(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 820 554**

(51) Int. CI.:

***H04L 9/32*** (2006.01)
***H04L 29/06*** (2006.01)
***H04W 12/06*** (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.03.2016 PCT/CN2016/076415**

(87) Fecha y número de publicación internacional: **06.10.2016 WO16155497**

(96) Fecha de presentación y número de la solicitud europea: **15.03.2016 E 16771252 (0)**

(97) Fecha y número de publicación de la concesión europea: **26.08.2020 EP 3280090**

(54) Título: **Método y aparato para autentificar un usuario, método y aparato para registrar un dispositivo ponible**

(30) Prioridad:

**02.04.2015 CN 201510155552**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**21.04.2021**

(73) Titular/es:

**ADVANCED NEW TECHNOLOGIES CO., LTD. (100.0%)**
**Cayman Corporate Centre, 27 Hospital Road George Town, Grand Cayman KY1-9008, KY**

(72) Inventor/es:

**JIANG, LONG**

(74) Agente/Representante:

**VIDAL GONZÁLEZ, Maria Ester**

## DESCRIPCIÓN

Método y aparato para autentificar un usuario, método y aparato para registrar un dispositivo ponible

Campo técnico

La presente solicitud se refiere al campo de las tecnologías de Internet y, en particular, a un método y un aparato para autenticar a un usuario y un método y un aparato para registrar un dispositivo ponible.

Técnica anterior

Con el rápido desarrollo de las tecnologías de Internet, los usuarios realizan todo tipo de actividades, tales como el manejo de negocios oficiales, entretenimiento, compras y administración de dinero, utilizando cada vez más las redes. Un usuario obtiene usualmente estos servicios de varios proveedores de servicios. El usuario se registra en los servidores de los proveedores de servicios, y necesita proporcionar una cuenta y una contraseña cada vez que el usuario obtiene un servicio, para que el servidor autentique al usuario y brinde el servicio correspondiente.

Por motivos de seguridad, el usuario debe intentar evitar el uso de la misma cuenta y la misma contraseña en varios proveedores de servicios. Cuando el usuario desea obtener cada vez más servicios, memorizar una cuenta en cada proveedor de servicios y una contraseña correspondiente se convierte en una carga creciente para el usuario. Al mismo tiempo, como los servicios de red se popularizan cada vez más en todos los aspectos de la vida, el usuario siempre necesita introducir cuentas y contraseñas para lograr la autenticación, lo que tiene operaciones complejas y reduce la eficiencia para adquirir los servicios de red.

DIEZ PANIAGUA FIDEL Y OTROS, "Toward self-authenticable wearable devices", IEEE Wireless Communications, febrero de 2015, define un protocolo de autenticación que permite la autenticación mutua segura de extremo a extremo entre un dispositivo ponible y cualquier otra entidad.

Resumen de la invención

La invención está definida por las reivindicaciones 1, 11, 19 y 20.

En vista de lo anterior, la presente solicitud proporciona un método para autenticar a un usuario, aplicado a un servidor, en donde el servidor almacena una relación correspondiente entre una identificación de usuario, una identificación del dispositivo ponible y una clave de autenticación del servidor del usuario, y el método incluye:

recibir una solicitud de autenticación enviada por el usuario a través de un terminal, la solicitud de autenticación que porta la identificación del usuario y/o la identificación del dispositivo ponible del usuario;

adquirir información de autenticación de enlace descendente y emitir al terminal una instrucción de detección que porta la información de autenticación de enlace descendente y la identificación del dispositivo ponible del usuario;

recibir un acuse de recibo de detección, devuelto por el terminal, que porta la información de autenticación de enlace ascendente, la información de autenticación de enlace ascendente se genera, por un dispositivo ponible designado en la instrucción de detección, de acuerdo con una clave de autenticación del dispositivo y la información de autenticación de enlace descendente, y la clave de autenticación del dispositivo es la misma que o corresponde a la clave de autenticación del servidor; y

hacer coincidir la información de autenticación de enlace descendente con la información de autenticación de enlace ascendente utilizando la clave de autenticación del servidor del usuario, en donde el usuario pasa la autenticación si la coincidencia tiene éxito.

