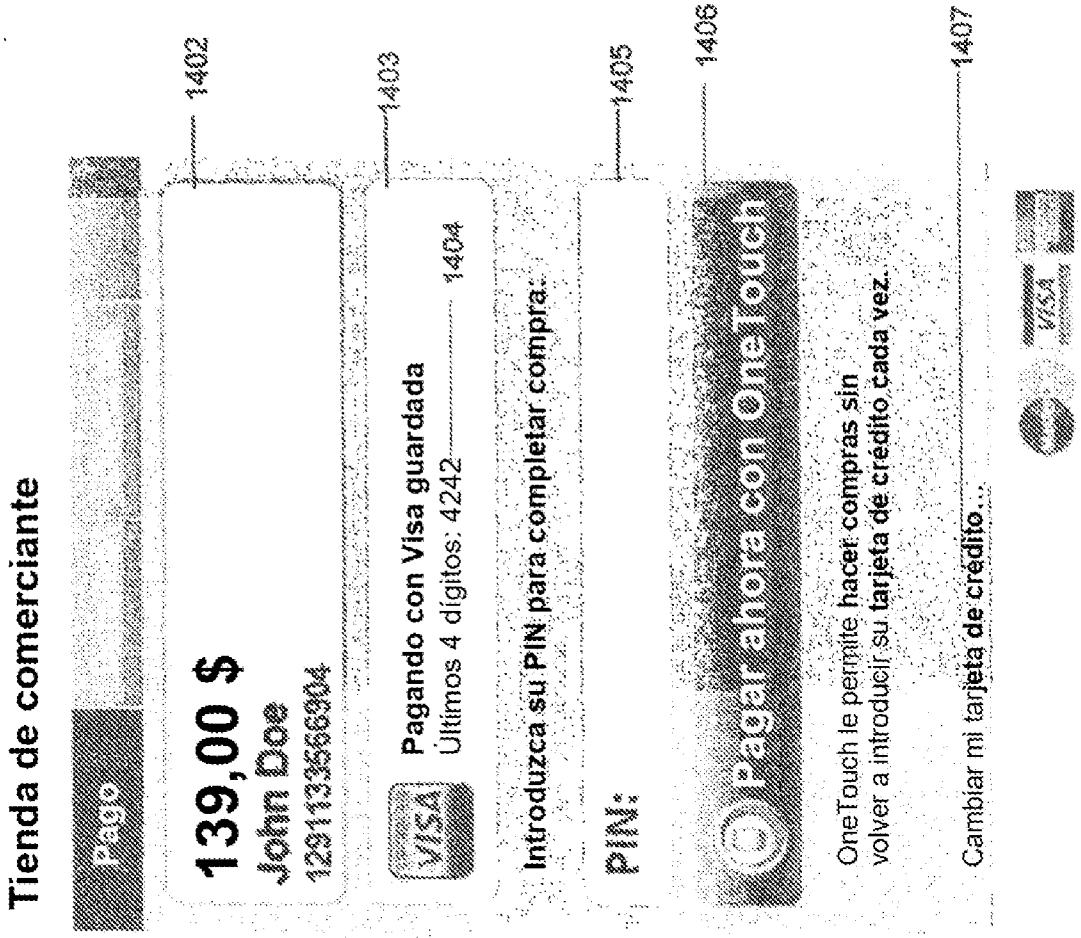
GUI de ejemplo
1401
Tienda de comerciante
Pago
1402
139,00 $
John Doe
1291133566304
1403
Pagando con Visa guardada
Últimos 4 dígitos: 4242
1404
Introduzca su PIN para completar compra:
PIN:
1405
Pagar ahora con OneTouch
1406
OneTouch le permite hacer compras sin volver a introducir su tarjeta de crédito cada vez.
Cambiar mi tarjeta de crédito...
1407

FIG. 14

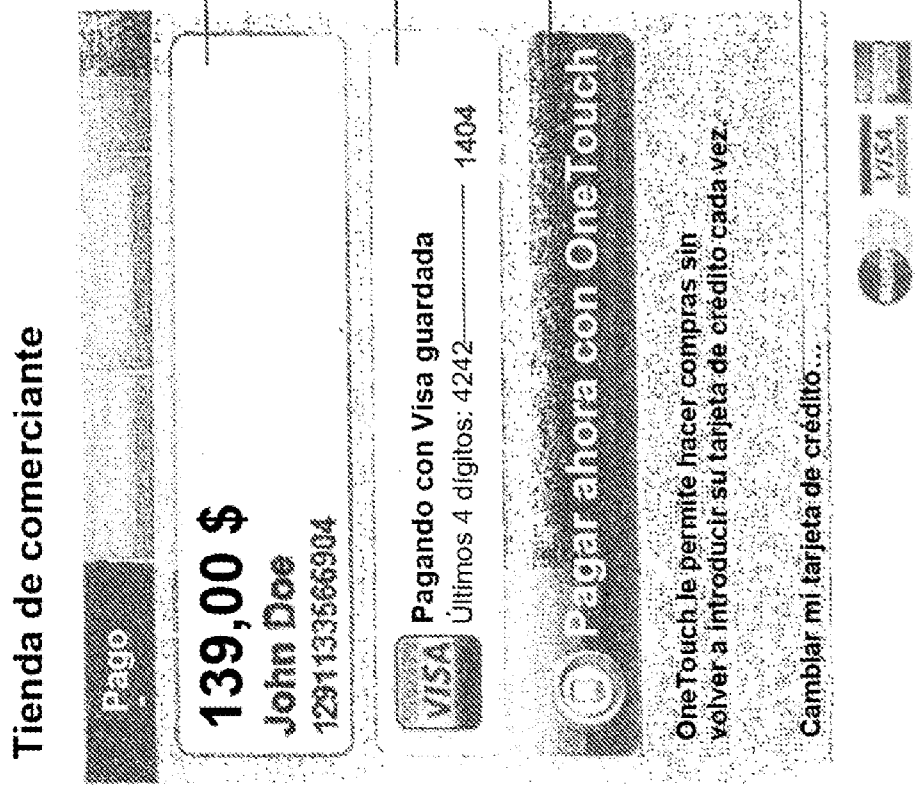
GUI de ejemplo
Tienda de comerciante
Pedido
139,00 $
John Doe
12911335666904
1402
1403
Pagando con Visa guardada
Últimos 4 dígitos: 4242
1404
Pagar ahora con OneTouch
1406
OneTouch le permite hacer compras sin volver a introducir su tarjeta de crédito cada vez.
Cambiar mi tarjeta de crédito...
1407
1501

