

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 926 590**

51 Int. Cl.:

H04W 8/20 (2009.01)

H04W 12/08 (2011.01)

H04W 12/069 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **28.04.2014** **E 18196982 (5)**

97 Fecha y número de publicación de la concesión europea: **22.06.2022** **EP 3484199**

54 Título: **Método de descarga de la tarjeta virtual y terminal**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
27.10.2022

73 Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian,
Longgang District
Shenzhen, Guangdong 518129, CN

72 Inventor/es:

SUI, SANJUN

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 926 590 T3

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

DESCRIPCIÓN

Método de descarga de la tarjeta virtual y terminal

La presente invención se refiere al campo de las tecnologías de la comunicación y, en particular, con un método de descarga de tarjeta virtual, un terminal y un medio de almacenamiento legible por ordenador.

5 Antecedentes

La tarjeta SIM virtual (virtual sim card, VSIM para abreviar) es un concepto totalmente nuevo actualmente en el campo de los terminales móviles. Desde la perspectiva de las funciones, la VSIM puede reemplazar a una tarjeta SIM física que actualmente se coloca dentro de un terminal. La VSIM puede descargarse convenientemente mediante el uso de una red y proporciona más comodidad para que un usuario use servicios, tales como servicios de itinerancia.

10 Un usuario que usa la VSIM no necesita insertar otra tarjeta SIM física en un teléfono móvil, excepto una tarjeta SIM de ubicación local, sino que solicita un servidor usando un número recién creado, usa un canal de datos de un estándar de comunicaciones 2G/3G u otro estándar, descarga e instala datos VSIM que son equivalentes a otra tarjeta SIM en el teléfono móvil, de modo que el usuario tiene un número de teléfono móvil extra.

15 En el estado de la técnica, descargar la VSIM se realiza totalmente a través de internet, es decir, un terminal conectado a internet puede descargar, directamente a través de internet, la VSIM desde un servidor de datos desplegado por un operador. Se puede ver que la descarga de VSIM es muy cómoda, pero la limitación también es muy obvia, es decir, la implementación depende de internet.

20 Debido a esto, las desventajas de la técnica anterior son: cuando un usuario no puede conectarse a internet debido a razones de itinerancia, atravesar áreas de servicio o similares, el usuario no puede descargar normalmente la VSIM y no puede usar los servicios relacionados.

La patente EP 2076071 A1 describe disponer una capacidad para respaldar información de suministro de telefonía celular y datos personales desde un teléfono móvil, en un servidor.

Compendio

25 De acuerdo con la invención, se da a conocer un método de descarga de tarjeta virtual, un dispositivo terminal y un medio de almacenamiento legible por ordenador, tal como se expone en las reivindicaciones.

La presente invención da a conocer un método de descarga de tarjeta virtual, un terminal y un dispositivo intermedio, de manera que mediante un método para descargar una tarjeta virtual utilizando un dispositivo intermedio, el terminal puede usar normalmente un servicio VSIM sin estar conectado a internet.

30 Los siguientes aspectos primero, cuarto, séptimo y décimo no son según la invención y están presentes únicamente con fines ilustrativos.

Para resolver el problema técnico anterior, las soluciones técnicas utilizadas por la presente invención son:

según un primer aspecto, la presente invención da a conocer un método de descarga de tarjeta virtual, donde el método incluye:

35 preestablecer, por un terminal, una condición de escenario, y notificar la información del terminal a un servidor cuando se cumple la condición de escenario preestablecida, donde la información del terminal se usa para permitir que el servidor cree una cuenta para el terminal y asocie la cuenta con datos de tarjeta virtual; y

acceder, mediante el terminal, al servidor utilizando la cuenta, y descargar los datos de tarjeta virtual asociados con la cuenta, donde

la condición de escenario es que el terminal establezca una conexión de comunicación con el servidor.

40 En una primera posible forma de implementación del primer aspecto, el método incluye además:

realizar, mediante el terminal, negociación de cifrado con el servidor, y obtener una clave de negociación, donde la clave de negociación se usa para permitir que el servidor cifre la cuenta y los datos de tarjeta virtual usando la clave de negociación.

45 En una segunda posible forma de implementación del primer aspecto, acceder, mediante el terminal, al servidor utilizando la cuenta, y descargar los datos de tarjeta virtual asociados con la cuenta, es específicamente:

descifrar, mediante el terminal, la cuenta del terminal utilizando la clave de negociación, y acceder al servidor utilizando la cuenta; y descifrar, mediante el terminal usando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta, y descargar los datos de tarjeta virtual.

Según un segundo aspecto, la presente invención da a conocer un método de descarga de tarjeta virtual, donde el método incluye:

establecer, por un terminal, una conexión de comunicación a un dispositivo intermedio conectado a un servidor;

5 notificar, mediante el terminal, información del terminal al servidor usando el dispositivo intermedio, donde la información del terminal se usa para permitir al servidor crear una cuenta para el terminal y asociar la cuenta con datos de tarjeta virtual; y

acceder, mediante el terminal, al dispositivo intermedio utilizando la cuenta, y descargar los datos de tarjeta virtual asociados a la cuenta.

10 En una primera posible forma de implementación del segundo aspecto, establecer, por un terminal, una conexión de comunicación a un dispositivo intermedio, es específicamente:

establecer, mediante el terminal, una conexión de comunicación de campo cercano al dispositivo intermedio.

En una segunda posible forma de implementación del segundo aspecto, el método incluye además:

15 realizar, mediante el terminal, negociación de cifrado con una clave pública del servidor almacenada en el dispositivo intermedio, y obtener una clave de negociación, donde la clave de negociación se usa para permitir que el servidor o el dispositivo intermedio cifren la cuenta y los datos de tarjeta virtual usando la clave de negociación.

En una tercera posible forma de implementación del segundo aspecto, acceder, mediante el terminal, al dispositivo intermedio mediante el uso de la cuenta, y descargar los datos de tarjeta virtual asociados a la cuenta, es específicamente:

20 descifrar, mediante el terminal, la cuenta del terminal utilizando la clave de negociación, y acceder al dispositivo intermedio utilizando la cuenta; y descifrar, mediante el terminal usando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta, y descargar los datos de tarjeta virtual.

Según un tercer aspecto, la presente invención da a conocer un método de descarga de tarjeta virtual, donde el método incluye:

establecer, mediante un dispositivo intermedio, una conexión de comunicación a un terminal, y conectar, mediante el dispositivo intermedio, a un servidor;

25 recibir, por el dispositivo intermedio, información del terminal notificada mediante el terminal;

enviar, por el dispositivo intermedio, la información del terminal al servidor, donde el servidor utiliza la información del terminal para crear una cuenta para el terminal y determinar los datos de tarjeta virtual asociados con la cuenta; y

recibir, por el dispositivo intermedio, el acceso del terminal, y enviar los datos de tarjeta virtual al terminal.

30 En una primera posible forma de implementación del tercer aspecto, establecer, por un dispositivo intermedio, de una conexión de comunicación a un terminal, es específicamente:

establecer, por el dispositivo intermedio, una conexión de comunicación de campo cercano al terminal.

En una segunda posible forma de implementación del tercer aspecto, enviar, por el dispositivo intermedio, los datos de tarjeta virtual al terminal, es específicamente:

35 buscar, por el dispositivo intermedio, para encontrar si los datos de tarjeta virtual están almacenados en almacenamiento del dispositivo intermedio, y si los datos de tarjeta virtual están almacenados en el almacenamiento del dispositivo intermedio, extraer los datos de tarjeta virtual del almacenamiento del dispositivo intermedio y enviar los datos de tarjeta virtual; en caso contrario, adquirir, por el dispositivo intermedio, los datos de tarjeta virtual del servidor y enviar los datos de tarjeta virtual al terminal.

40 En una tercera posible forma de implementación del tercer aspecto, el método incluye además:

realizar, por el dispositivo intermedio, negociación de cifrado con el terminal utilizando una clave pública del servidor almacenada en el dispositivo intermedio, obteniendo una clave de negociación y cifrando la cuenta y los datos de tarjeta virtual utilizando la clave de negociación.

45 En una cuarta posible forma de implementación del tercer aspecto, el cifrado de la cuenta y los datos de tarjeta virtual mediante el uso de la clave de negociación, es específicamente:

buscar, por el dispositivo intermedio, para encontrar si la clave de negociación está almacenada en almacenamiento del dispositivo intermedio, y si la clave de negociación está almacenada en el almacenamiento del dispositivo intermedio, realizar, por el dispositivo intermedio, el cifrado utilizando la clave de negociación

almacenado en el almacenamiento del dispositivo intermedio; en caso contrario, adquirir, por el dispositivo intermedio, la clave de negociación del servidor y realizar el cifrado.

Según un cuarto aspecto, la presente invención da a conocer un terminal, donde el terminal incluye:

5 un primer módulo de notificación, configurado para preestablecer una condición de escenario, y notificar la información del terminal a un servidor cuando se cumple la condición de escenario preestablecida, donde la información del terminal se usa para permitir que el servidor cree una cuenta para el terminal y para asociar la cuenta con datos de tarjeta virtual, y la condición de escenario es que el terminal establezca una conexión de comunicación con el servidor; y

10 un primer módulo de descarga, configurado para acceder al servidor utilizando la cuenta, y descargar los datos de tarjeta virtual asociados a la cuenta.

En una primera posible forma de implementación del cuarto aspecto, el terminal incluye además:

un primer módulo de negociación, configurado para realizar negociación de cifrado con el servidor y obtener una clave de negociación, donde la clave de negociación se usa para permitir que el servidor cifre la cuenta y los datos de tarjeta virtual usando la clave de negociación; y

15 un primer módulo de descifrado, configurado para descifrar la cuenta del terminal utilizando la clave de negociación, y descifrar, utilizando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta.

Según un quinto aspecto, la presente invención da a conocer un terminal, donde el terminal incluye:

un módulo de comunicaciones, configurado para establecer una conexión de comunicación con un dispositivo intermedio conectado a un servidor;

20 un segundo módulo de notificación, configurado para notificar la información del terminal al servidor usando el dispositivo intermedio, donde la información del terminal se usa para permitir que el servidor cree una cuenta para el terminal y asocie la cuenta con los datos de tarjeta virtual; y

un segundo módulo de descarga, configurado para acceder al dispositivo intermedio utilizando la cuenta, y descargar los datos de tarjeta virtual asociados a la cuenta.

25 En una primera posible forma de implementación del quinto aspecto, el terminal incluye además:

un segundo módulo de negociación, configurado para realizar negociación de cifrado con una clave pública del servidor almacenada en el dispositivo intermedio, y obtener una clave de negociación, donde la clave de negociación se usa para permitir que el servidor o el dispositivo intermedio cifren la cuenta y los datos de tarjeta virtual mediante el uso de la clave de negociación; y

30 un segundo módulo de descifrado, configurado para descifrar la cuenta del terminal utilizando la clave de negociación, y descifrar, utilizando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta.

Según un sexto aspecto, la presente invención da a conocer un dispositivo intermedio, donde el dispositivo intermedio incluye:

35 un módulo de conexión, configurado para establecer una conexión de comunicación a un terminal, y conectarse a un servidor;

un módulo de notificación, configurado para recibir información del terminal notificada mediante el terminal, y enviar la información del terminal al servidor, donde el servidor utiliza la información del terminal para crear una cuenta para el terminal y determinar los datos de tarjeta virtual asociados con la cuenta; y

40 un módulo de intercambio, configurado para recibir el acceso del terminal, y enviar los datos de tarjeta virtual al terminal.