La presente solicitud proporciona un método para autenticar a un usuario, aplicado a un terminal conectado a un dispositivo ponible del usuario, en donde el método incluye:

enviar una solicitud de autenticación a un servidor de acuerdo con una operación del usuario, la solicitud de autenticación que porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario;

recibir una instrucción de detección del servidor, la instrucción de detección que porta la información de autenticación de enlace descendente y la identificación del dispositivo ponible;

enviar la información de autenticación de enlace descendente a un dispositivo ponible designado en la instrucción de detección y recibir la información de autenticación de enlace ascendente devuelta por el dispositivo ponible; la información de autenticación de enlace ascendente se genera por el dispositivo ponible de acuerdo con una clave de autenticación del dispositivo almacenada y la información de autenticación de enlace descendente, la clave de

autenticación del dispositivo es la misma o correspondiente a una clave de autenticación del servidor almacenada en el servidor;

enviar al servidor un acuse de recibo de detección que porta la información de autenticación de enlace ascendente; y

recibir un resultado de autenticación de usuario determinado por el servidor de acuerdo con la información de autenticación de enlace ascendente, la información de autenticación de enlace descendente y la clave de autenticación del servidor.

La presente solicitud proporciona un método para registrar un dispositivo ponible, aplicado a un servidor, que incluye:

recibir una solicitud de registro del dispositivo ponible enviada por un usuario a través de un terminal, la solicitud de registro que porta una identificación de usuario y una identificación del dispositivo ponible del usuario;

adquirir una clave de autenticación del servidor del usuario y una clave de autenticación del dispositivo, y emitir al terminal una instrucción de escritura que porta la clave de autenticación del dispositivo y la identificación del dispositivo ponible del usuario; y

recibir un acuse de recibo de escritura devuelto por el terminal, y si el acuse de recibo de escritura indica que la clave de autenticación del dispositivo se ha almacenado con éxito en un dispositivo ponible designado en la instrucción de escritura, almacenar una relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario.

La presente solicitud proporciona un método para registrar un dispositivo ponible, aplicado a un terminal, que incluye:

enviar una solicitud de registro del dispositivo ponible a un servidor de acuerdo con una operación de un usuario; la solicitud de registro que porta una identificación de usuario y una identificación del dispositivo ponible del usuario;

recibir una instrucción de escritura del servidor, la instrucción de escritura que porta una clave de autenticación del dispositivo y la identificación del dispositivo ponible del usuario;

ejecutar una operación de escritura de la clave de autenticación del dispositivo en un dispositivo ponible designado en la instrucción de escritura; y

enviar un acuse de recibo de escritura al servidor, el acuse de recibo de escritura que porta un mensaje que indica si la clave de autenticación del dispositivo se ha escrito exitosamente.

La presente solicitud proporciona además un aparato para autenticar a un usuario, aplicado a un servidor, en donde el servidor almacena una relación correspondiente entre una identificación de usuario, una identificación del dispositivo ponible y una clave de autenticación del servidor del usuario, y el aparato incluye:

una unidad receptora de solicitud de autenticación configurada para recibir una solicitud de autenticación enviada por el usuario a través de un terminal, la solicitud de autenticación que porta la identificación del usuario y/o la identificación del dispositivo ponible del usuario;

una unidad de emisión de instrucciones de detección configurada para adquirir información de autenticación de enlace descendente y emitir al terminal una instrucción de detección que porta la información de autenticación de enlace descendente y la identificación del dispositivo ponible del usuario;

una unidad receptora de acuse de recibo de detección configurada para recibir un acuse de recibo de detección, devuelto por el terminal, que porta la información de autenticación de enlace ascendente, la información de autenticación de enlace ascendente se genera, mediante un dispositivo ponible designado en la instrucción de detección, de acuerdo con una clave de autenticación del dispositivo y la autenticación de enlace descendente información, y la clave de autenticación del dispositivo es la misma o corresponde a la clave de autenticación del servidor; y

una unidad de coincidencia configurada para hacer coincidir la información de autenticación de enlace descendente con la información de autenticación de enlace ascendente utilizando la clave de autenticación del servidor del usuario, en donde el usuario pasa la autenticación si la coincidencia tiene éxito.