FIG. 15

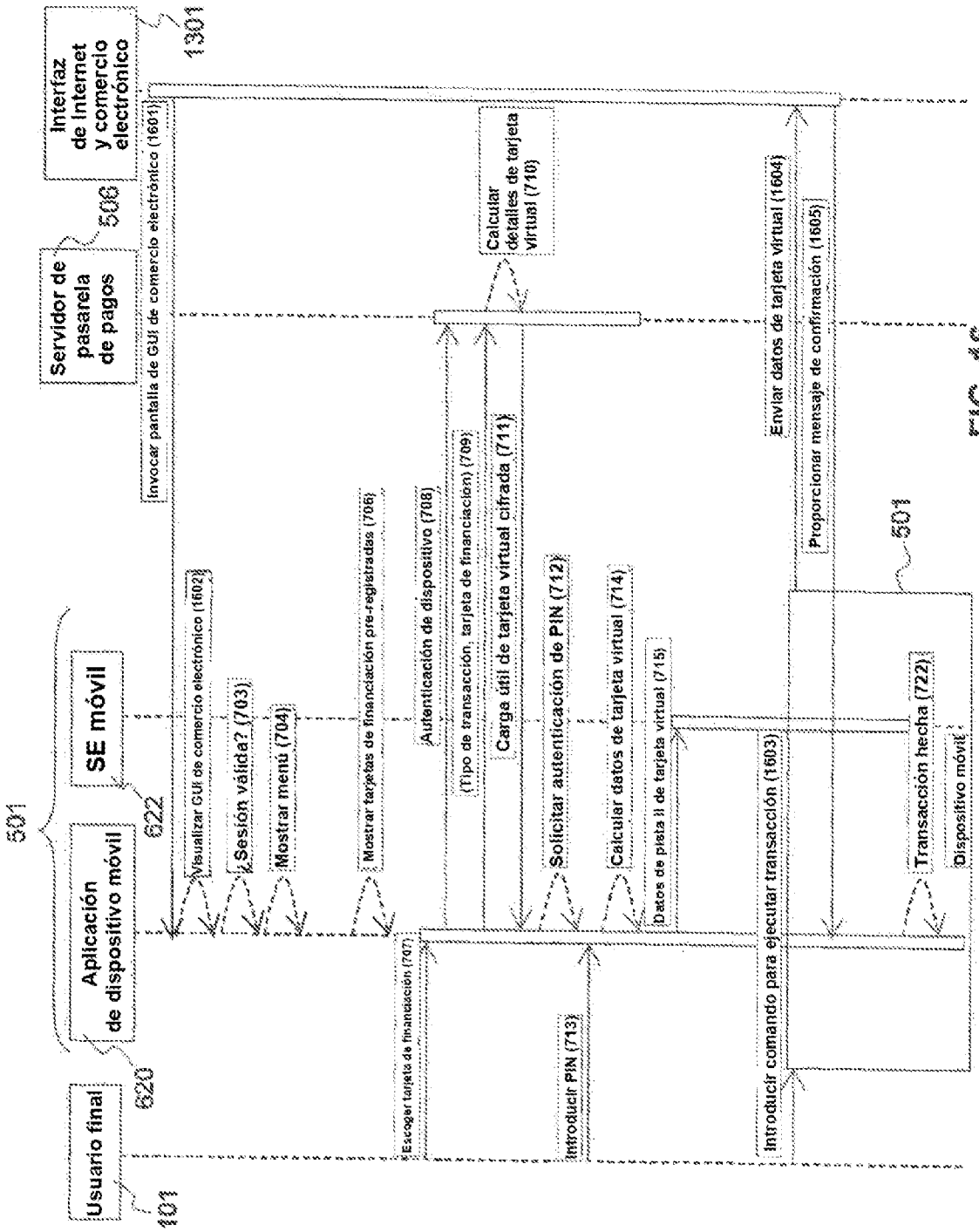
Usuario final
101
Aplicación de dispositivo móvil
620
SE móvil
622
501
Interfaz de Internet y comercio electrónico
1301
Servidor de pasarela de pagos
508
Invocar pantalla de GUI de comercio electrónico (1601)
Visualizar GUI de comercio electrónico (1602)
¿Sesión válida? (703)
Mostrar menú (704)
Mostrar tarjetas de financiación pre-registradas (706)
Escoger tarjeta de financiación (707)
Autenticación de dispositivo (708)
(Tipo de transacción, tarjeta de financiación) (709)
Carga útil de tarjeta virtual cifrada (711)
Solicitar autenticación de PIN (712)
Introducir PIN (713)
Calcular datos de tarjeta virtual (714)
Datos de pista II de tarjeta virtual (715)
Calcular detalles de tarjeta virtual (716)
Introducir comando para ejecutar transacción (1603)
Enviar datos de tarjeta virtual (1604)
Proporcionar mensaje de confirmación (1605)
Transacción hecha (722)
Dispositivo móvil

FIG. 16

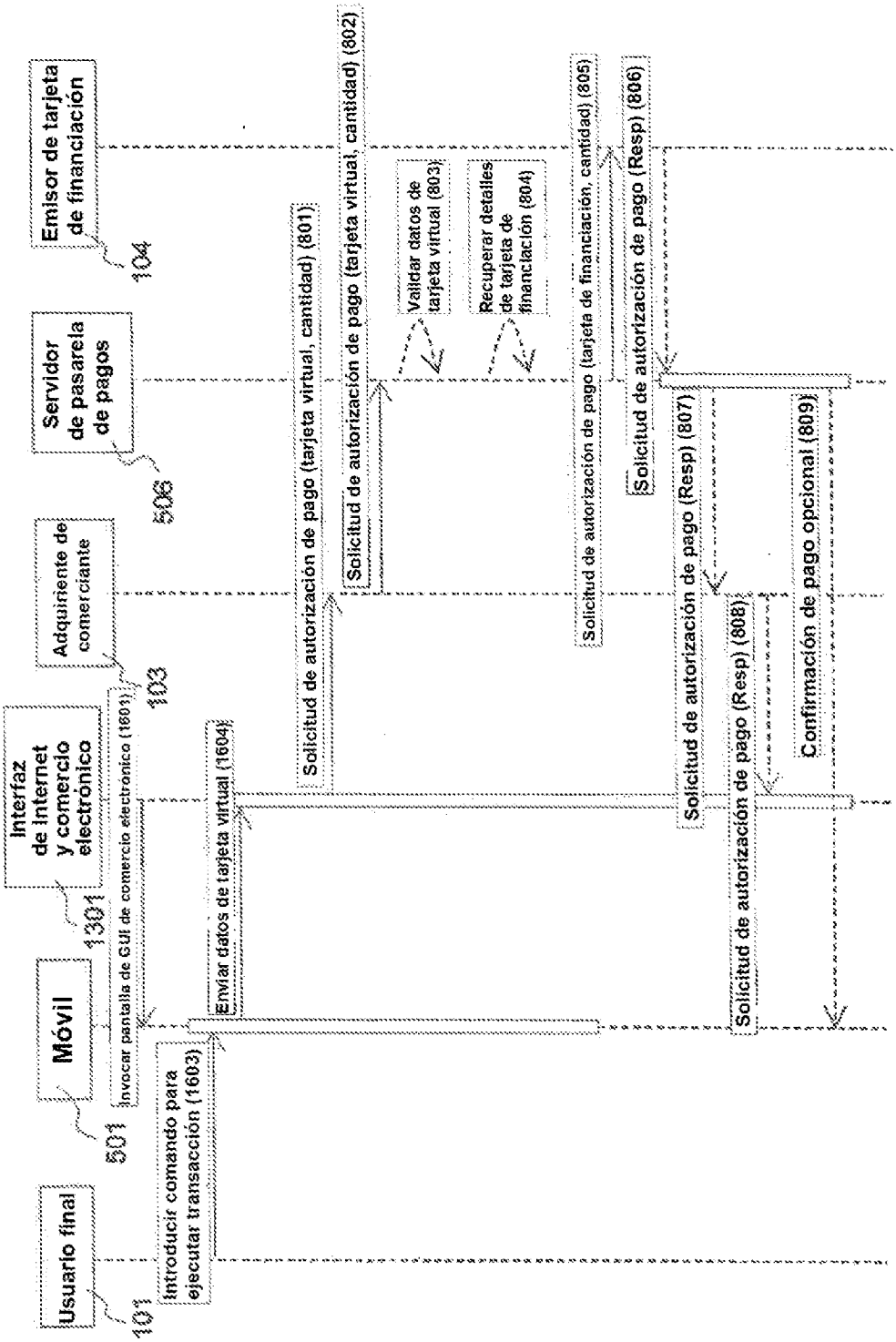
Usuario final
101
Móvil
601
Interfaz de internet y comercio electrónico
1301
Adquiriente de comerciante
103
Servidor de pasarela de pagos
606
Emisor de tarjeta de financiación
104
Invocar pantalla de GUI de comercio electrónico (1601)
Introducir comando para ejecutar transacción (1603)
Enviar datos de tarjeta virtual (1604)
Solicitud de autorización de pago (tarjeta virtual, cantidad) (801)
Solicitud de autorización de pago (tarjeta virtual, cantidad) (802)
Validar datos de tarjeta virtual (803)
Recuperar detalles de tarjeta de financiación (804)
Solicitud de autorización de pago (tarjeta de financiación, cantidad) (805)
Solicitud de autorización de pago (Resp) (806)
Solicitud de autorización de pago (Resp) (807)
Solicitud de autorización de pago (Resp) (808)
Confirmación de pago opcional (809)

FIG. 17

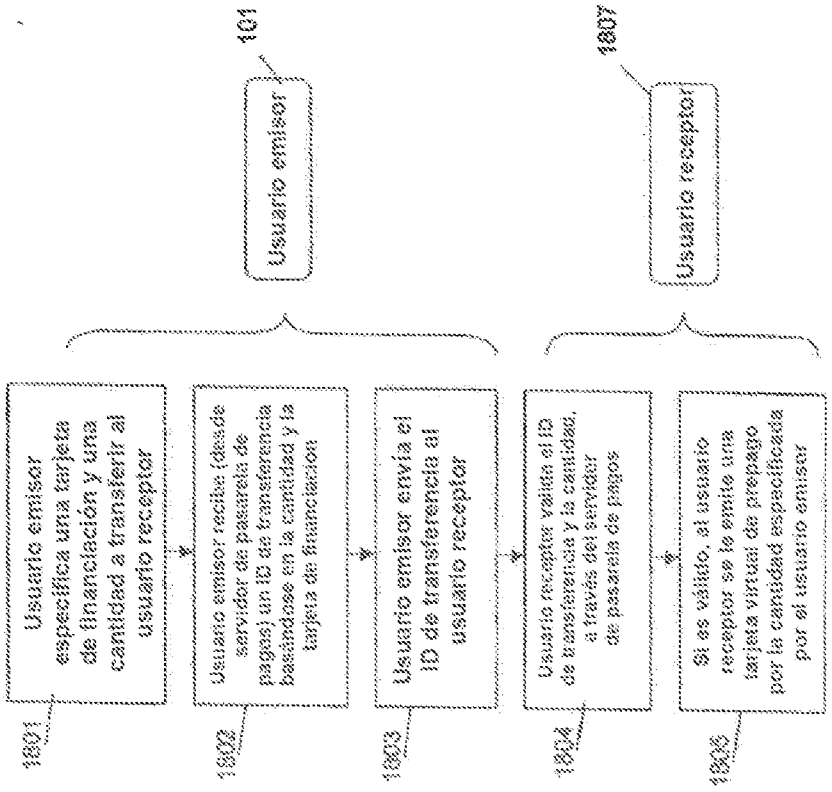
101
Usuario emisor
1807
Usuario receptor
1801
Usuario emisor especifica una tarjeta de financiación y una cantidad a transferir al usuario receptor
1802
Usuario emisor recibe (desde servidor de pasarela de pagos) un ID de transferencia basándose en la cantidad y la tarjeta de financiación
1803
Usuario emisor envía el ID de transferencia al usuario receptor
1804
Usuario receptor valida el ID de transferencia y la cantidad, a través del servidor de pasarela de pagos
1805
Si es válido, al usuario receptor se le emite una tarjeta virtual de prepago por la cantidad especificada por el usuario emisor