En una primera posible forma de implementación del sexto aspecto, el módulo de intercambio incluye:

una unidad de consulta, configurada para buscar si los datos de tarjeta virtual están almacenados en un módulo de almacenamiento;

45 una unidad de almacenamiento, configurada para almacenar los datos de tarjeta virtual y enviar los datos de tarjeta virtual al terminal; y

una unidad de adquisición, configurada para: cuando los datos de tarjeta virtual no están almacenados en el módulo de almacenamiento, adquirir los datos de tarjeta virtual del servidor y almacenar los datos de tarjeta virtual en la unidad de almacenamiento.

En una segunda posible forma de implementación del sexto aspecto, el dispositivo intermedio incluye además:

un módulo de cifrado, configurado para realizar negociación de cifrado con el terminal mediante el uso de una clave pública del servidor almacenada en el dispositivo intermedio, obtener una clave de negociación y cifrar la cuenta y los datos de tarjeta virtual mediante el uso de la clave de negociación.

5 Según un séptimo aspecto, la presente invención da a conocer un terminal, donde el terminal incluye: un procesador, un emisor y un receptor, el procesador está conectado al emisor y el procesador está conectado al receptor, donde

el procesador está configurado para preestablecer una condición de escenario, donde la condición de escenario es que el terminal establezca una conexión de comunicación con un servidor;

10 el emisor está configurado para: cuando se cumple la condición de escenario preestablecida, notificar información del terminal al servidor, donde la información del terminal se utiliza para permitir que el servidor cree una cuenta para el terminal y asocie la cuenta con los datos de tarjeta virtual; y acceda al servidor usando la cuenta; y

el receptor está configurado para: después de que el emisor acceda al servidor usando la cuenta, descargar los datos de tarjeta virtual asociados con la cuenta.

15 En una primera posible forma de implementación del séptimo aspecto, el procesador está configurado además para realizar negociación de cifrado con el servidor y obtener una clave de negociación, donde la clave de negociación se usa para permitir que el servidor cifre la cuenta y los datos de tarjeta virtual mediante utilizar la clave de negociación; descifrar la cuenta del terminal usando la clave de negociación; y descifrar, utilizando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta;

20 el emisor está específicamente configurado para: después de que el procesador descifre la cuenta del terminal usando la clave de negociación, acceder al servidor usando la cuenta; y

el receptor está específicamente configurado para: después de que el procesador descifre, utilizando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta, descargar los datos de tarjeta virtual asociados con la cuenta.

25 Según un octavo aspecto, la presente invención da a conocer un terminal, donde el terminal incluye: un procesador, un emisor y un receptor, el procesador está conectado al emisor y el procesador está conectado al receptor, donde

el procesador está configurado para establecer una conexión de comunicación con un dispositivo intermedio conectado a un servidor;

30 el emisor está configurado para notificar información del terminal al servidor usando el dispositivo intermedio, donde la información del terminal se usa para permitir que el servidor cree una cuenta para el terminal y asocie la cuenta con los datos de tarjeta virtual; y acceda al servidor utilizando la cuenta; y

el receptor está configurado para: después de que el emisor acceda al servidor usando la cuenta, descargar los datos de tarjeta virtual asociados con la cuenta.

35 En una primera posible forma de implementación del octavo aspecto, el procesador está configurado además para realizar negociación de cifrado con una clave pública del servidor almacenada en el dispositivo intermedio y obtener una clave de negociación, donde la clave de negociación se usa para habilitar el servidor o el dispositivo intermedio para cifrar la cuenta y los datos de tarjeta virtual mediante el uso de la clave de negociación; descifrar la cuenta del terminal usando la clave de negociación; y descifrar, utilizando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta;

40 el emisor está específicamente configurado para: después de que el procesador descifre la cuenta del terminal usando la clave de negociación, acceder al servidor usando la cuenta; y

el receptor está específicamente configurado para: después de que el procesador descifre, utilizando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta, descargar los datos de tarjeta virtual asociados con la cuenta.

45 Según un noveno aspecto, la presente invención da a conocer un dispositivo intermedio, donde el dispositivo intermedio incluye: un procesador, un emisor y un receptor, el procesador está conectado al emisor y el procesador está conectado al receptor, donde

el procesador está configurado para establecer una conexión de comunicación con un terminal y conectarse a un servidor;

50 el emisor está configurado para enviar información del terminal al servidor, donde el servidor utiliza la información del terminal para crear una cuenta para el terminal y determinar los datos de tarjeta virtual asociados con la cuenta; y enviar los datos de tarjeta virtual al terminal; y

el receptor está configurado para recibir la información del terminal notificada mediante el terminal, y recibir acceso del terminal.

5 En una primera posible forma de implementación del noveno aspecto, el procesador está configurado además para buscar si los datos de tarjeta virtual están almacenados en almacenamiento del dispositivo intermedio, y si los datos de tarjeta virtual están almacenados en almacenamiento del dispositivo intermedio, extraer los datos de tarjeta virtual del almacenamiento del dispositivo intermedio; y

el receptor está además configurado para: cuando los datos de tarjeta virtual no están almacenados en el almacenamiento del dispositivo intermedio, adquirir los datos de tarjeta virtual del servidor.

10 En una segunda posible forma de implementación del noveno aspecto, el procesador está configurado además para realizar negociación de cifrado con el terminal mediante el uso de una clave pública del servidor almacenada en el dispositivo intermedio, obtener una clave de negociación y cifrar la cuenta y los datos de tarjeta virtual mediante utilizando la clave de negociación.

De acuerdo con un décimo aspecto, la presente invención da a conocer un terminal, donde el terminal incluye: una memoria, donde la memoria está configurada para almacenar datos de tarjeta virtual preestablecidos.

15 En una primera posible forma de implementación del décimo aspecto, el terminal incluye además: un procesador y un módulo de transmisión de datos; el procesador está conectado a la memoria; y el procesador está conectado al módulo de transmisión de datos, donde antes de que la memoria almacene los datos de tarjeta virtual preestablecidos,

el módulo de transmisión de datos está configurado para establecer una conexión física con un primer dispositivo; y

20 el procesador está configurado para: después de que el módulo de transmisión de datos establezca la conexión física con el primer dispositivo, adquirir los datos de tarjeta virtual preestablecidos utilizando el módulo de transmisión de datos.

25 Se puede saber de acuerdo con las soluciones técnicas anteriores que, los efectos beneficiosos existentes en la presente invención son: se preestablece una condición de escenario, de manera que un terminal descarga datos de tarjeta virtual previamente cuando establece una conexión de comunicación con un servidor; o bien un dispositivo intermedio y un terminal se conectan mediante comunicación de campo cercano, de forma que el dispositivo intermedio se conecta indirectamente con el terminal y el servidor, y por tanto el terminal puede descargar los datos de tarjeta virtual sin internet, lo que evita un caso especial en el que si ocurre que un terminal no está conectado a internet cuando un usuario tiene la necesidad urgente de utilizar un servicio de tarjeta virtual, la aplicación del servicio de tarjeta virtual se ve impedida.

30 **Breve descripción de los dibujos**

35 Para describir más claramente las soluciones técnicas en las realizaciones de la presente invención o en la técnica anterior, a continuación se describen brevemente los dibujos adjuntos necesarios para describir las realizaciones o la técnica anterior. Evidentemente, los dibujos adjuntos en la siguiente descripción muestran meramente algunas realizaciones de la presente invención, y una persona con experiencia ordinaria en la técnica puede obtener otros dibujos a partir de estos dibujos adjuntos sin esfuerzos creativos.

la figura 1 y la figura 2 son diagramas de flujo de métodos según una realización de la presente invención;

la figura 3 es un diagrama estructural esquemático de un terminal según una realización de la presente invención;

la figura 4 y la figura 5 son diagramas de flujo de métodos según otra realización de la presente invención;

la figura 6 y la figura 7 son diagramas de flujo de métodos según otra realización más de la presente invención;

40 la figura 8 es un diagrama estructural esquemático de un terminal según una realización de la presente invención;

la figura 9 es un diagrama estructural esquemático de un dispositivo intermedio según una realización de la presente invención;

la figura 10 es un diagrama estructural esquemático de un terminal según una realización de la presente invención;

45 la figura 11 y la figura 12 son diagramas estructurales esquemáticos de un terminal y un dispositivo intermedio según una realización de la presente invención; y

la figura 13 es un diagrama estructural esquemático de un terminal según una realización de la presente invención.

Descripción de realizaciones

Las siguientes realizaciones que se relacionan con las figuras 1, 2, 3, 10 y 13 no son según la invención y se presentan únicamente con fines ilustrativos. Para permitir que un experto en la materia comprenda mejor las soluciones en las

realizaciones de la presente invención, a continuación se describen las realizaciones de la presente invención con más detalle haciendo referencia a los dibujos adjuntos y formas de implementación.

5 En la etapa actual, un terminal generalmente depende de internet, especialmente de internet móvil, para descargar datos de tarjeta virtual (es decir, VSIM) desde un servidor. Si el terminal siempre se mantiene conectado a internet, el terminal puede descargar los datos de tarjeta virtual en cualquier momento cuando necesite comenzar a utilizar un servicio de tarjeta virtual, lo cual es muy cómodo y eficiente. Sin embargo, la forma en que el terminal depende tan solo de internet para descargar datos de tarjeta virtual tiene limitaciones obvias. Por ejemplo, cuando el terminal se encuentra en un escenario especial, tal como itinerando, atravesando áreas de servicio, o similar, el terminal no puede mantenerse conectado a internet o es inoportuno que el terminal se mantenga conectado a internet, y entonces, el terminal no puede comenzar a usar el servicio de tarjeta virtual.

Además, en muchos casos, el usuario tiene una necesidad urgente de usar el servicio de tarjeta virtual en un escenario especial tal como itinerando, atravesando áreas de servicio o similares. Puede verse que la forma en que el terminal depende tan solo de internet para descargar los datos de tarjeta virtual tiene deficiencias relativamente serias, lo que también es un problema para resolver en la presente invención.

15 Haciendo referencia a la figura 1, la figura 1 es una realización específica de un método descrito en la presente invención. Esta realización describe un proceso de descarga de datos de tarjeta virtual en el lado de un terminal, y el método incluye específicamente las siguientes etapas:

20 Etapa 101: el terminal preestablece una condición de escenario y notifica información del terminal a un servidor cuando se cumple la condición de escenario preestablecida, donde la información del terminal se usa para permitir que el servidor cree una cuenta para el terminal y para asociar la cuenta con los datos de tarjeta virtual.

Para evitar un caso especial en el que si el terminal no está conectado a internet cuando un usuario tiene una necesidad urgente de usar un servicio de tarjeta virtual, la aplicación del servicio de tarjeta virtual se ve impedida, en esta realización, la condición de escenario está preestablecida para el terminal, de modo que el terminal activa automáticamente un proceso de descarga de datos de tarjeta virtual en la condición de escenario.

25 En esta realización, la condición de escenario es que el terminal establezca una conexión de comunicación con el servidor. Es decir, el terminal activa automáticamente la descarga de los datos de tarjeta virtual cuando la condición de la red es buena y obtiene los datos de tarjeta virtual por adelantado. De esta forma, el terminal puede empezar directamente a utilizar el servicio de tarjeta virtual cuando lo necesita.