La presente solicitud proporciona un aparato para autenticar a un usuario, aplicado a un terminal conectado a un dispositivo ponible del usuario, en donde el aparato incluye:

una unidad de envío de solicitud de autenticación configurada para enviar una solicitud de autenticación a un servidor de acuerdo con una operación del usuario, la solicitud de autenticación que porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario;

una unidad receptora de instrucciones de detección configurada para recibir una instrucción de detección del servidor, la instrucción de detección que porta la información de autenticación de enlace descendente y la identificación del dispositivo ponible;

una unidad de información de autenticación de enlace ascendente configurada para enviar la información de autenticación de enlace descendente a un dispositivo ponible designado en la instrucción de detección, y recibir la información de autenticación de enlace ascendente devuelta por el dispositivo ponible; la información de autenticación de enlace ascendente se genera por el dispositivo ponible de acuerdo con una clave de autenticación del dispositivo almacenada y la información de autenticación de enlace descendente, la clave de autenticación del dispositivo es la misma o correspondiente a una clave de autenticación del servidor almacenada en el servidor;

una unidad de envío de acuse de recibo de detección configurada para enviar al servidor un acuse de recibo de detección que porta la información de autenticación de enlace ascendente; y

una unidad receptora de resultados de autenticación configurada para recibir un resultado de autenticación de usuario determinado por el servidor de acuerdo con la información de autenticación de enlace ascendente, la información de autenticación de enlace descendente y la clave de autenticación del servidor.

La presente solicitud proporciona un aparato para registrar un dispositivo ponible, aplicado a un servidor, que incluye:

una unidad receptora de solicitud de registro configurada para recibir una solicitud de registro del dispositivo ponible enviada por un usuario a través de un terminal, la solicitud de registro que porta una identificación de usuario y una identificación del dispositivo ponible del usuario;

una unidad de emisión de instrucciones de escritura configurada para adquirir una clave de autenticación del servidor del usuario y una clave de autenticación del dispositivo, y emitir al terminal una instrucción de escritura que porta la clave de autenticación del dispositivo y la identificación del dispositivo ponible del usuario; y

una unidad receptora de acuse de recibo de escritura configurada para recibir un acuse de recibo de escritura devuelto por el terminal, y si el acuse de recibo de escritura indica que la clave de autenticación del dispositivo se ha almacenado con éxito en un dispositivo ponible designado en la instrucción de escritura, almacenar una relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario.

La presente solicitud proporciona un aparato para registrar un dispositivo ponible, aplicado a un terminal, que incluye:

una unidad de envío de solicitud de registro configurada para enviar una solicitud de registro del dispositivo ponible a un servidor de acuerdo con una operación de un usuario, la solicitud de registro que porta una identificación de usuario y una identificación del dispositivo ponible del usuario;

una unidad receptora de instrucciones de escritura configurada para recibir una instrucción de escritura del servidor, la instrucción de escritura que porta una clave de autenticación del dispositivo y la identificación del dispositivo ponible del usuario;

una unidad de ejecución de operación de escritura configurada para ejecutar una operación de escritura de la clave de autenticación del dispositivo en un dispositivo ponible designado en la instrucción de escritura; y

una unidad de envío de acuse de recibo de escritura configurada para enviar un acuse de recibo de escritura al servidor, el acuse de recibo de escritura que porta un mensaje que indica si la clave de autenticación del dispositivo se ha escrito exitosamente.