FIG. 18

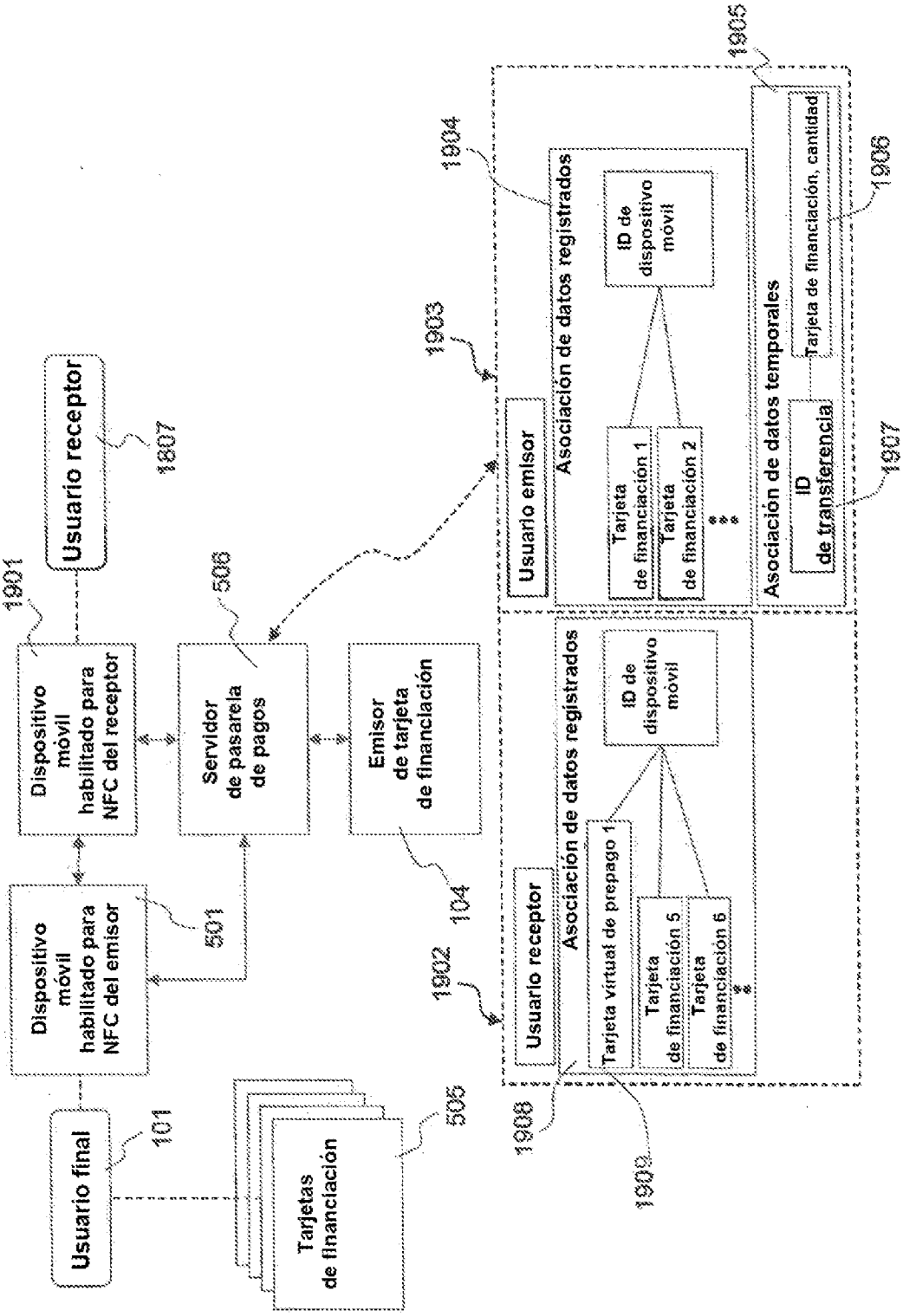
Usuario final
101
Dispositivo móvil habilitado para NFC del emisor
501
Dispositivo móvil habilitado para NFC del receptor
1901
Usuario receptor
1807
Tarjetas de financiación
505
Servidor de pasarela de pagos
508
Emisor de tarjeta de financiación
104
1902
Usuario receptor
1908
Asociación de datos registrados
Tarjeta virtual de prepago 1
Tarjeta de financiación 5
Tarjeta de financiación 6
ID de dispositivo móvil
1909
1903
Usuario emisor
1904
Asociación de datos registrados
Tarjeta de financiación 1
Tarjeta de financiación 2
ID de dispositivo móvil
1905
Asociación de datos temporales
ID de transferencia
1907
Tarjeta de financiación, cantidad
1906

FIG. 19

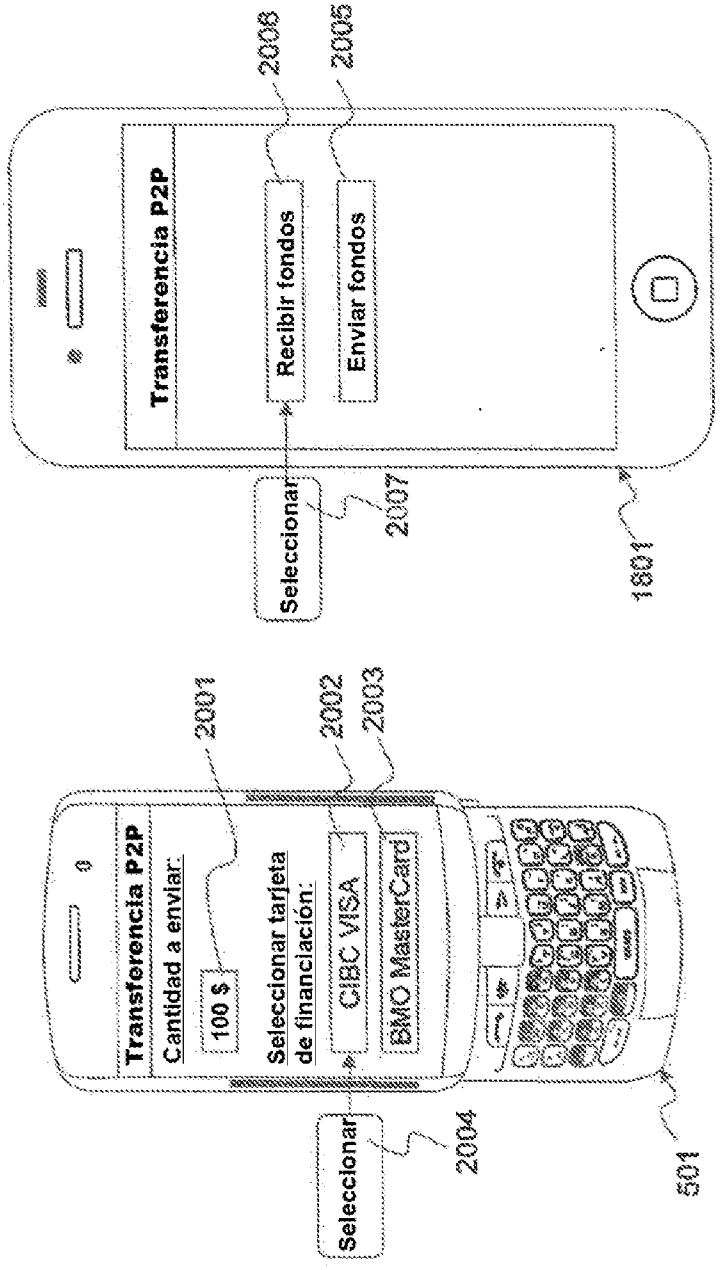
Transferencia P2P
Recibir fondos
Enviar fondos
2006
2005
Seleccionar
2007
1601
Transferencia P2P
Cantidad a enviar:
100 $
Seleccionar tarjeta de financiación:
CIBC VISA
BMO MasterCard
2001
2002
2003
Seleccionar
2004
501