30 Cabe señalar además que la conexión de comunicación anterior entre el terminal y el servidor no se limita simplemente a la conexión a internet. Todas las conexiones de comunicación que pueden implementar la descarga de los datos de tarjeta virtual se encuentran dentro de las soluciones generales de esta realización, y no se necesita ninguna limitación específica en este documento.

35 Después de que se activa el proceso de descarga de datos de tarjeta virtual, el terminal primero notifica la información del terminal al servidor. La información del terminal puede incluir información que indica una identidad del terminal, tal como una IMEI (International Mobile Equipment Identity, es decir, identidad internacional de equipo móvil), un número de secuencia de la CPU y una dirección MAC (Media Access Control, control de acceso al medio) del terminal. Después de recibir la información del terminal, el servidor crea una cuenta para el terminal de acuerdo con la información del terminal, donde la cuenta corresponde de forma fija al terminal. Mientras tanto, el servidor adquiere los datos de tarjeta virtual que un operador proporciona al terminal y asocia los datos de tarjeta virtual con la cuenta, de modo que el terminal descarga los datos de tarjeta virtual posteriormente. La asociación de los datos de tarjeta virtual con la cuenta significa que los datos de tarjeta virtual se pueden invocar directamente mediante el uso de la cuenta, y cuando el terminal accede a la cuenta, el terminal puede descargar, directamente de la cuenta, los datos de tarjeta virtual que necesita el terminal.

Etapa 102: el terminal accede al servidor usando la cuenta y descarga los datos de tarjeta virtual asociados con la cuenta.

45 Después de que el servidor crea la cuenta correspondiente para el terminal y asocia la cuenta con los datos de tarjeta virtual, cuando el terminal accede al servidor utilizando la cuenta, el servidor puede verificar la información del terminal incluida en el terminal (consultar la IMEI, el número de secuencia de la CPU, la dirección MAC y similares del terminal), y a continuación recibe acceso al terminal. A continuación, el terminal descarga, mediante la conexión de comunicación, los datos de tarjeta virtual asociados con la cuenta del terminal.

50 Se puede saber de acuerdo con la solución técnica anterior que, los efectos beneficiosos existentes en esta realización son: se preestablece una condición de escenario, de modo que un terminal descarga datos de tarjeta virtual previamente cuando establece una conexión de comunicación con un servidor, evitando así un caso especial en el que si un terminal no está conectado a internet cuando un usuario tiene una necesidad urgente de utilizar un servicio de tarjeta virtual, la aplicación del servicio de tarjeta virtual se ve impedida.

55 En una realización de la presente invención, el servidor puede ser un servidor de operador, y que el terminal descargue, en la condición de escenario preestablecida, los datos de tarjeta virtual asociados con la cuenta, pueden ser

específicamente que: el terminal descarga, en un escenario preestablecido, los datos de tarjeta virtual utilizando un canal de transmisión de datos del servidor del operador. Por ejemplo, el servidor del operador aprende la información de la cuenta de una tarjeta de circuito integrado universal (Universal Integrated Circuit Card, UICC) del terminal, y el servidor del operador puede enviar los datos de tarjeta virtual o un enlace de adquisición de los datos de tarjeta virtual a modo de un mensaje del servicio de mensajes cortos o un mensaje multimedia. En la condición de escenario preestablecida, es decir, cuando el terminal puede establecer una conexión de comunicación con el servidor del operador, el terminal recibe el mensaje del servicio de mensajes cortos o el mensaje multimedia enviado por el servidor del operador, y descarga los datos de tarjeta virtual por adelantado utilizando un canal de transmisión de datos entre el terminal y el servidor del operador, de modo que el terminal puede invocar los datos de tarjeta virtual cuando el terminal no pueda conectarse al servidor pero tenga una necesidad urgente de utilizar el servicio de tarjeta virtual.

Haciendo referencia a la figura 2, la figura 2 es otra realización específica de un método descrito en la presente invención. En base a la realización mostrada en la figura 1, en esta realización se añade una solución técnica de negociación de cifrado. El método en esta realización incluye las siguientes etapas:

Etapa 201: un terminal preestablece una condición de escenario y notifica la información del terminal a un servidor cuando se cumple la condición de escenario preestablecida, donde la información del terminal se usa para permitir que el servidor cree una cuenta para el terminal y para asociar la cuenta con los datos de tarjeta virtual.

La condición de escenario es que el terminal establezca una conexión de comunicación con el servidor.

Etapa 202: el terminal realiza una negociación de cifrado con el servidor y obtiene una clave de negociación, donde la clave de negociación se usa para permitir que el servidor cifre la cuenta y los datos de tarjeta virtual usando la clave de negociación.

En esta realización, después de crear la cuenta y asociar los datos de tarjeta virtual con la cuenta, para garantizar la seguridad de la cuenta y los datos de tarjeta virtual, se añade la solución técnica de negociación de cifrado. La negociación de cifrado es específicamente negociación de DH (protocolo/algoritmo de intercambio de claves (Diffie-Hellman)). La negociación de DH es una tecnología de cifrado existente, y el principio de la negociación de DH se puede resumir brevemente como: dos partes negocian utilizando el algoritmo DH y obtienen una clave de negociación simétrica, y a continuación realizan el cifrado y descifrado utilizando la clave de negociación. Después de que el terminal realiza la negociación de DH con el servidor, se obtiene la clave de negociación. En esta realización, la clave de negociación incluye dos pares de claves, es decir, una clave pública del servidor y una clave privada del servidor, y una clave pública del terminal y una clave privada del terminal. De acuerdo con el principio de la negociación de DH, en esta etapa, el servidor cifra, utilizando la clave pública de servidor, la clave privada del servidor y la clave pública del terminal de los dos pares de claves, la cuenta y los datos de tarjeta virtual asociados con la cuenta.

Etapa 203: el terminal descifra la cuenta del terminal utilizando la clave de negociación y accede al servidor utilizando la cuenta; y el terminal descifra, usando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta, y descarga los datos de tarjeta virtual.

Debido a que la cuenta y los datos de tarjeta virtual ya están cifrados, el terminal puede acceder a la cuenta y descargar los datos de tarjeta virtual solo después de realizar el descifrado. De acuerdo con el principio de la negociación de DH, en esta etapa, el terminal descifra la cuenta y los datos de tarjeta virtual utilizando la clave pública del terminal, la clave privada del terminal y la clave pública de servidor. Cabe señalar que tanto la cuenta como los datos de tarjeta virtual se cifran mediante el uso de la clave de negociación, es decir, el terminal primero tiene que descifrar la cuenta antes de realizar el acceso y la descarga de datos de tarjeta virtual, y además tiene que descifrar los datos de tarjeta virtual antes de implementar un servicio relacionado con la tarjeta virtual utilizando los datos de tarjeta virtual.

Se puede saber de acuerdo con la solución técnica anterior que, los efectos beneficiosos existentes en esta realización son: la solución técnica de negociación de cifrado se añade al método, de modo que se garantiza la seguridad de una cuenta y los datos de tarjeta virtual de un terminal.

Haciendo referencia a la figura 3, la figura 3 es una realización específica de un terminal descrito en la presente invención. En esta realización, el terminal es un dispositivo que descarga datos de tarjeta virtual de acuerdo con los métodos que se muestran en la figura 1 y la figura 2. El terminal incluye:

un primer módulo de notificación 301, configurado para preestablecer una condición de escenario y notificar la información del terminal a un servidor cuando se cumple la condición de escenario preestablecida, donde la información del terminal se usa para permitir que el servidor cree una cuenta para el terminal y para asociar la cuenta con datos de tarjeta virtual, y la condición de escenario es que el terminal establezca una conexión de comunicación con el servidor;

un primer módulo de descarga 302, configurado para acceder al servidor usando la cuenta, y descargar los datos de tarjeta virtual asociados con la cuenta;

un primer módulo de negociación 303, configurado para realizar negociación de cifrado con el servidor y obtener una clave de negociación, donde la clave de negociación se usa para permitir que el servidor cifre la cuenta y los

datos de tarjeta virtual usando la clave de negociación; y

un primer módulo de descifrado 304, configurado para descifrar la cuenta del terminal utilizando la clave de negociación, y descifrar, utilizando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta.

5 Se puede saber de acuerdo con la solución técnica anterior que, los efectos beneficiosos que existen en el terminal en esta realización son: se preestablece una condición de escenario, para que el terminal descargue los datos de tarjeta virtual previamente cuando establece una conexión de comunicación con un servidor, evitando así un caso especial en el que si un terminal no está conectado a internet cuando un usuario necesita urgentemente utilizar un servicio de tarjeta virtual, la aplicación del servicio de tarjeta virtual se ve impedida; la seguridad de una cuenta y los datos de tarjeta virtual de un terminal se garantizan mediante el uso de la solución técnica de negociación de cifrado.

10 Las tres realizaciones mostradas en la figura 1 a la figura 3 describen un método para resolver el problema en la técnica anterior utilizando una condición de escenario y un terminal correspondiente. Además, las realizaciones de la presente invención dan a conocer también soluciones técnicas para resolver problemas técnicos relacionados, mediante el uso de un dispositivo intermedio entre un terminal y un servidor, y las soluciones técnicas se describen específicamente en las siguientes realizaciones.

15 Haciendo referencia a la figura 4, la figura 4 es otra realización específica de un método de descarga de tarjeta virtual según una realización de la presente invención. Esta realización describe un proceso de descarga de datos de tarjeta virtual en el lado de un terminal, y el método incluye específicamente las siguientes etapas:

Etapa 401: un terminal establece una conexión de comunicación con un dispositivo intermedio conectado a un servidor.

20 En esta realización, cuando no hay una red de comunicaciones para que el terminal se conecte directamente al servidor, el terminal se puede conectar indirectamente y comunicarse con el servidor utilizando el dispositivo intermedio. El terminal y el dispositivo intermedio están conectados en modo comunicación de campo cercano (como Bluetooth o wifi).

25 El dispositivo intermedio puede considerarse como una extensión para el despliegue del servidor y, naturalmente, tiene una relación de conexión con el servidor. Cada dispositivo intermedio cubre un rango particular (un rango en el que se puede conseguir comunicación de campo cercano) desde la perspectiva de la comunicación. Si un terminal que no está conectado a una red necesita descargar datos de tarjeta virtual y usar un servicio de tarjeta virtual, el terminal tiene que estar situado dentro del rango de cobertura del dispositivo intermedio, y se conecta al dispositivo intermedio por medio de comunicación de campo cercano que no se ve afectada por una red, lo que equivale a que se puede implementar la comunicación con el servidor. Por lo tanto, se resuelve el problema de que el terminal no puede descargar los datos de tarjeta virtual cuando no está conectado a una red.

30 Etapa 402: el terminal notifica información del terminal al servidor utilizando el dispositivo intermedio, donde la información del terminal se utiliza para permitir que el servidor cree una cuenta para el terminal y asocie la cuenta con los datos de tarjeta virtual.

35 Etapa 403: el terminal accede al dispositivo intermedio utilizando la cuenta y descarga los datos de tarjeta virtual asociados con la cuenta.

40 En esta realización, el terminal se comunica directamente con el dispositivo intermedio, pero un dispositivo que crea específicamente la cuenta para el terminal y proporciona los datos de tarjeta virtual sigue siendo el servidor. Por lo tanto, tanto la notificación de la información del terminal como la descarga de los datos de tarjeta virtual tienen que transferirse entre el terminal y el servidor utilizando el dispositivo intermedio. Excepto por esto, otras características técnicas de esta realización son todas consistentes con las de la realización mostrada en la figura 1.