La presente aplicación proporciona un método de pago, que incluye:

recibir una solicitud de pago enviada por un usuario a través de un terminal de cliente de pago, la solicitud de pago que porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario;

adquirir información de autenticación de enlace descendente y emitir al terminal de cliente de pago una instrucción de autenticación que incluye la información de autenticación de enlace descendente y la identificación del dispositivo ponible;

recibir la información de respuesta de autenticación, devuelta por el terminal de cliente de pago, que porta la información de autenticación de enlace ascendente, la información de autenticación de enlace ascendente se genera, por un dispositivo ponible designado en la instrucción de autenticación, de acuerdo con una clave de autenticación del dispositivo y la información de autenticación de enlace descendente, y la clave de autenticación del dispositivo es la misma o corresponde a una clave de autenticación del servidor; y

hacer coincidir la información de autenticación de enlace descendente con la información de autenticación de enlace ascendente utilizando la clave de autenticación del servidor del usuario, en donde el usuario pasa la autenticación si la coincidencia tiene éxito, y se lleva a cabo una operación de pago después de que la autenticación sea exitosa.

La presente aplicación proporciona un método de pago, que incluye:

enviar una solicitud de pago a un servidor en respuesta a una operación de pago de un usuario en un terminal de cliente de pago, la solicitud de pago que porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario;

recibir una instrucción de autenticación, emitida por el servidor, que incluye la información de autenticación de enlace descendente y la identificación del dispositivo ponible, y enviar la información de autenticación de enlace descendente a un dispositivo ponible, de modo que el dispositivo ponible genera la información de autenticación de enlace ascendente utilizando una clave de autenticación del dispositivo almacenada por el dispositivo ponible y la información de autenticación de enlace descendente; y

recibir la información de autenticación de enlace ascendente devuelta por el dispositivo ponible y enviar la información de autenticación de enlace ascendente al servidor, de modo que el servidor autentica al usuario de acuerdo con la información de autenticación de enlace ascendente y realiza una operación de pago después de que la autenticación sea exitosa.

La presente solicitud proporciona un método de pago para un dispositivo ponible, que incluye:

recibir la información de autenticación de pago enviada por un terminal de cliente de pago, la solicitud de pago una que porta la información de autenticación de enlace descendente emitida por un servidor en base a una solicitud de pago de un usuario enviada por el terminal de cliente de pago; y

generar información de autenticación de enlace ascendente basada en una clave de autenticación del dispositivo almacenada y la información de autenticación de enlace descendente, y enviar la información de autenticación de enlace ascendente al terminal de cliente de pago, de modo que el terminal de cliente de pago envíe la información de autenticación de enlace ascendente al servidor, de modo que el servidor pueda autenticar al usuario en base a la información de autenticación de enlace ascendente y realiza una operación de pago después de que la autenticación sea exitosa.

La presente solicitud proporciona un aparato de pago, que incluye:

una unidad receptora de solicitud de pago configurada para recibir una solicitud de pago enviada por un usuario a través de un terminal de cliente de pago, la solicitud de pago que porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario;

una unidad de emisión de instrucciones de autenticación configurada para adquirir información de autenticación de enlace descendente y emitir al terminal de cliente de pago una instrucción de autenticación que incluye la información de autenticación de enlace descendente y la identificación del dispositivo ponible;

una unidad receptora de respuesta de autenticación configurada para recibir la información de respuesta de autenticación, devuelta por el terminal de cliente de pago, que porta la información de autenticación de enlace ascendente, la información de autenticación de enlace ascendente se genera, mediante un dispositivo ponible designado en la instrucción de autenticación, de acuerdo con una clave de autenticación del dispositivo y la información de autenticación de enlace descendente y la clave de autenticación del dispositivo es la misma o corresponde a una clave de autenticación del servidor; y

una unidad de coincidencia de pago configurada para hacer coincidir la información de autenticación de enlace descendente con la información de autenticación de enlace ascendente utilizando la clave de autenticación del servidor del usuario, en donde el usuario pasa la autenticación si la coincidencia tiene éxito, y se lleva a cabo una operación de pago después de que la autenticación sea exitosa.