FIG. 20

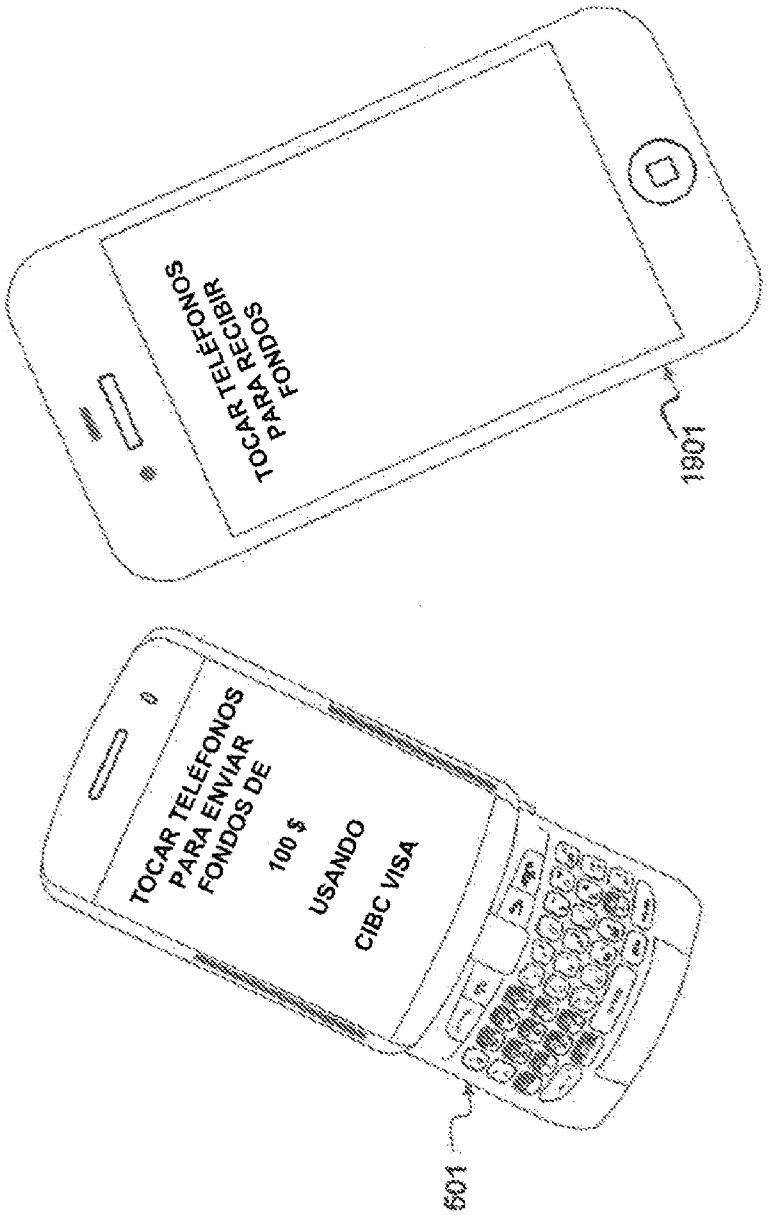
TOCAR TELÉFONOS PARA RECIBIR FONDOS
1901
TOCAR TELÉFONOS PARA ENVIAR FONDOS DE
100 $
USANDO
CIBC VISA
601

FIG. 21

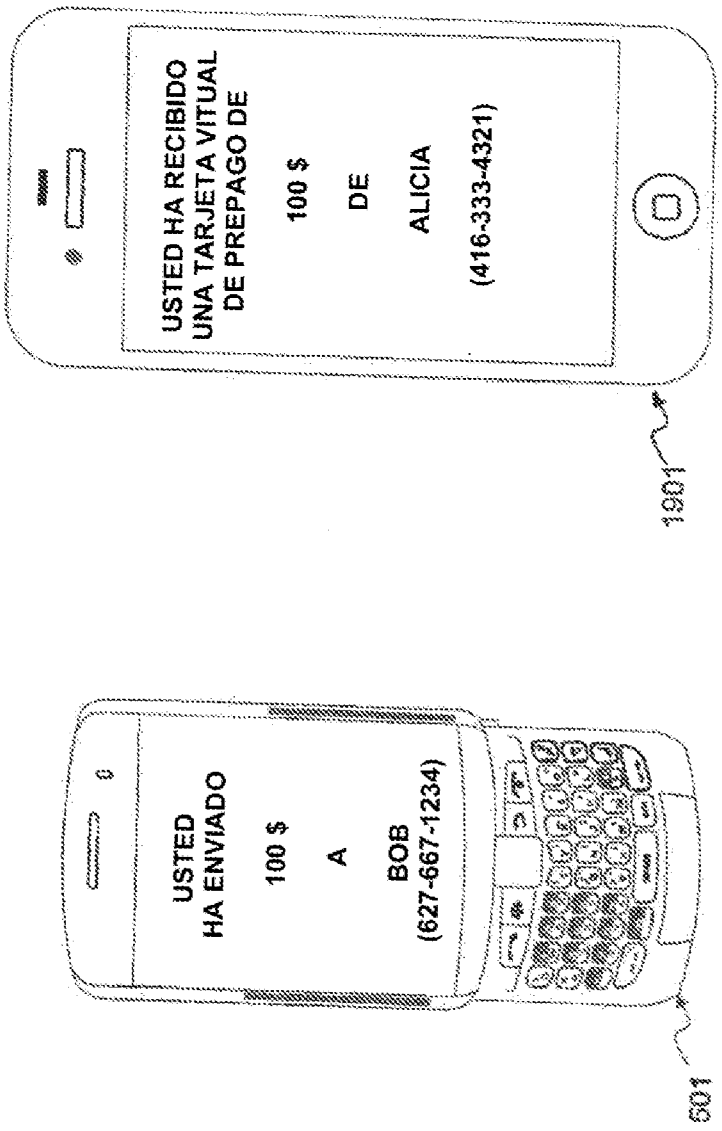
USTED HA RECIBIDO UNA TARJETA VITUAL DE PREPAGO DE
100 $
DE
ALICIA
(416-333-4321)
1901
USTED HA ENVIADO
100 $
A
BOB
(627-667-1234)
601

FIG. 22

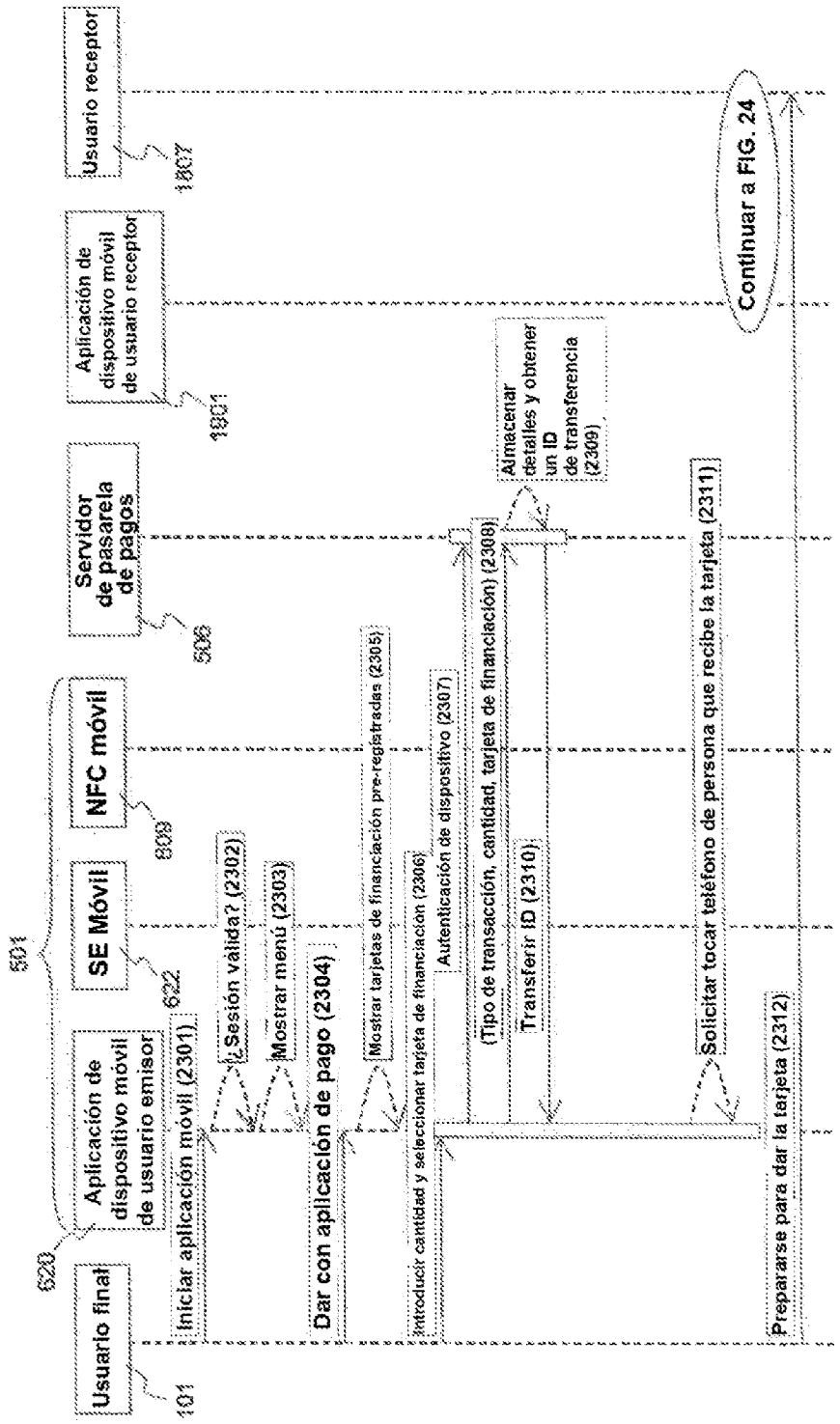
Usuario final
Aplicación de dispositivo móvil de usuario emisor
SE Móvil
NFC móvil
Servidor de pasarela de pagos
Aplicación de dispositivo móvil de usuario receptor
Usuario receptor
620
501
101
622
809
808
1801
1807
Iniciar aplicación móvil (2301)
¿Sesión válida? (2302)
Mostrar menú (2303)
Dar con aplicación de pago (2304)
Mostrar tarjetas de financiación pre-registradas (2305)
Introducir cantidad y seleccionar tarjeta de financiación (2306)
Autenticación de dispositivo (2307)
(Tipo de transacción, cantidad, tarjeta de financiación) (2308)
Almacenar detalles y obtener un ID de transferencia (2309)
Transferir ID (2310)
Solicitar tocar teléfono de persona que recibe la tarjeta (2311)
Prepararse para dar la tarjeta (2312)
Continuar a FIG. 24