Haciendo referencia a la figura 5, la figura 5 es una realización específica de un método descrito en la presente invención. En correspondencia con la realización mostrada en la figura 4, esta realización describe el proceso de descarga desde la perspectiva de un dispositivo intermedio. El método en esta realización, es específicamente:

45 Etapa 501: un dispositivo intermedio establece una conexión de comunicación con un terminal y el dispositivo intermedio se conecta con un servidor.

50 Se puede considerar aproximadamente que el dispositivo intermedio es equivalente a un punto de acceso de comunicación ampliamente desplegado por el servidor, y dentro de la cobertura de comunicación del dispositivo intermedio, el terminal normalmente puede descargar datos de tarjeta virtual y usar un servicio de tarjeta virtual sin estar conectado a internet. Cuando el servidor implementa una gran cantidad de dispositivos intermedios y mejora continuamente la tasa de cobertura del dispositivo intermedio, el terminal puede descargar los datos de tarjeta virtual en cualquier lugar y en cualquier momento.

Etapa 502: el dispositivo intermedio recibe información del terminal notificada mediante el terminal, y el dispositivo intermedio envía la información del terminal al servidor, donde el servidor utiliza la información del terminal para crear una cuenta para el terminal y determinar los datos de tarjeta virtual asociados con la cuenta.

Etapa 503: el dispositivo intermedio recibe acceso del terminal y envía los datos de tarjeta virtual al terminal.

5 Se puede conocer según las soluciones técnicas mostradas en la figura 4 y la figura 5 que, los efectos beneficiosos existentes en las realizaciones son: un dispositivo intermedio y un terminal están conectados por medio de comunicación de campo cercano, de modo que el dispositivo intermedio se conecta indirectamente con el terminal y el servidor, y por lo tanto el terminal puede descargar los datos de tarjeta virtual sin internet, evitando así un caso especial en el que si un terminal no está conectado a internet cuando un usuario necesita urgentemente utilizar un servicio de tarjeta virtual, la aplicación del servicio de tarjeta virtual se ve impedida.

10 Las realizaciones mostradas en la figura 4 y la figura 5 son realizaciones de tecnologías de descarga de datos de tarjeta virtual utilizando el dispositivo intermedio. Para mejorar la seguridad de las soluciones técnicas, de forma similar, se puede añadir una solución de optimización de la negociación de cifrado sobre la base de las soluciones técnicas. Específicamente:

haciendo referencia a la figura 6, la figura 6 es otra realización específica de un método de descarga de tarjeta virtual según la presente invención. El método en esta realización incluye:

Etapa 601: un terminal establece una conexión de comunicación con un dispositivo intermedio conectado a un servidor.

15 Etapa 602: el terminal notifica información del terminal al servidor utilizando el dispositivo intermedio, donde la información del terminal se utiliza para permitir que el servidor cree una cuenta para el terminal y asocie la cuenta con los datos de tarjeta virtual.

20 Etapa 603: el terminal realiza una negociación de cifrado con una clave pública del servidor almacenada en el dispositivo intermedio y obtiene una clave de negociación, donde la clave de negociación se usa para permitir que el servidor o el dispositivo intermedio cifre la cuenta y los datos de tarjeta virtual usando la clave de negociación.

En esta realización, la negociación de cifrado es también negociación de DH. Específicamente, el terminal realiza negociación de DH con la clave pública de servidor, pero en esta realización, el terminal ya no está directamente conectado al servidor; por lo tanto, el dispositivo intermedio almacena la clave pública de servidor y reemplaza al servidor para realizar la negociación de DH con el terminal.

25 La negociación de DH es una tecnología de cifrado existente y se ha descrito en las realizaciones anteriores, y el principio de la negociación de DH no se describe de nuevo aquí. Después de que el terminal realiza la negociación de DH con la clave pública de servidor, el terminal obtiene la clave de negociación, y tanto el dispositivo intermedio como el servidor deberán conservar la clave de negociación. En esta realización, la clave de negociación incluye dos pares de claves, es decir, una clave pública del servidor y una clave privada del servidor, y una clave pública del terminal y una clave privada del terminal. De acuerdo con el principio de la negociación de DH, en esta etapa, el dispositivo intermedio cifra, utilizando la clave pública de servidor, la clave privada del servidor y la clave pública del terminal de los dos pares de claves, la cuenta y los datos de tarjeta virtual asociados con la cuenta.

30 Etapa 604: el terminal descifra la cuenta del terminal usando la clave de negociación y accede al dispositivo intermedio usando la cuenta; y el terminal descifra, usando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta, y descarga los datos de tarjeta virtual.

Dado que la cuenta y los datos de tarjeta virtual ya están cifrados, el terminal puede acceder a la cuenta y descargar los datos de tarjeta virtual solo después de realizar el descifrado. De acuerdo con el principio de la negociación de DH, en esta etapa, el terminal descifra la cuenta y los datos de tarjeta virtual utilizando la clave pública del terminal, la clave privada del terminal y la clave pública de servidor.

40 Haciendo referencia a la figura 7, la figura 7 es otra realización específica más, de un método descrito en la presente invención. En correspondencia con la realización mostrada en la figura 6, esta realización describe el proceso de descarga desde la perspectiva de un dispositivo intermedio. El método en esta realización, es específicamente:

Etapa 701: un dispositivo intermedio establece una conexión de comunicación con un terminal, y el dispositivo intermedio se conecta a un servidor y almacena una clave pública del servidor.

45 Etapa 702: el dispositivo intermedio recibe la información del terminal notificada mediante el terminal, y el dispositivo intermedio envía la información del terminal al servidor, donde el servidor utiliza la información del terminal para crear una cuenta para el terminal y determinar los datos de tarjeta virtual asociados con la cuenta.

50 Etapa 703: el dispositivo intermedio realiza negociación de cifrado con el terminal usando la clave pública de servidor almacenada en el dispositivo intermedio, obtiene una clave de negociación y cifra la cuenta y los datos de tarjeta virtual usando la clave de negociación.

Generalmente, después de que el dispositivo intermedio reemplace al servidor para realizar negociación de cifrado con el terminal, el propio dispositivo intermedio debe mantener la clave de negociación, pero es posible que la clave de negociación solo se mantenga en el servidor, pero no se almacene en el dispositivo intermedio. Por lo tanto, en un proceso de cifrado, el dispositivo intermedio busca si la clave de negociación está almacenada en almacenamiento

del dispositivo intermedio, y si la clave de negociación está almacenada en el almacenamiento del dispositivo intermedio, el dispositivo intermedio realiza el cifrado utilizando la clave de negociación almacenada en el almacenamiento del dispositivo intermedio; de lo contrario, el dispositivo intermedio adquiere la clave de negociación del servidor y realiza el cifrado.

5 Etapa 704: el dispositivo intermedio recibe acceso del terminal, busca si los datos de tarjeta virtual están almacenados en almacenamiento del dispositivo intermedio, y si los datos de tarjeta virtual están almacenados en el almacenamiento del dispositivo intermedio, extrae los datos de tarjeta virtual del almacenamiento del dispositivo intermedio y envía los datos de tarjeta virtual; de lo contrario, el dispositivo intermedio adquiere los datos de tarjeta virtual del servidor y envía los datos de tarjeta virtual al terminal.

10 El terminal completa un proceso de descifrado correspondiente, accede al dispositivo intermedio y solicita la descarga de los datos de tarjeta virtual. En este caso, el dispositivo intermedio primero necesita buscar si los datos de tarjeta virtual que el terminal necesita descargar están almacenados en el dispositivo intermedio, y si los datos de tarjeta virtual están almacenados en el dispositivo intermedio, el dispositivo intermedio proporciona directamente la descarga; si los datos de tarjeta virtual están almacenados en el dispositivo intermedio, el dispositivo intermedio primero necesita adquirir los datos de tarjeta virtual del servidor y a continuación proporciona la descarga.

Se puede saber de acuerdo con las soluciones técnicas anteriores que, los efectos beneficiosos existentes en las realizaciones mostradas en la figura 6 y la figura 7 son: la solución técnica de negociación de cifrado se añade al método, de modo que se garantiza la seguridad de una cuenta y los datos de tarjeta virtual de un terminal.

20 En correspondencia con las realizaciones mostradas en la figura 4 a la figura 7, un terminal y un dispositivo intermedio se dan a conocer correspondientemente a continuación. El terminal y el dispositivo intermedio están configurados para implementar los métodos mostrados en la figura 4 a la figura 7. Específicamente:

Haciendo referencia a la figura 8, el terminal incluye:

un módulo de comunicaciones 801, configurado para establecer una conexión de comunicación con un dispositivo intermedio conectado a un servidor;

25 un segundo módulo de notificación 802, configurado para notificar información del terminal al servidor usando el dispositivo intermedio, donde la información del terminal se utiliza para permitir que el servidor cree una cuenta para el terminal y asocie la cuenta con los datos de tarjeta virtual;

un segundo módulo de descarga 803, configurado para acceder al dispositivo intermedio usando la cuenta, y descargar los datos de tarjeta virtual asociados con la cuenta;

30 un segundo módulo de negociación 804, configurado para realizar negociación de cifrado con una clave pública del servidor almacenada en el dispositivo intermedio, y obtener una clave de negociación, donde la clave de negociación se usa para permitir que el servidor o el dispositivo intermedio cifren la cuenta y los datos de tarjeta virtual utilizando la clave de negociación; y

35 un segundo módulo de descifrado 805, configurado para descifrar la cuenta del terminal usando la clave de negociación, y descifrar, usando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta.

Haciendo referencia a la figura 9, el dispositivo intermedio incluye:

un módulo de conexión 901, configurado para establecer una conexión de comunicación con un terminal y conectarse a un servidor;

40 un módulo de notificación 902, configurado para recibir información del terminal notificada mediante el terminal, y enviar la información del terminal al servidor, donde el servidor utiliza la información del terminal para crear una cuenta para el terminal y determinar los datos de tarjeta virtual asociados con la cuenta; y

un módulo de intercambio 903, configurado para recibir el acceso del terminal, y enviar los datos de tarjeta virtual al terminal.

El módulo de intercambio incluye:

45 una unidad de consulta 931, configurada para buscar si los datos de tarjeta virtual están almacenados en un módulo de almacenamiento;

una unidad de almacenamiento 932, configurada para almacenar los datos de tarjeta virtual y enviar los datos de tarjeta virtual al terminal; y

50 una unidad de adquisición 933, configurada para: cuando los datos de tarjeta virtual no están almacenados en el módulo de almacenamiento, adquirir los datos de tarjeta virtual del servidor y almacenar los datos de tarjeta virtual en la unidad de almacenamiento.

Un módulo de cifrado 904 está configurado para realizar negociación de cifrado con el terminal usando una clave pública del servidor almacenada en el dispositivo intermedio, obtener una clave de negociación y cifrar la cuenta y los datos de tarjeta virtual usando la clave de negociación.

5 Los efectos beneficiosos existentes en las realizaciones mostradas en la figura 8 y la figura 9 son: un dispositivo intermedio y un terminal se conectan mediante comunicación de campo cercano, de manera que el dispositivo intermedio se conecta indirectamente con el terminal y el servidor, y por lo tanto el terminal puede descargar los datos de tarjeta virtual sin internet, evitando así un caso especial en el que si un terminal no está conectado a internet cuando un usuario tiene la necesidad urgente de utilizar un servicio de tarjeta virtual, la aplicación del servicio de tarjeta virtual se ve impedida; se añade al método la solución técnica de negociación de cifrado, y se garantiza la seguridad de una
10 cuenta y los datos de tarjeta virtual de un terminal.