La presente solicitud proporciona un aparato de pago, que incluye:

una unidad de envío de solicitud de pago configurada para enviar una solicitud de pago a un servidor en respuesta a una operación de pago de un usuario en un terminal de cliente de pago, la solicitud de pago que porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario;

una unidad receptora de instrucciones de autenticación configurada para recibir una instrucción de autenticación, emitida por el servidor, que incluye la información de autenticación de enlace descendente y la identificación del dispositivo ponible, y envía la información de autenticación de enlace descendente a un dispositivo ponible, de modo que el dispositivo ponible genera la información de autenticación de enlace ascendente utilizando una clave de

autenticación del dispositivo almacenada por el dispositivo ponible y la información de autenticación de enlace descendente; y

una unidad de envío de respuesta de autenticación configurada para recibir la información de autenticación de enlace ascendente devuelta por el dispositivo ponible y enviar la información de autenticación de enlace ascendente al servidor, de modo que el servidor autentica al usuario de acuerdo con la información de autenticación de enlace ascendente y realiza una operación de pago después de que la autenticación sea exitosa.

La presente solicitud proporciona además un aparato de pago para un dispositivo ponible, que incluye:

una unidad receptora de información de autenticación de pago configurada para recibir la información de autenticación de pago enviada por un terminal de cliente de pago, la información de autenticación de pago que incluye la información de autenticación de enlace descendente emitida por un servidor en base a una solicitud de pago de un usuario enviada por el terminal de cliente de pago; y

una unidad de generación de información de autenticación de enlace ascendente configurada para generar información de autenticación de enlace ascendente basada en una clave de autenticación del dispositivo almacenada y la información de autenticación de enlace descendente, y enviar la información de autenticación de enlace ascendente al terminal de cliente de pago, de modo que el terminal de cliente de pago envíe la información de autenticación de enlace ascendente al servidor, de modo que el servidor pueda autenticar al usuario en base a la información de autenticación de enlace ascendente y realizar una operación de pago después de que la autenticación sea exitosa.

Se puede ver en las soluciones técnicas anteriores que, de acuerdo con las modalidades de la presente solicitud, una clave de autenticación del servidor y una clave de autenticación del dispositivo se establecen en un servidor y un dispositivo ponible, y el servidor autentica, a través de la interacción con un terminal, un dispositivo ponible designado mediante el uso de la clave de autenticación del servidor configurada y la clave de autenticación del dispositivo configurada, logrando de esta manera la autenticación en un usuario correspondiente al dispositivo ponible. El usuario no necesita memorizar ninguna cuenta y contraseña ni necesita introducir ninguna cuenta y contraseña durante la autenticación, lo que reduce la carga para el usuario y mejora la eficiencia del usuario para adquirir un servicio de red.

Breve descripción de los dibujos

La Figura 1 muestra un diagrama de estructura de red de un escenario de aplicación de acuerdo con la presente solicitud;

La Figura 2 es un diagrama de flujo de un método para autenticar a un usuario aplicado a un servidor de acuerdo con una modalidad de la presente solicitud;

La Figura 3 es un diagrama de flujo de un método para autenticar a un usuario aplicado a un terminal de acuerdo con una modalidad de la presente solicitud;

La Figura 4 es un diagrama de flujo de un método para registrar un dispositivo ponible aplicado a un servidor de acuerdo con una modalidad de la presente solicitud;

La Figura 5 es un diagrama de flujo de un método para registrar un dispositivo ponible aplicado a un terminal de acuerdo con una modalidad de la presente solicitud;

La Figura 6 es un diagrama de estructura de hardware de un servidor, un dispositivo ponible o un terminal;

La Figura 7 es un diagrama de estructura lógica de un aparato para autenticar a un usuario aplicado a un servidor de acuerdo con una modalidad de la presente solicitud;

La Figura 8 es un diagrama de estructura lógica de un aparato para autenticar a un usuario aplicado a un terminal de acuerdo con una modalidad de la presente solicitud;

La Figura 9 es un diagrama de estructura lógica de un aparato para registrar un dispositivo ponible aplicado a un servidor de acuerdo con una modalidad de la presente solicitud; y

La Figura 10 es un diagrama de estructura lógica de un aparato para registrar un dispositivo ponible aplicado a un terminal de acuerdo con una modalidad de la presente solicitud.