FIG. 23

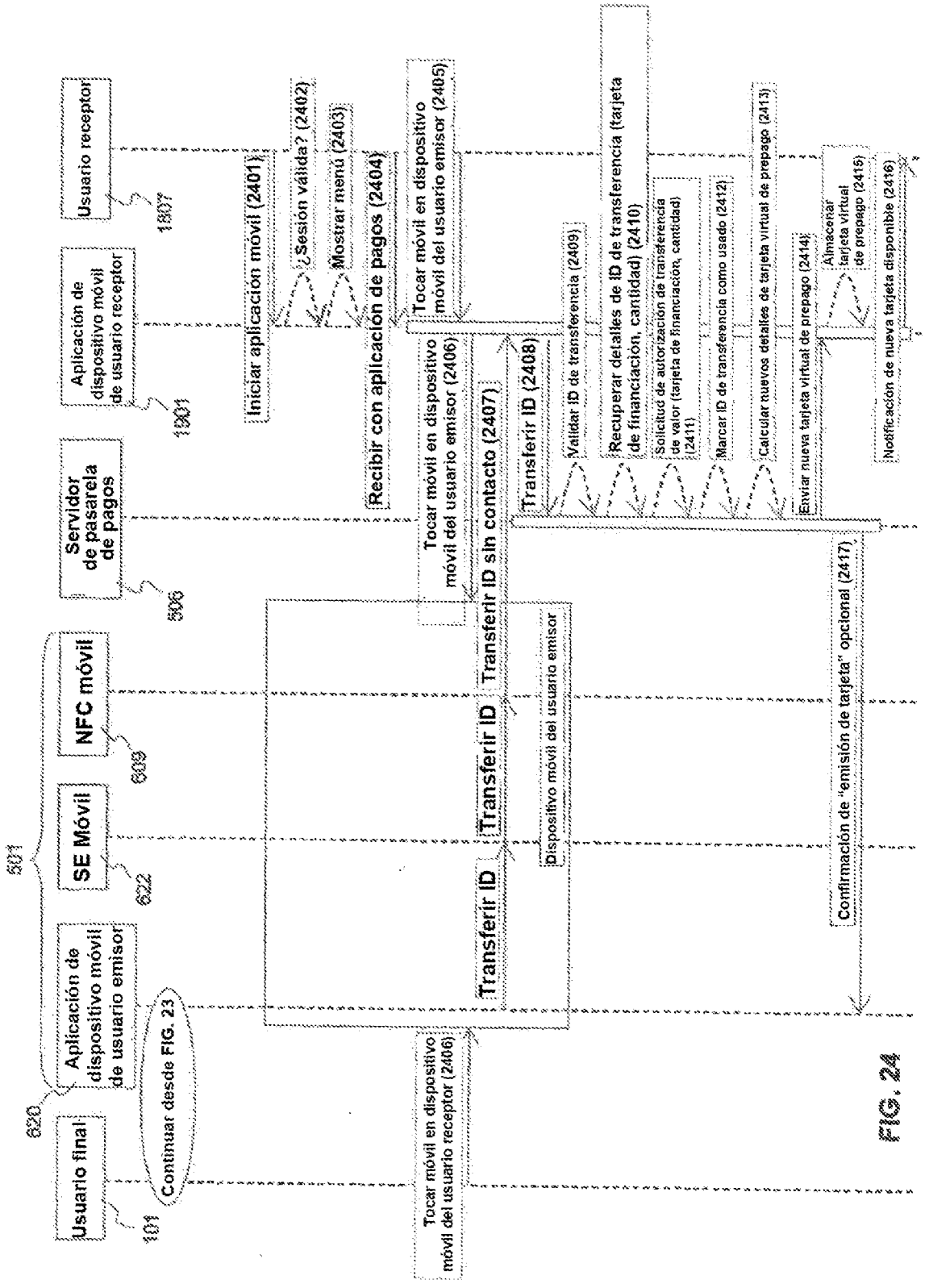
Usuario final
101
Continuar desde FIG. 23
620
Aplicación de dispositivo móvil de usuario emisor
SE Móvil
622
NFC móvil
609
621
Servidor de pasarela de pagos
506
Aplicación de dispositivo móvil de usuario receptor
1801
Usuario receptor
1807
Tocar móvil en dispositivo móvil del usuario receptor (2406)
Transferir ID
Transferir ID sin contacto (2407)
Dispositivo móvil del usuario emisor
Tocar móvil en dispositivo móvil del usuario emisor (2406)
Iniciar aplicación móvil (2401)
¿Sesión válida? (2402)
Mostrar menú (2403)
Recibir con aplicación de pagos (2404)
Tocar móvil en dispositivo móvil del usuario emisor (2405)
Transferir ID (2408)
Validar ID de transferencia (2409)
Recuperar detalles de ID de transferencia (tarjeta de financiación, cantidad) (2410)
Solicitud de autorización de transferencia de valor (tarjeta de financiación, cantidad) (2411)
Marcar ID de transferencia como usado (2412)
Calcular nuevos detalles de tarjeta virtual de prepago (2413)
Enviar nueva tarjeta virtual de prepago (2414)
Almacenar tarjeta virtual de prepago (2416)
Notificación de nueva tarjeta disponible (2416)
Confirmación de "emisión de tarjeta" opcional (2417)