En una realización de la presente invención, el terminal puede preestablecer datos de tarjeta virtual interactuando con un servidor. Haciendo referencia a la figura 10, el terminal en esta realización, es específicamente como sigue:

15 el terminal incluye: un procesador 1001, un emisor 1002, un receptor 1003 y una memoria 1004 (que no se muestra en la figura), el procesador 1001 está conectado al emisor 1002 y el procesador 1001 está conectado al receptor 1003, dónde

el procesador 1001 está configurado para preestablecer una condición de escenario, donde la condición de escenario es que el terminal establezca una conexión de comunicación con un servidor;

20 el emisor 1002 está configurado para: cuando se cumple la condición de escenario preestablecida, notificar la información del terminal al servidor, donde la información del terminal se usa para permitir que el servidor cree una cuenta para el terminal y asocie la cuenta con los datos de tarjeta virtual; y acceda al servidor utilizando la cuenta; y

el receptor 1003 está configurado para: después de que el emisor 1002 acceda al servidor usando la cuenta, descargar los datos de tarjeta virtual asociados con la cuenta.

25 El procesador 1001 está configurado además para realizar negociación de cifrado con el servidor y obtener una clave de negociación, donde la clave de negociación se usa para permitir que el servidor cifre la cuenta y los datos de tarjeta virtual usando la clave de negociación; descifrar la cuenta del terminal usando la clave de negociación; y descifrar, utilizando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta;

el emisor 1002 está específicamente configurado para: después de que el procesador 1001 descifre la cuenta del terminal usando la clave de negociación, acceder al servidor usando la cuenta; y

30 el receptor 1003 está específicamente configurado para: después de que el procesador 1001 descifre, usando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta, descargar los datos de tarjeta virtual asociados con la cuenta.

La memoria 1004 está configurada para almacenar la información del terminal, los datos de tarjeta virtual y la clave de negociación.

35 En una realización de la presente invención, el terminal puede preestablecer datos de tarjeta virtual interactuando indirectamente, usando un dispositivo intermedio, con un servidor. Haciendo referencia a la figura 11 y la figura 12, el terminal y el dispositivo intermedio en esta realización son específicamente como sigue:

40 Haciendo referencia a la figura 11, el terminal incluye: un procesador 1101, un emisor 1102, un receptor 1103 y una memoria 1104 (que no se muestra en la figura), el procesador 1101 está conectado al emisor 1102 y el procesador 1101 está conectado al receptor 1103, donde

el procesador está configurado para establecer una conexión de comunicación con un dispositivo intermedio conectado a un servidor;

45 el emisor está configurado para notificar información del terminal al servidor usando el dispositivo intermedio, donde la información del terminal se usa para permitir que el servidor cree una cuenta para el terminal y asocie la cuenta con los datos de tarjeta virtual; y acceda al servidor utilizando la cuenta; y

el receptor está configurado para: después de que el emisor acceda al servidor usando la cuenta, descargar los datos de tarjeta virtual asociados con la cuenta.

50 El procesador está configurado además para realizar negociación de cifrado con una clave pública del servidor almacenada en el dispositivo intermedio y obtener una clave de negociación, donde la clave de negociación se usa para permitir que el servidor o el dispositivo intermedio cifren la cuenta y los datos de tarjeta virtual mediante utilizando la clave de negociación; descifrar la cuenta del terminal usando la clave de negociación; y descifrar, utilizando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta;

el emisor está específicamente configurado para: después de que el procesador descifre la cuenta del terminal usando la clave de negociación, acceder al servidor usando la cuenta; y

5 el receptor está específicamente configurado para: después de que el procesador descifre, utilizando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta, descargar los datos de tarjeta virtual asociados con la cuenta.

La memoria está configurada para almacenar la información del terminal, los datos de tarjeta virtual y la clave de negociación.

Haciendo referencia a la figura 12, el dispositivo intermedio incluye: un procesador, un emisor, un receptor y una memoria, el procesador está conectado al emisor, y el procesador está conectado al receptor, donde

10 el procesador está configurado para establecer una conexión de comunicación con un terminal y conectarse a un servidor;

el emisor está configurado para enviar información del terminal al servidor, donde el servidor utiliza la información del terminal para crear una cuenta para el terminal y determinar los datos de tarjeta virtual asociados con la cuenta; y enviar los datos de tarjeta virtual al terminal; y

15 el receptor está configurado para recibir la información del terminal notificada mediante el terminal, y recibir acceso del terminal.

El procesador está además configurado para buscar si los datos de tarjeta virtual están almacenados en almacenamiento del dispositivo intermedio y, si los datos de tarjeta virtual están almacenados en el almacenamiento del dispositivo intermedio, extraer los datos de tarjeta virtual del almacenamiento del dispositivo intermedio; y

20 el receptor está además configurado para: cuando los datos de tarjeta virtual no están almacenados en el almacenamiento del dispositivo intermedio, adquirir los datos de tarjeta virtual del servidor.

El procesador está configurado además para realizar negociación de cifrado con el terminal usando una clave pública del servidor almacenada en el dispositivo intermedio, obtener una clave de negociación y cifrar la cuenta y los datos de tarjeta virtual usando la clave de negociación.

25 La memoria está configurada para almacenar la información del terminal, la clave pública de servidor, la clave de negociación y los datos de tarjeta virtual.

En una realización de la presente invención, el terminal almacena por adelantado datos de tarjeta virtual. Haciendo referencia a la figura 13, el terminal incluye:

una memoria, donde la memoria está configurada para almacenar los datos de tarjeta virtual preestablecidos.

30 El terminal incluye además: un procesador y un módulo de transmisión de datos; el procesador está conectado a la memoria; y el procesador está conectado al módulo de transmisión de datos, donde antes de que la memoria almacene los datos de tarjeta virtual preestablecidos,

el módulo de transmisión de datos está configurado para establecer una conexión física con un primer dispositivo; y

35 el procesador está configurado para: después de que el módulo de transmisión de datos establezca la conexión física con el primer dispositivo, adquirir los datos de tarjeta virtual preestablecidos utilizando el módulo de transmisión de datos.

En esta realización, el terminal puede preestablecer los datos de tarjeta virtual localmente en el terminal. Específicamente, como se muestra en la figura 13, el terminal puede incluir una memoria, donde la memoria está configurada para almacenar los datos de tarjeta virtual preestablecidos. Esta realización de la presente invención da a conocer otra manera de preestablecer los datos de tarjeta virtual, donde el terminal puede no necesitar realizar intercambio de datos con un servidor antes de adquirir los datos de tarjeta virtual y, en su lugar, uno o más datos de tarjeta virtual se preestablecen directamente localmente en el terminal, por ejemplo, uno o más elementos de datos de tarjeta virtual se almacenan en una memoria en el momento de la entrega del terminal.

40 Además, en una forma de implementación de esta realización de la presente invención, como se muestra en la figura 45 13, el terminal incluye además: un procesador y un módulo de transmisión de datos; el procesador está conectado a la memoria; y el procesador está conectado al módulo de transmisión de datos, donde antes de que la memoria almacene los datos de tarjeta virtual preestablecidos, el módulo de transmisión de datos está configurado para establecer una conexión física con un primer dispositivo; y el procesador está configurado para: después de que el módulo de transmisión de datos establezca la conexión física con el primer dispositivo, adquirir los datos de tarjeta virtual preestablecidos utilizando el módulo de transmisión de datos. Específicamente, el terminal puede no incluir datos de tarjeta virtual en el momento de la entrega del terminal, o simplemente incluir datos de tarjeta virtual de un tipo fijo. El terminal incluye un módulo de transmisión de datos y el módulo de transmisión de datos está configurado

5 para establecer una conexión física con un primer dispositivo, por ejemplo, el módulo de transmisión de datos puede ser una interfaz USB y el primer dispositivo puede ser un ordenador portátil. Después de conectar la interfaz USB del terminal y el ordenador portátil mediante una línea de datos USB, el procesador adquiere, mediante un canal de transmisión de datos USB entre el terminal y el ordenador portátil, datos de tarjeta virtual almacenados en el ordenador portátil. El terminal adquiere los datos de tarjeta virtual mediante la conexión física.

10 Cabe señalar además que, en todos los dibujos de la memoria descriptiva de la presente invención, un segmento de línea con una flecha significa que una señal fluye a lo largo de la dirección de la flecha, y un segmento de línea con dos flechas en sentidos opuestos significa interacción bidireccional de señales; sin embargo, que exista el segmento de línea anterior no es equivalente a que exista una relación de conexión real entre módulos; en base a las necesidades de descripción de la memoria descriptiva de la presente invención, en los dibujos no se muestra específicamente una conexión física o una conexión de otro tipo entre módulos internos de un terminal.

15 Como se puede saber de las descripciones anteriores de las formas de implementación, un experto en la materia puede comprender claramente que algunas o todas las etapas de los métodos en las realizaciones pueden implementarse mediante software más una plataforma de hardware universal necesaria. Basándose en tal comprensión, las soluciones técnicas de la presente invención esencialmente, o la parte que contribuye a la técnica anterior, pueden implementarse en forma de un producto de software. El producto de software se puede almacenar en un medio de almacenamiento, tal como una ROM/RAM, un disco magnético o un disco óptico, e incluye varias instrucciones para instruir a un dispositivo informático (que puede ser un ordenador personal, un servidor o un dispositivo de comunicación en red, tal como una puerta de enlace de medios) para realizar los métodos descritos en las realizaciones o algunas partes de las realizaciones de la presente invención.

20 Cabe señalar que todas las realizaciones en esta memoria descriptiva, se describen de manera progresiva, para partes iguales o similares en las realizaciones, se puede hacer referencia mutua a estas realizaciones, y cada realización se centra en una diferencia con respecto a otras realizaciones. Especialmente, las realizaciones de dispositivo y de sistema son básicamente similares a una realización de método y, por lo tanto, se describen brevemente; para las partes relacionadas, se hace referencia a las partes de las descripciones en la realización del método. Las realizaciones de dispositivo y sistema descritas son meramente ejemplares. Las unidades descritas como partes separadas pueden o no estar físicamente separadas, y las partes mostradas como unidades pueden o no ser unidades físicas, pueden estar ubicadas en una posición o pueden estar distribuidas en una pluralidad de unidades de red. Algunos o todos los módulos pueden seleccionarse según las necesidades reales para conseguir los objetivos de las soluciones de las realizaciones. Un experto en la materia puede comprender e implementar las realizaciones de la presente invención sin esfuerzos creativos.