Descripción detallada

Un dispositivo ponible es un dispositivo ponible que un usuario puede usar o integrar en la ropa o accesorio de un usuario, por ejemplo, pulseras, relojes inteligentes, zapatos inteligentes, ropa inteligente, gafas inteligentes, cascos

inteligentes, anillos inteligentes, etc. El dispositivo ponible tiene algunas funciones informáticas, se puede conectar a un terminal tal como un teléfono inteligente, una tableta y una computadora personal a través de una interfaz de hardware o una red de área local inalámbrica, e implementa una variedad de funciones al intercambiar datos con el terminal.

Un dispositivo ponible es generalmente específico para un usuario. Los usuarios pueden usar algunos dispositivos ponibles siempre que sea posible. Hasta cierto punto, dicho dispositivo ponible representa a un usuario. Una modalidad de la presente solicitud propone un método para autenticar a un usuario, que autentica al usuario utilizando las funciones de almacenamiento e informáticas de un dispositivo ponible sin requerir que el usuario memorice e ingrese frecuentemente una cuenta y una contraseña, resolviendo de esta manera los problemas existentes en el estado de la técnica.

Un entorno de red al que se aplica la modalidad de la presente aplicación es como se muestra en la Figura 1. Un dispositivo ponible se conecta a un terminal a través de una interfaz de hardware o una red de área local inalámbrica. La interfaz de hardware puede ser una interfaz de audio, una interfaz de bus serie universal (USB) o similar. La red de área local inalámbrica puede ser Bluetooth, Wireless-Fidelity (Wi-Fi), ZigBee (protocolo ZigBee) o similares. El terminal puede ser un teléfono inteligente, una tableta, una computadora personal o similar. El terminal se comunica con un servidor a través de una red de comunicación (tal como Internet y/o una red de comunicación móvil). Un usuario envía una solicitud de acceso al servidor con el terminal y el servidor autentica al usuario. En la modalidad de la presente solicitud, no se imponen limitaciones al tipo de terminal, la interfaz de hardware o un protocolo de red de área local inalámbrica a través del cual el dispositivo ponible se conecta al terminal, el protocolo y la estructura de red de la red de comunicación y una implementación específica del servidor.

En una modalidad de la presente solicitud, un proceso del método para autenticar a un usuario en un servidor es como se muestra en la Figura 2, y un proceso del mismo en un terminal es como se muestra en la Figura 3.

En esta modalidad, el servidor almacena una relación correspondiente entre una identificación de usuario, una identificación del dispositivo ponible y una clave de autenticación del servidor de un usuario. La identificación de usuario es una identificación de identidad única de acuerdo con la cual un usuario se distingue de otros usuarios para el servidor, por ejemplo, un nombre de usuario, un correo registrado o similares. Si el usuario está vinculado a un terminal móvil, la identificación de usuario también puede ser un número, una identidad de equipo móvil internacional (IMIE) o similar del terminal móvil al que está vinculado el usuario. La identificación del dispositivo ponible se utiliza para representar de forma única el dispositivo ponible y varía con un tipo de dispositivo específico diferente y un protocolo de red de área local inalámbrica diferente adoptado. La identificación del dispositivo ponible puede ser generalmente una dirección de hardware del dispositivo ponible, por ejemplo, una dirección de control de acceso a medios (MAC). La clave de autenticación del servidor se almacena en el servidor y es la misma o corresponde a una clave de autenticación del dispositivo almacenada en el dispositivo ponible de acuerdo con un algoritmo de cifrado que utiliza la clave de autenticación del servidor. La identificación del dispositivo ponible y la clave de autenticación del servidor almacenada en el servidor son uno a uno correspondientes entre sí. Si un usuario puede tener más de un dispositivo ponible para la autenticación, una identificación de usuario puede corresponder a dos o más identificaciones del dispositivo ponible y claves de autenticación del servidor. Además, debe tenerse en cuenta que la relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor puede almacenarse en el servidor localmente, y también puede almacenarse en otros dispositivos de almacenamiento accesibles al servidor, por ejemplo, un matriz de discos para almacenar redes de área local o una red de almacenamiento en la nube, que no está limitada en esta modalidad.