FIG. 24

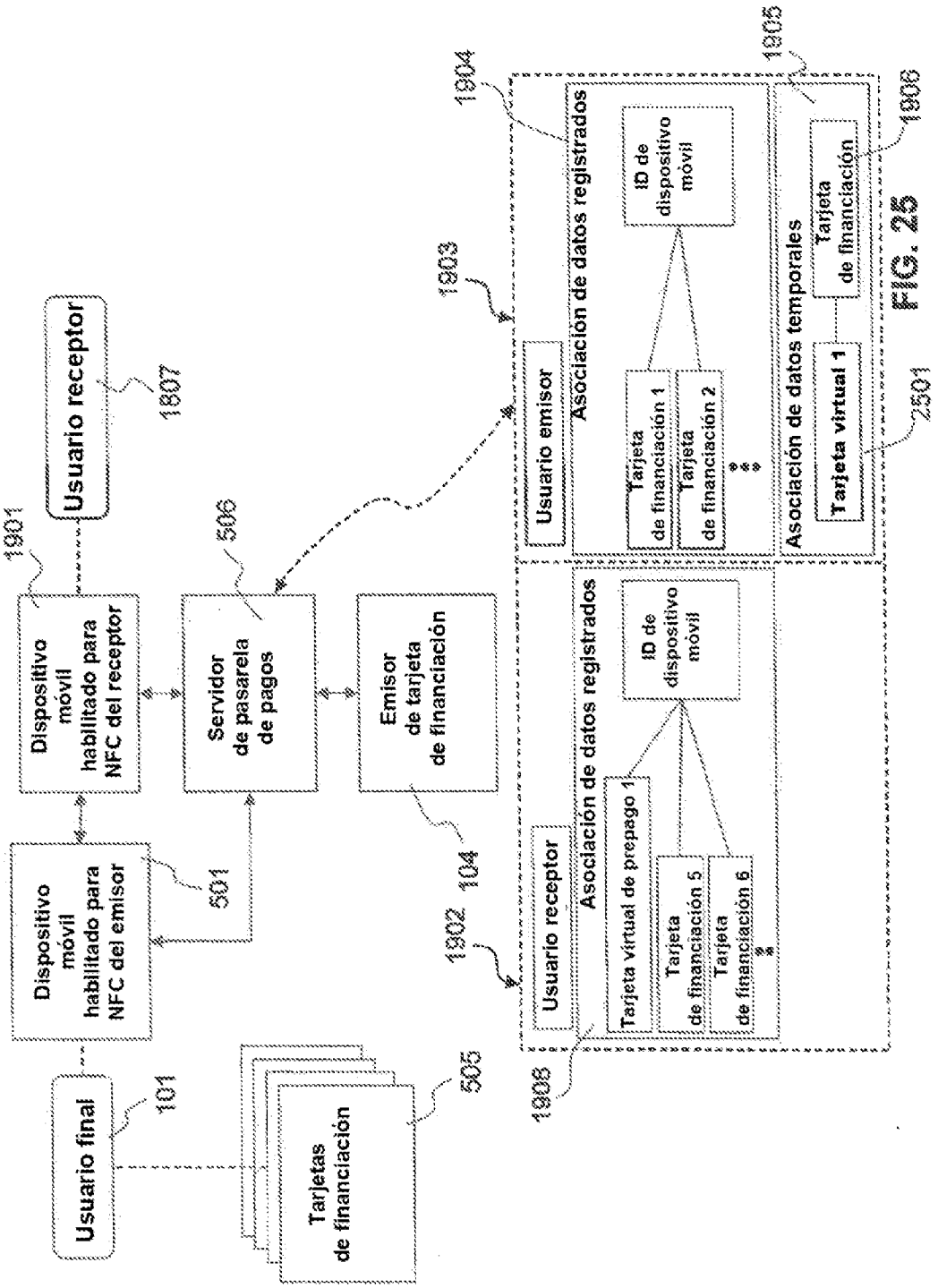
Usuario final
101
Tarjetas de financiación
505
Dispositivo móvil habilitado para NFC del emisor
501
Dispositivo móvil habilitado para NFC del receptor
1901
Usuario receptor
1807
Servidor de pasarela de pagos
506
Emisor de tarjeta de financiación
104
1902
1903
1904
1905
1906
Usuario receptor
Asociación de datos registrados
Tarjeta virtual de prepago 1
Tarjeta de financiación 5
Tarjeta de financiación 6
ID de dispositivo móvil
Usuario emisor
Asociación de datos registrados
Tarjeta de financiación 1
Tarjeta de financiación 2
ID de dispositivo móvil
Asociación de datos temporales
Tarjeta virtual 1
2501
Tarjeta de financiación
1908

FIG. 25

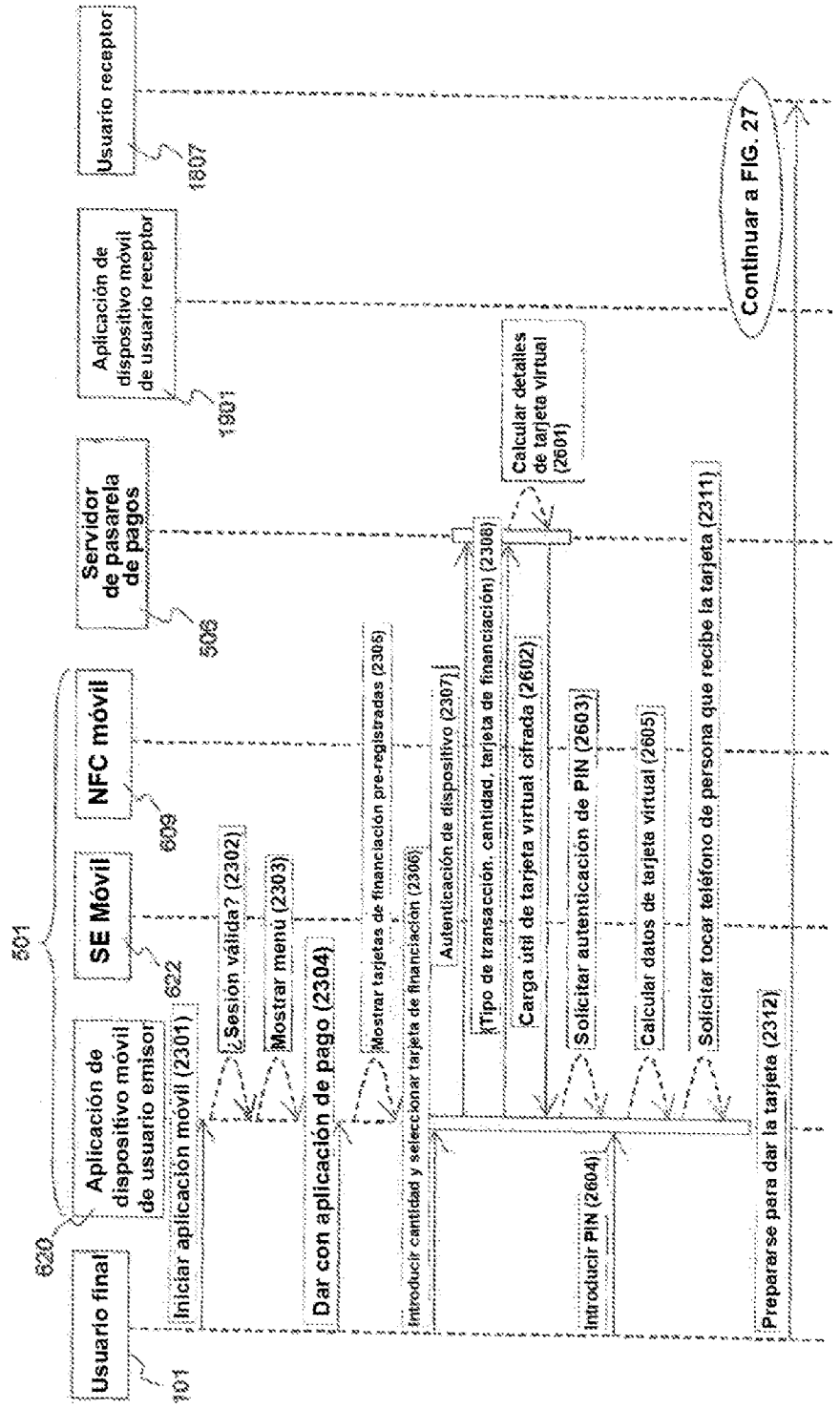
Usuario final
Aplicación de dispositivo móvil de usuario emisor
SE Móvil
NFC móvil
Servidor de pasarela de pagos
Aplicación de dispositivo móvil de usuario receptor
Usuario receptor
101
620
501
622
609
606
1901
1607
Iniciar aplicación móvil (2301)
Sesión válida? (2302)
Mostrar menú (2303)
Dar con aplicación de pago (2304)
Mostrar tarjetas de financiación pre-registradas (2305)
Introducir cantidad y seleccionar tarjeta de financiación (2306)
Autenticación de dispositivo (2307)
(Tipo de transacción, cantidad, tarjeta de financiación) (2308)
Calcular detalles de tarjeta virtual (2601)
Carga útil de tarjeta virtual cifrada (2602)
Solicitar autenticación de PIN (2603)
Introducir PIN (2604)
Calcular datos de tarjeta virtual (2605)
Solicitar tocar teléfono de persona que recibe la tarjeta (2311)
Preparar se para dar la tarjeta (2312)
Continuar a FIG. 27