25
30 Las descripciones anteriores son simplemente realizaciones ejemplares de la presente invención, pero no pretenden limitar el alcance de protección de la presente invención, tal como se establece en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método de descarga de tarjeta virtual, el método comprende:
- 5 establecer (401), mediante un terminal, una conexión de comunicación de campo cercano a un dispositivo intermedio conectado a un servidor, en el que la conexión de comunicación de campo cercano comprende una conexión Bluetooth o una conexión WiFi, y en el que el terminal no está conectado directamente al servidor a través de una red de comunicaciones;
- 10 notificar (402), mediante el terminal, información del terminal al servidor utilizando el dispositivo intermedio, donde la información del terminal se utiliza para permitir que el servidor cree una cuenta para el terminal, la cuenta está asociada con datos de tarjeta virtual para proporcionar un servicio de tarjeta virtual, los datos de tarjeta virtual son proporcionados al terminal por un operador;
- acceder (403), mediante el terminal, al dispositivo intermedio utilizando la cuenta, y descargar los datos de tarjeta virtual, asociados con la cuenta creada en el servidor, mediante la conexión de comunicación de campo cercano;
- utilizar, mediante el terminal, el servicio de tarjeta virtual invocando los datos de tarjeta virtual.
2. El método según la reivindicación 1, donde el método comprende además:
- 15 realizar, mediante el terminal, negociación de cifrado con una clave pública del servidor almacenada en el dispositivo intermedio, y obtener una clave de negociación, donde la clave de negociación permite al servidor o al dispositivo intermedio cifrar los datos de tarjeta virtual usando la clave de negociación.
3. El método según la reivindicación 2, en el que la descarga de los datos de tarjeta virtual comprende además:
- 20 descifrar, mediante el terminal, la cuenta del terminal utilizando la clave de negociación, y acceder al dispositivo intermedio utilizando la cuenta; y descifrar mediante el terminal usando la clave de negociación, los datos de tarjeta virtual asociados con la cuenta, y descargar los datos de tarjeta virtual.
4. El método según cualquiera de las reivindicaciones 1-3, en el que la información del terminal comprende información que indica una identidad del terminal.
5. El método según cualquiera de las reivindicaciones 1-3, en el que la información del terminal comprende una IMEI, identidad internacional de equipo móvil, un número de secuencia de la CPU o una dirección MAC, control de acceso al medio, del terminal.
- 25 6. El método según una cualquiera de las reivindicaciones 1-5, método que comprende además:
- obtener, mediante el servidor, los datos de tarjeta virtual proporcionados por un operador para el terminal, y asociar los datos de tarjeta virtual a la cuenta.
- 30 7. El método según una cualquiera de las reivindicaciones 1-6, en el que la cuenta corresponde de forma fija al terminal.
8. Un dispositivo terminal, donde el dispositivo terminal comprende una memoria, uno o más procesadores y uno o más programas, en el que el uno o más programas se almacenan en la memoria, y cuando los uno o más procesadores ejecutan los uno o más programas, el dispositivo terminal está adaptado para realizar todas las etapas del método según una cualquiera de las reivindicaciones 1 a 7.
- 35 9. Un medio de almacenamiento legible por ordenador, que comprende instrucciones que, cuando son ejecutadas por un ordenador asociado con un terminal, hacen que el terminal lleve a cabo todas las etapas del método según una cualquiera de las reivindicaciones 1 a 7.