FIG. 26

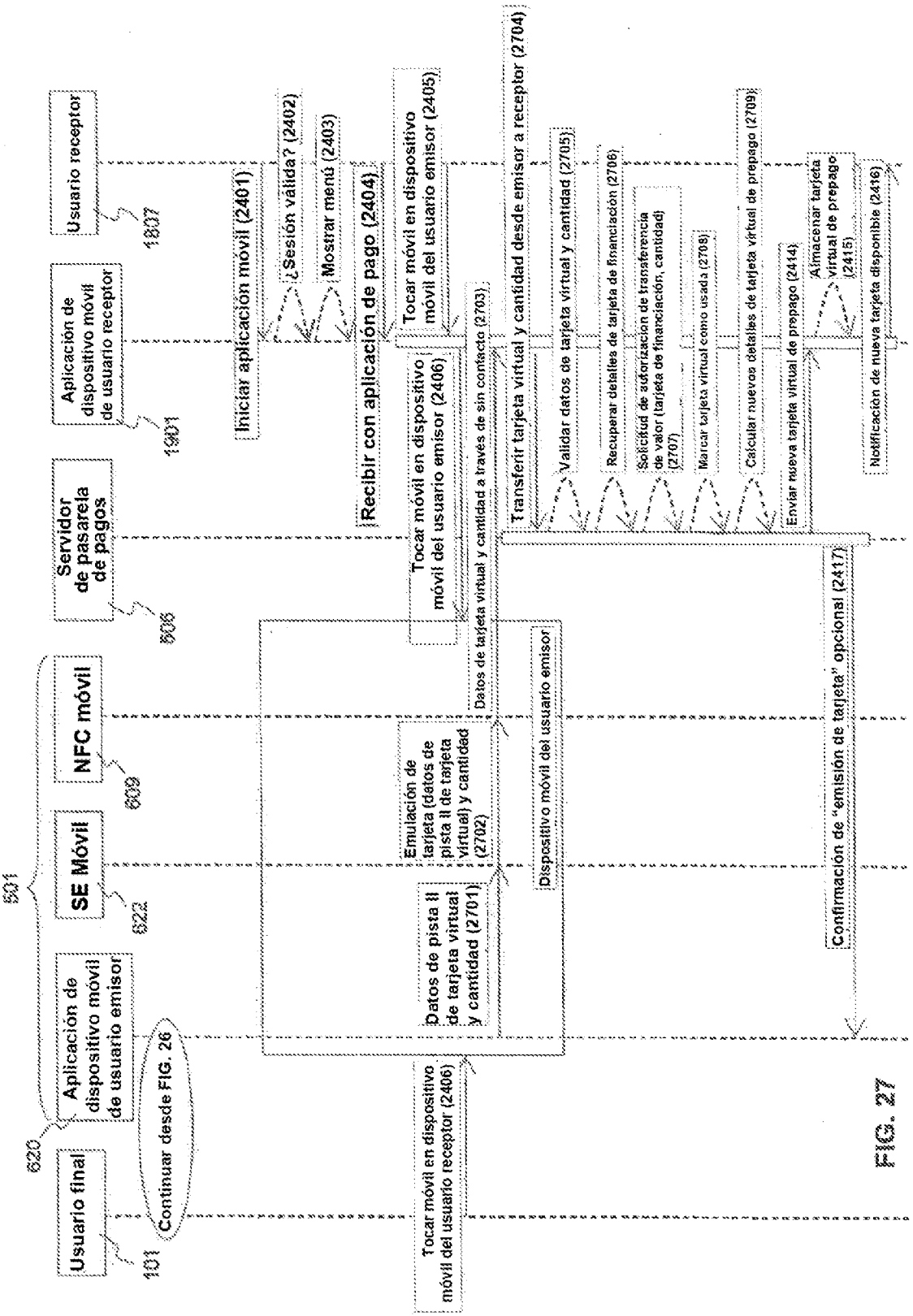
501
620
Usuario final
101
Aplicación de dispositivo móvil de usuario emisor
SE Móvil
622
NFC móvil
609
Servidor de pasarela de pagos
606
Aplicación de dispositivo móvil de usuario receptor
1901
Usuario receptor
1807
Continuar desde FIG. 26
Tocar móvil en dispositivo móvil del usuario receptor (2406)
Datos de pista II de tarjeta virtual y cantidad (2701)
Emulación de tarjeta (datos de pista II de tarjeta virtual) y cantidad (2702)
Datos de tarjeta virtual y cantidad a través de sin contacto (2703)
Dispositivo móvil del usuario emisor
Tocar móvil en dispositivo móvil del usuario emisor (2406)
Iniciar aplicación móvil (2401)
¿Sesión válida? (2402)
Mostrar menú (2403)
Recibir con aplicación de pago (2404)
Tocar móvil en dispositivo móvil del usuario emisor (2405)
Transferir tarjeta virtual y cantidad desde emisor a receptor (2704)
Validar datos de tarjeta virtual y cantidad (2705)
Recuperar detalles de tarjeta de financiación (2706)
Solicitud de autorización de transferencia de valor (tarjeta de financiación, cantidad) (2707)
Marcar tarjeta virtual como usada (2708)
Calcular nuevos detalles de tarjeta virtual de prepago (2709)
Enviar nueva tarjeta virtual de prepago (2414)
Almacenar tarjeta virtual de prepago (2415)
Confirmación de "emisión de tarjeta" opcional (2417)
Notificación de nueva tarjeta disponible (2416)

FIG. 27

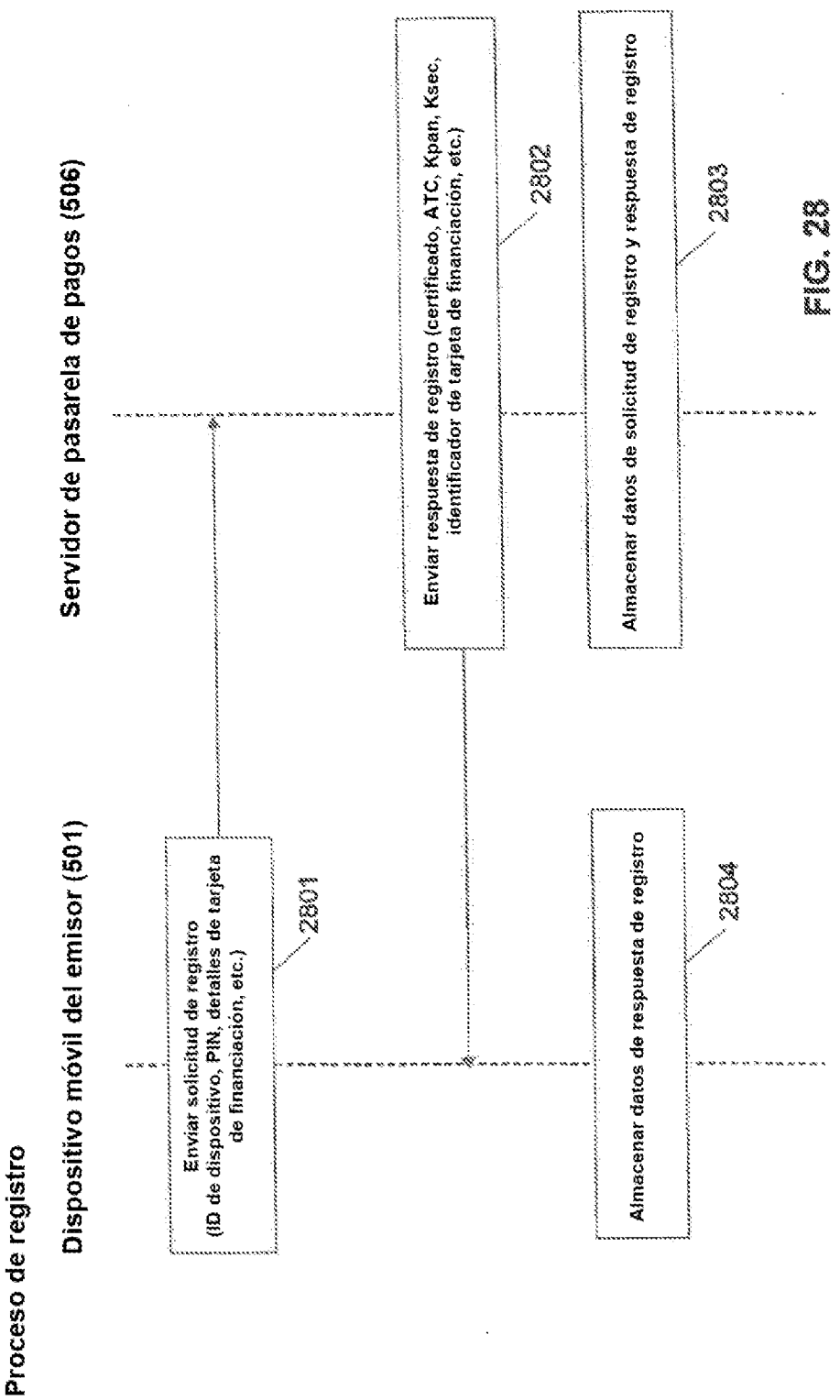
Proceso de registro
Dispositivo móvil del emisor (501)
Servidor de pasarela de pagos (506)
Enviar solicitud de registro (ID de dispositivo, PIN, detalles de tarjeta de financiación, etc.)
2801
Enviar respuesta de registro (certificado, ATC, Kpan, Ksec, identificador de tarjeta de financiación, etc.)
2802
Almacenar datos de solicitud de registro y respuesta de registro
2803
Almacenar datos de respuesta de registro
2804

FIG. 28

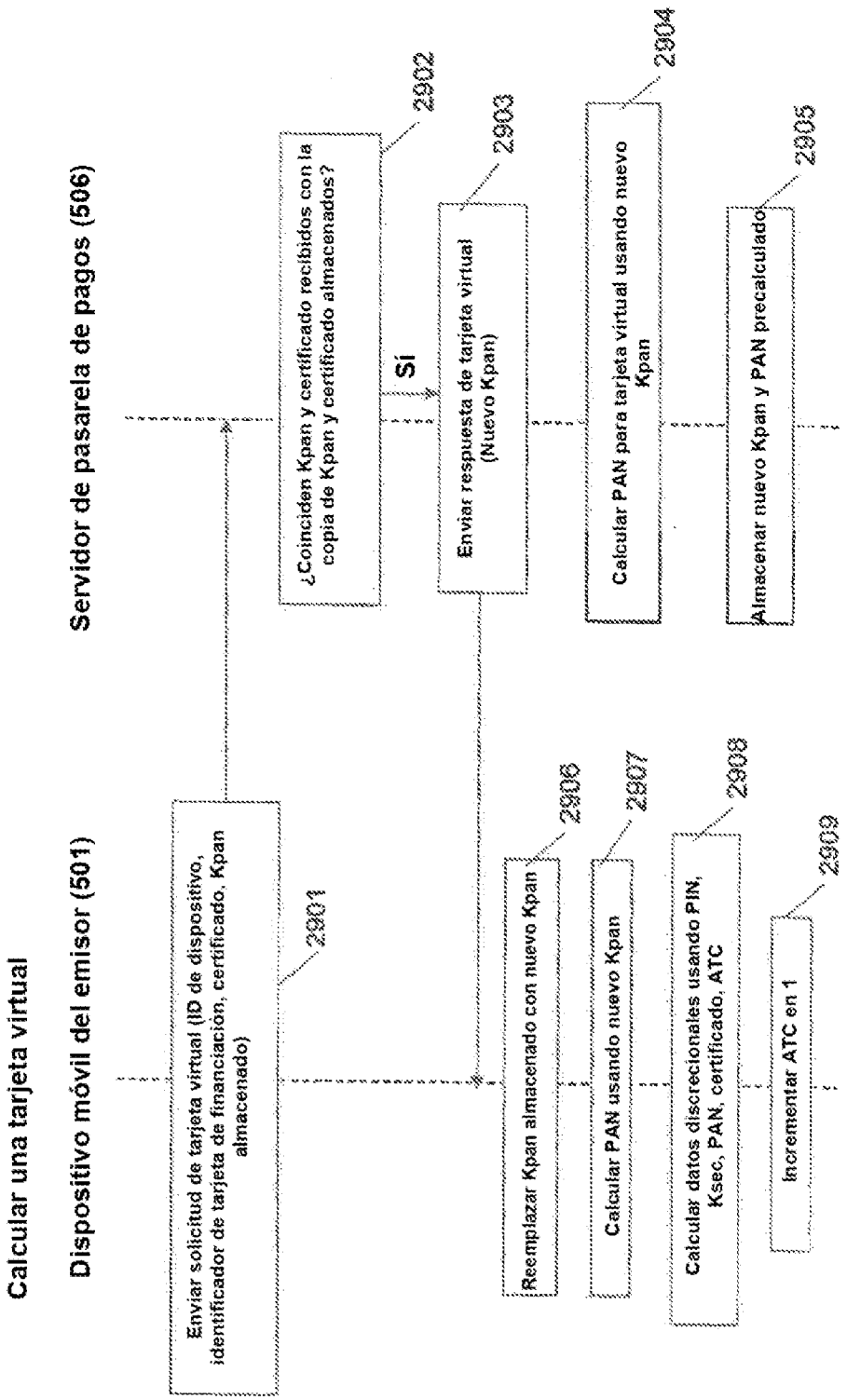
Calcular una tarjeta virtual
Dispositivo móvil del emisor (501)
Servidor de pasarela de pagos (506)
Enviar solicitud de tarjeta virtual (ID de dispositivo, identificador de tarjeta de financiación, certificado, Kpan almacenado)
2901
¿Coinciden Kpan y certificado recibidos con la copia de Kpan y certificado almacenados?
2902
Sí
Enviar respuesta de tarjeta virtual (Nuevo Kpan)
2903
Calcular PAN para tarjeta virtual usando nuevo Kpan
2904
Almacenar nuevo Kpan y PAN precalculado
2905
Reemplazar Kpan almacenado con nuevo Kpan
2906
Calcular PAN usando nuevo Kpan
2907
Calcular datos discrecionales usando PIN, Ksec, PAN, certificado, ATC
2908
Incrementar ATC en 1
2909

FIG. 29

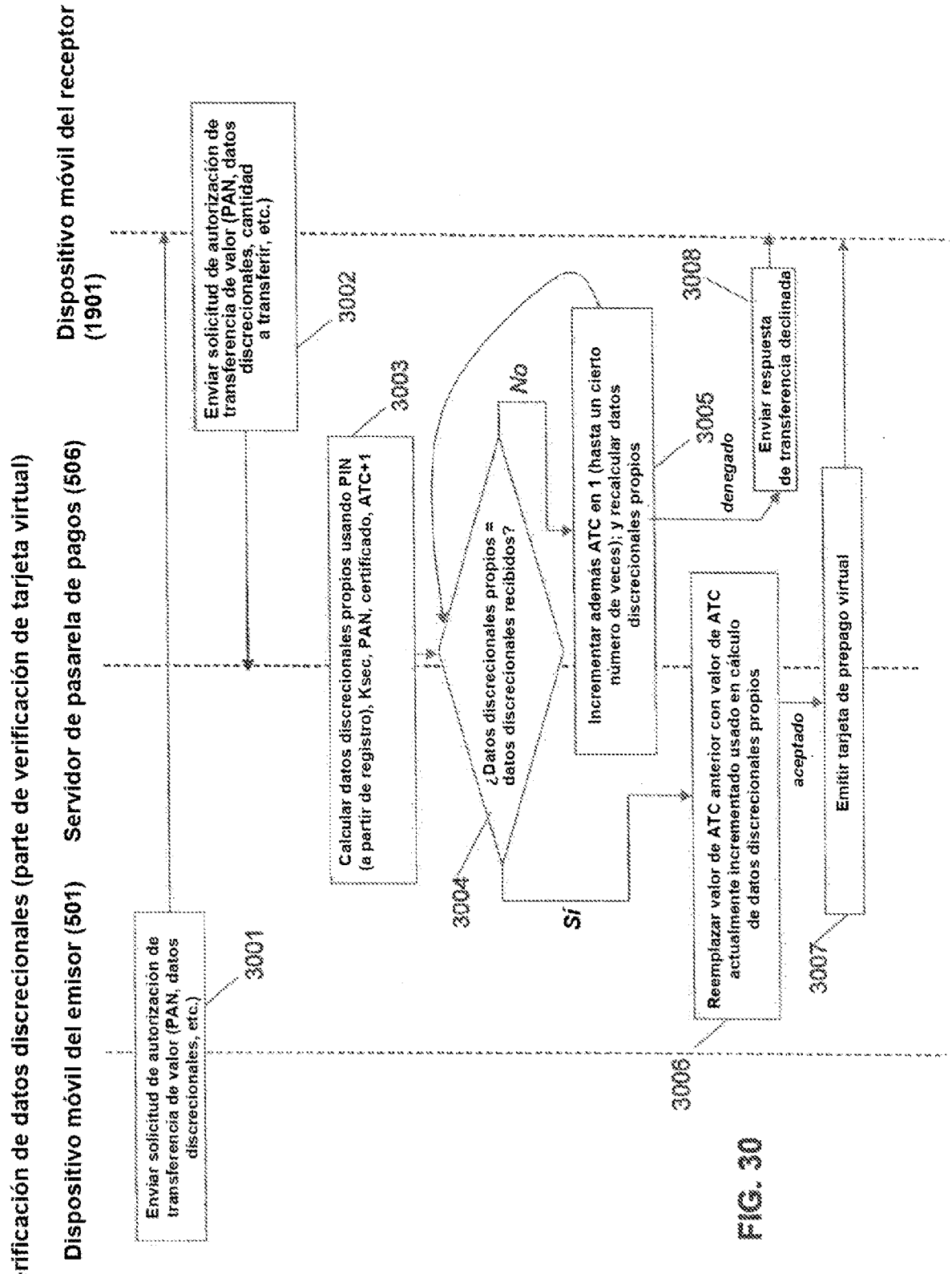
Verificación de datos discrecionales (parte de verificación de tarjeta virtual)
Dispositivo móvil del emisor (501)
Servidor de pasarela de pagos (506)
Dispositivo móvil del receptor (1901)
Enviar solicitud de autorización de transferencia de valor (PAN, datos discrecionales, etc.)
3001
Enviar solicitud de autorización de transferencia de valor (PAN, datos discrecionales, cantidad a transferir, etc.)
3002
Calcular datos discrecionales propios usando PIN (a partir de registro), Ksec, PAN, certificado, ATC+1
3003
¿Datos discrecionales propios = datos discrecionales recibidos?
3004
No
Sí
Incrementar además ATC en 1 (hasta un cierto número de veces); y recalcular datos discrecionales propios
3005
denegado
Enviar respuesta de transferencia declinada
3008
Reemplazar valor de ATC anterior con valor de ATC actualmente incrementado usado en cálculo de datos discrecionales propios
3006
aceptado
Emitir tarjeta de prepago virtual
3007

FIG. 30