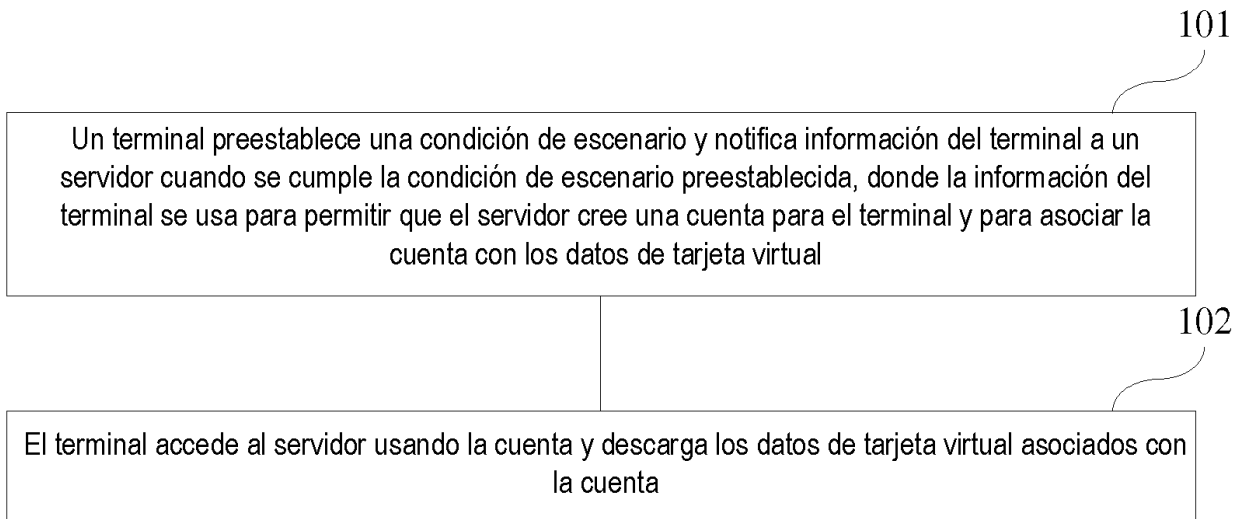


FIG. 1

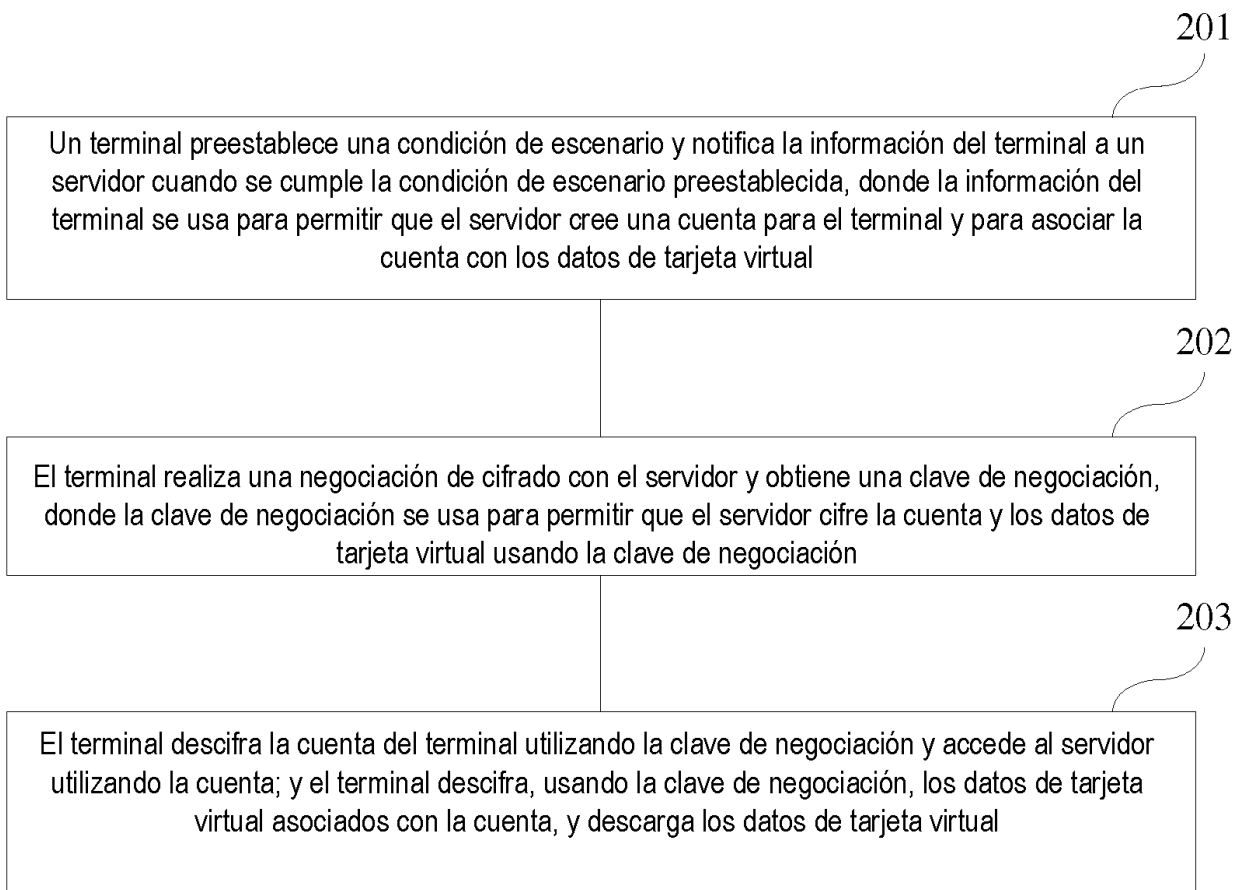


FIG. 2

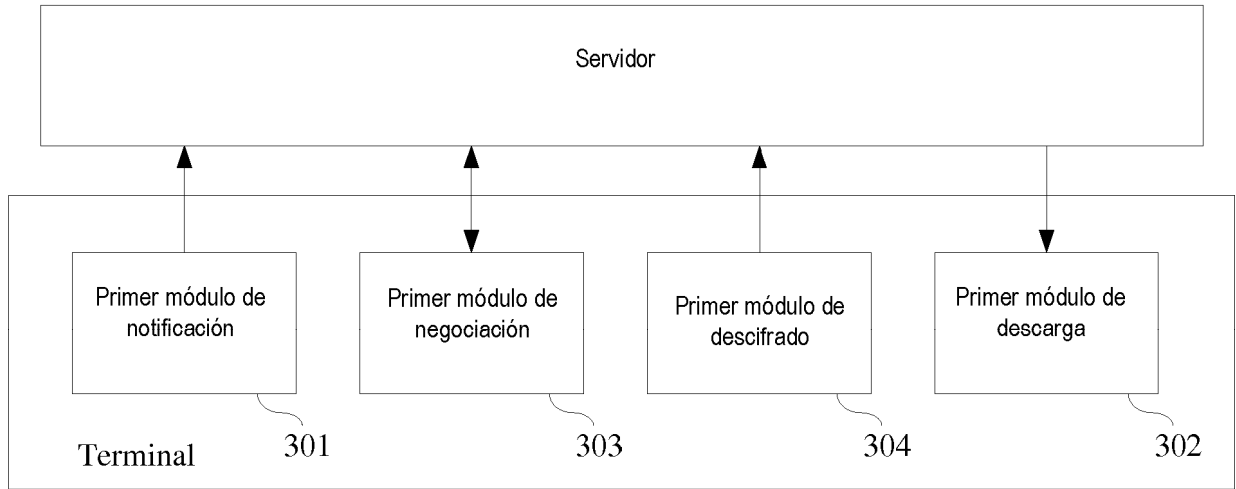


FIG. 3

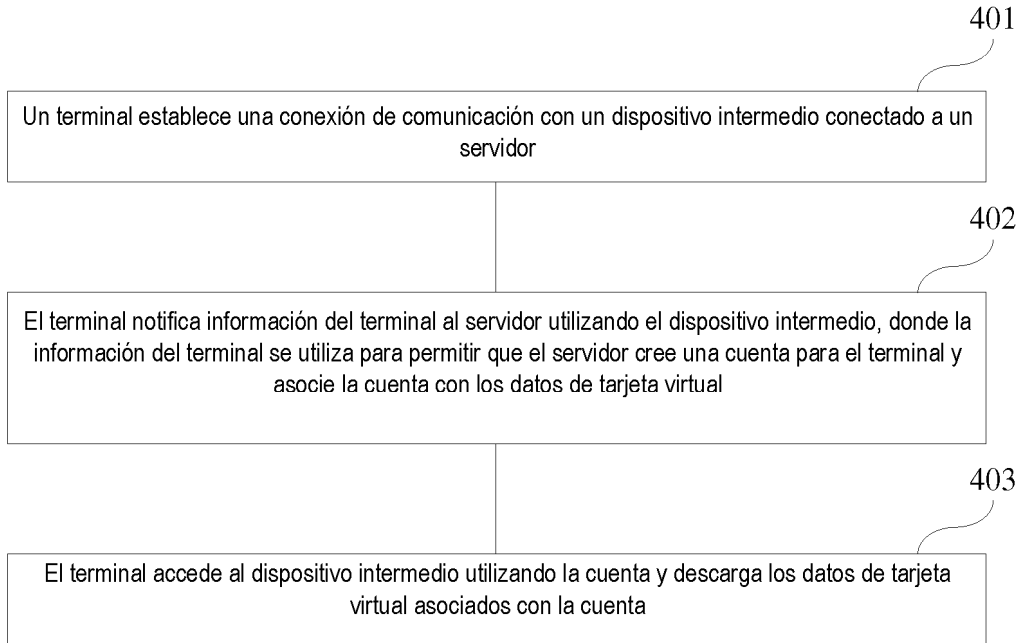


FIG. 4

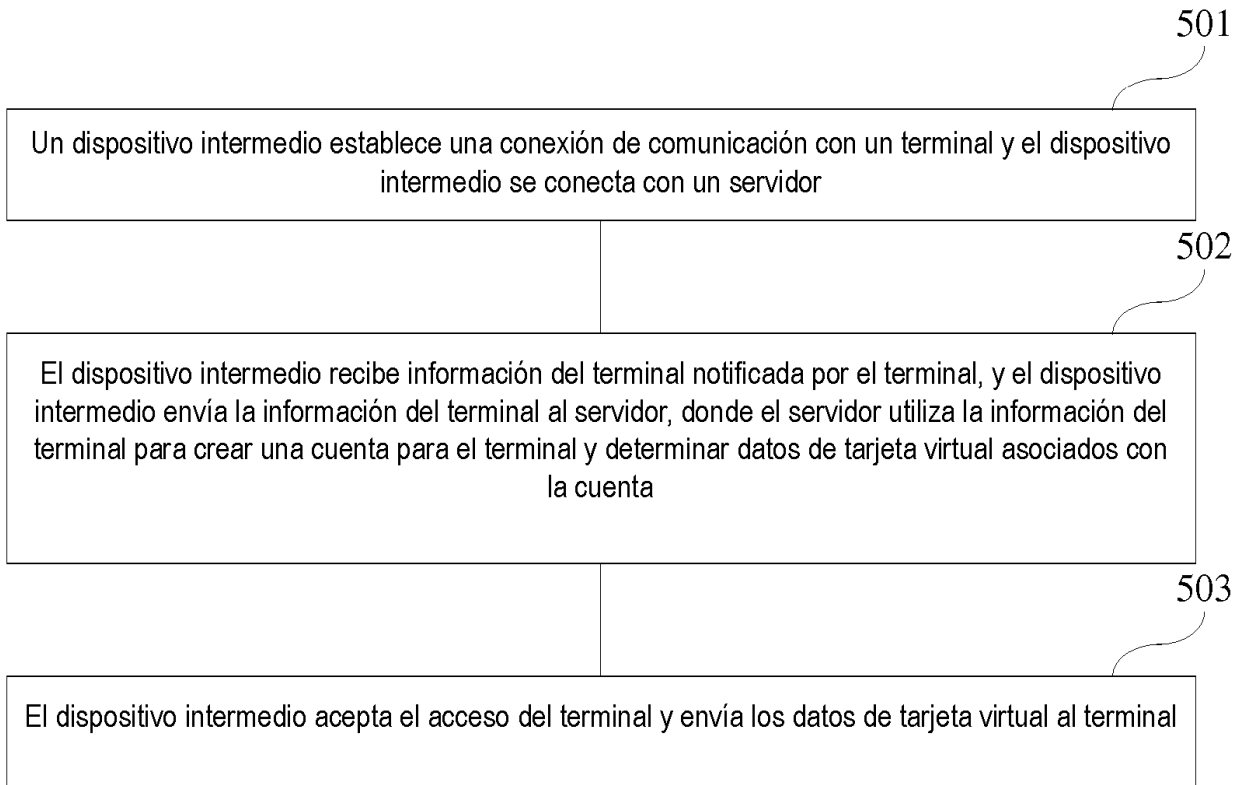


FIG. 5

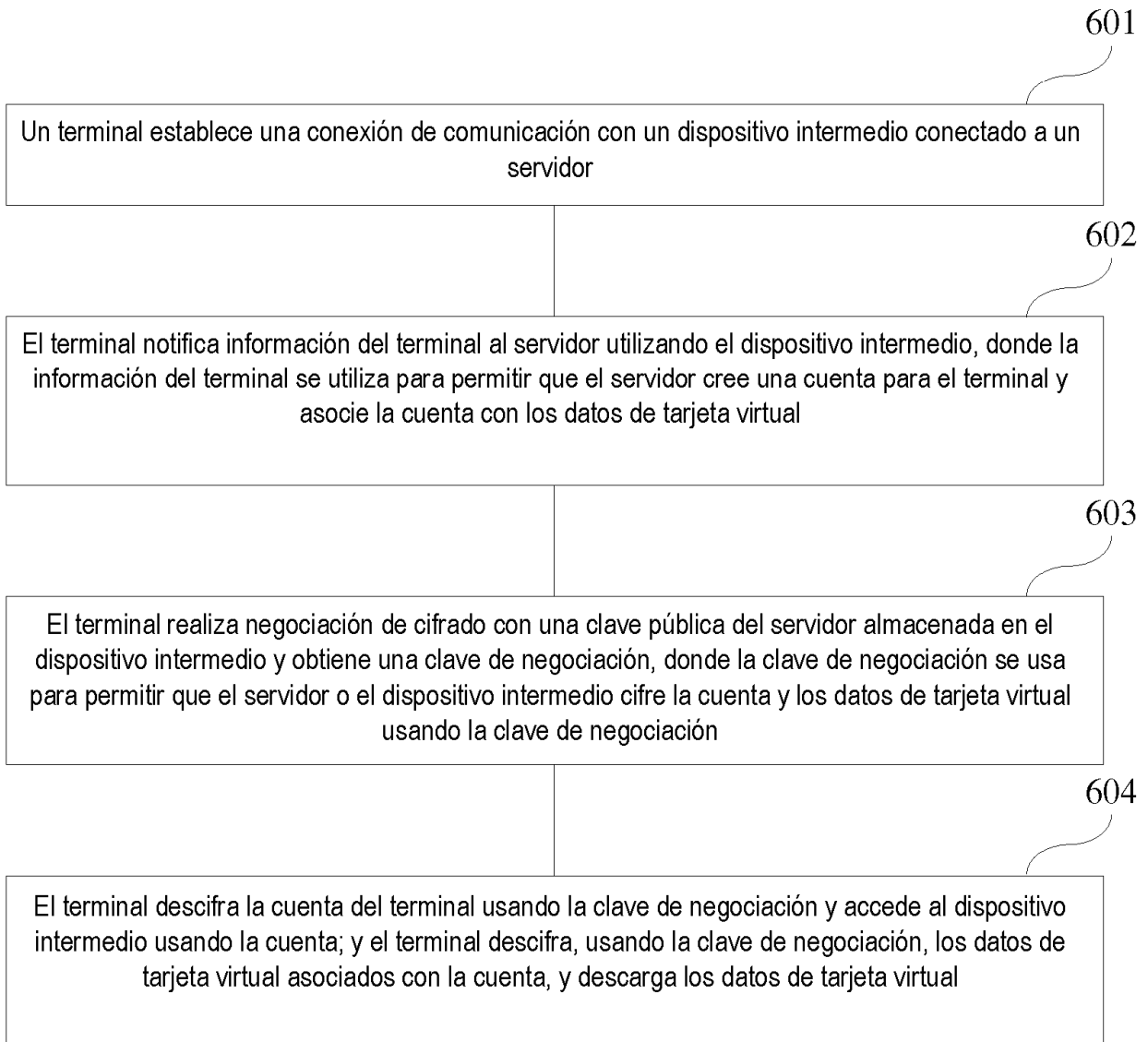


FIG. 6

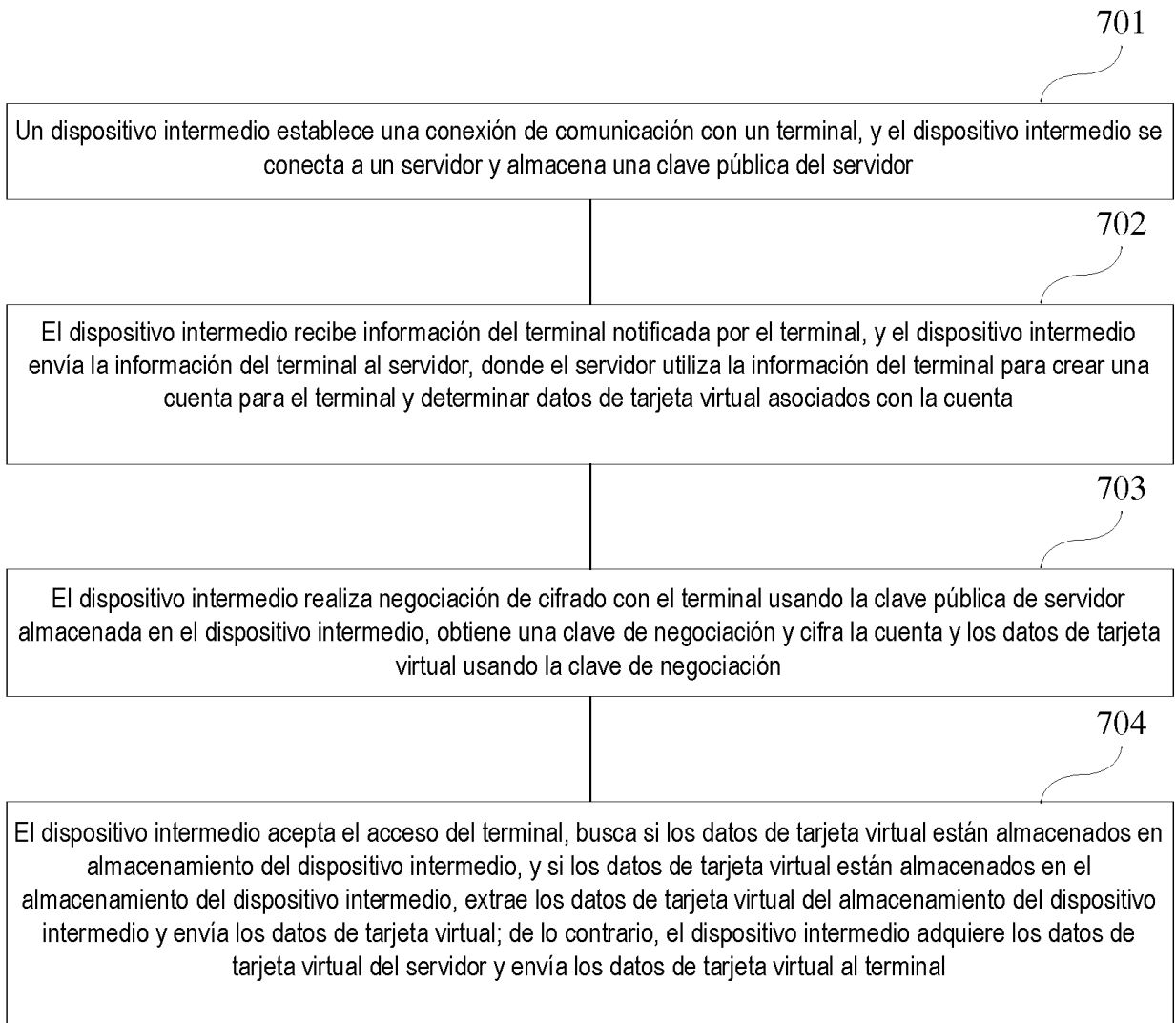


FIG. 7

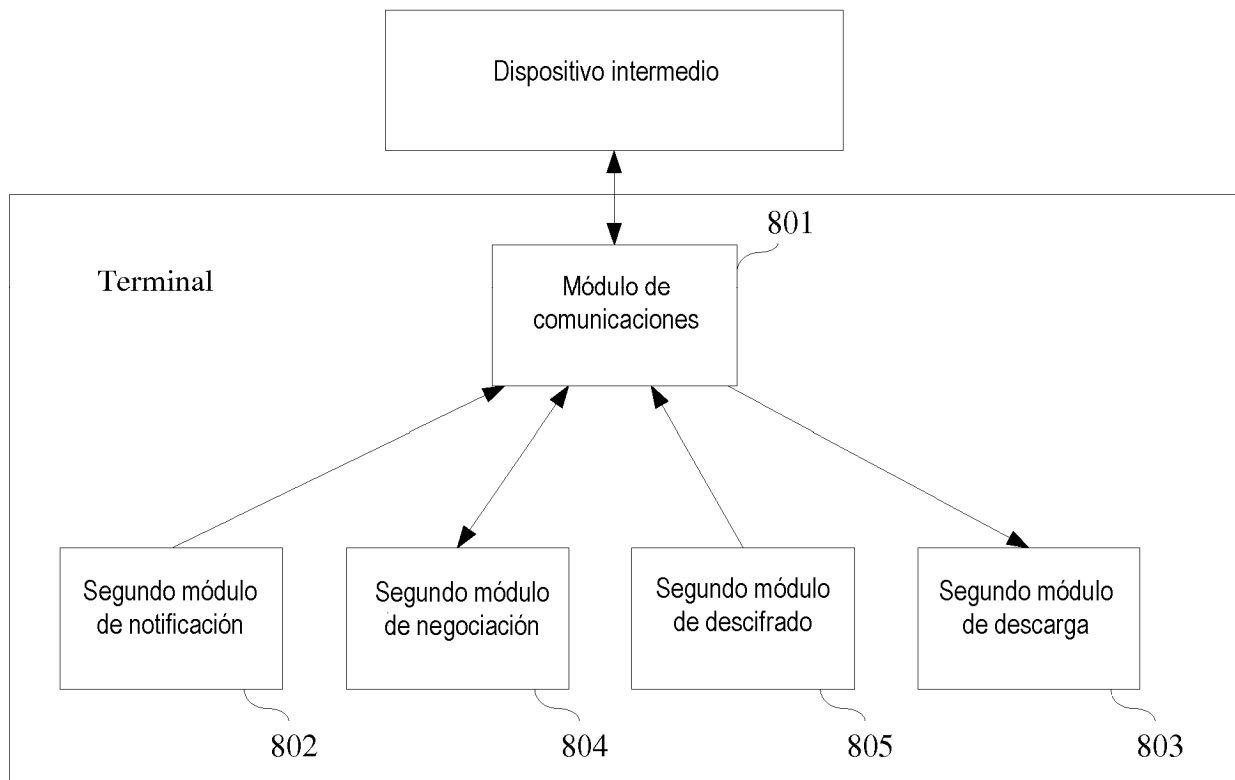


FIG. 8

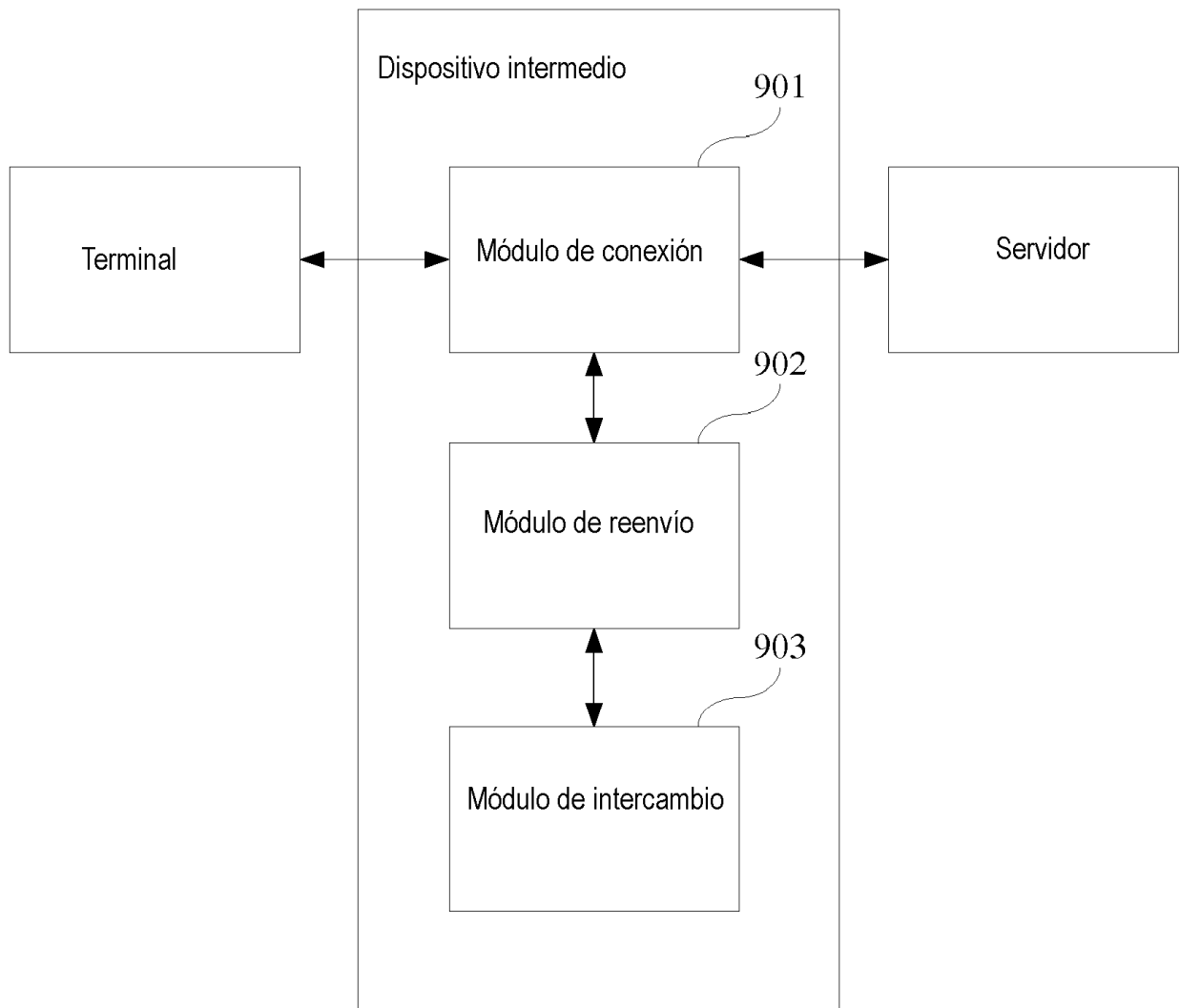


FIG. 9

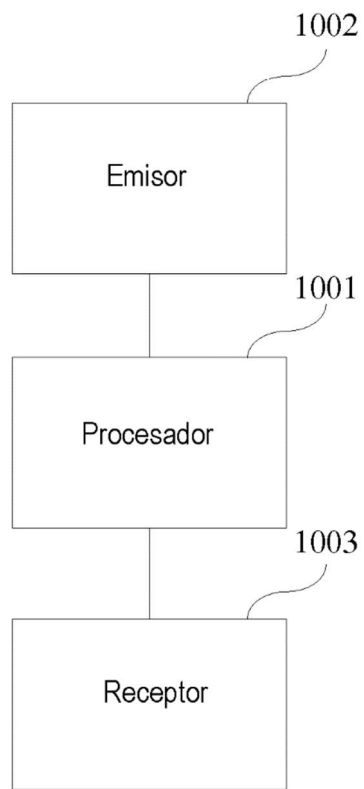


FIG. 10

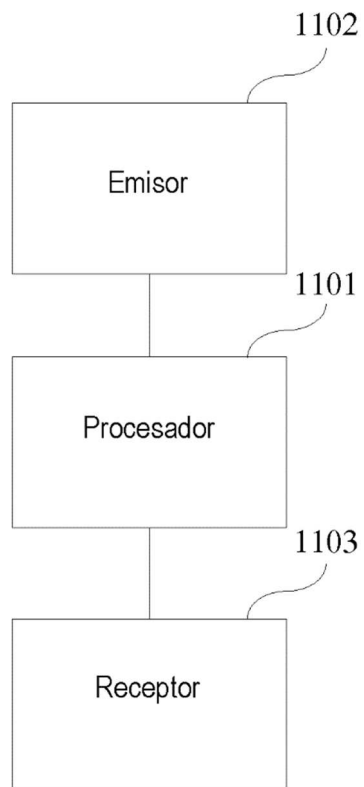


FIG. 11

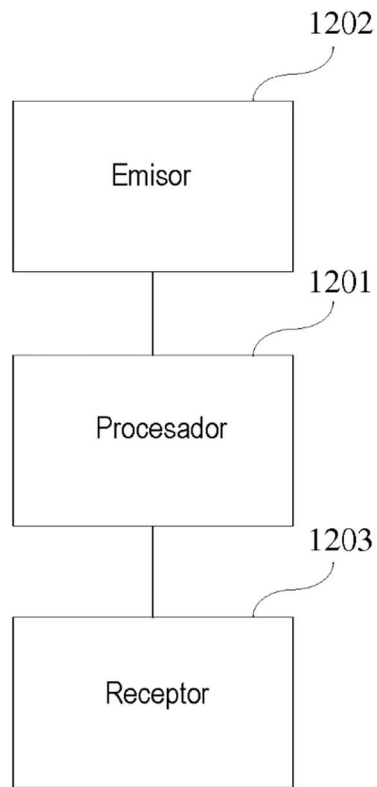


FIG. 12

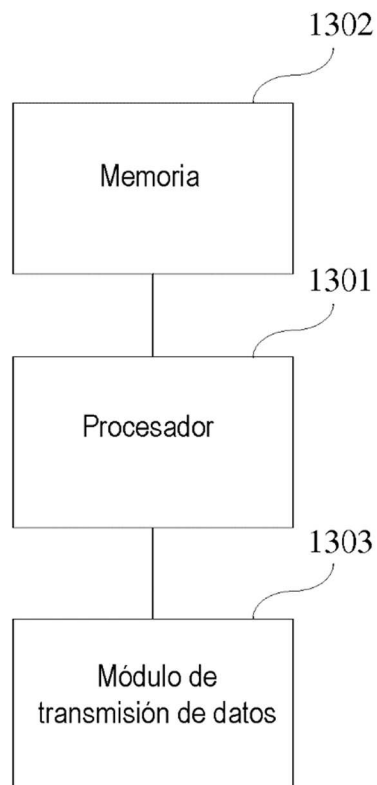


FIG. 13