En el terminal, en la etapa 310, se envía una solicitud de autenticación a un servidor de acuerdo con una operación de un usuario, la solicitud de autenticación que porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario.

En el servidor, en la etapa 210, se recibe una solicitud de autenticación enviada por un usuario a través de un terminal.

Cuando el usuario solicita, desde un servidor, un servicio que requiere autenticación de identidad (por ejemplo, inicio de sesión, acceso a una cuenta personal, pago o similar) en el terminal, el servidor requiere, desde el terminal, la información relacionada para autenticar al usuario. El terminal envía una solicitud de autenticación al servidor. La solicitud de autenticación porta la identificación de usuario del usuario, o la identificación del dispositivo ponible del usuario, o la identificación del usuario y la identificación del dispositivo ponible del usuario.

Después de que el servidor recibe la solicitud de autenticación del terminal, se puede determinar qué usuario solicita la autenticación mediante la identificación del usuario y/o la identificación del dispositivo ponible en la solicitud de autenticación.

En el servidor, en la etapa 220, se adquiere información de autenticación de enlace descendente, y se envía al terminal una instrucción de detección que porta la información de autenticación de enlace descendente y la identificación del dispositivo ponible del usuario.

La información de autenticación de enlace descendente puede ser una parte de los datos de autenticación y también puede ser un texto cifrado después de que los datos de autenticación se cifren utilizando la clave de autenticación del servidor almacenada en el servidor. El servidor puede obtener los datos de autenticación de cualquier manera, por ejemplo, el servidor genera aleatoriamente los datos de autenticación o captura un cierto número de bytes de un archivo o una imagen. El servidor puede generar los datos de autenticación localmente por sí mismo y también puede adquirir los datos de autenticación de otro servidor. Esta modalidad no lo limita.

Después de recibir la solicitud de autenticación del terminal, el servidor extrae la identificación del usuario y/o la identificación del dispositivo ponible en la solicitud de autenticación, encuentra, en la relación correspondiente almacenada entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor, si se incluye la identificación del usuario y/o la identificación del dispositivo ponible. Si la identificación del usuario y/o la identificación del dispositivo ponible no están incluidas o la identificación del usuario y la identificación del dispositivo ponible en la solicitud de autenticación no pertenecen a un mismo usuario, el servidor rechaza la solicitud de autenticación del terminal. De lo contrario, el servidor adquiere datos de autenticación. Para la información de autenticación de enlace descendente como texto sin formato, el servidor encapsula los datos de autenticación y la identificación del dispositivo ponible del usuario en una instrucción de detección y emite la instrucción de detección al terminal. Para la información de autenticación de enlace descendente como texto cifrado, el servidor cifra los datos de autenticación mediante el uso de una clave de autenticación del servidor correspondiente a la identificación del usuario o la identificación del dispositivo ponible en la solicitud de autenticación para generar información de autenticación de enlace descendente, encapsula la información de autenticación de enlace descendente y la identificación del dispositivo ponible del usuario en una instrucción de detección y emite la instrucción de detección al terminal.

En el terminal, en la etapa 320, se recibe una instrucción de detección del servidor, la instrucción de detección que porta la información de autenticación de enlace descendente y la identificación del dispositivo ponible.

En el terminal, en la etapa 330, la información de autenticación de enlace descendente se envía a un dispositivo ponible designado en la instrucción de detección, y se recibe la información de autenticación de enlace ascendente devuelta por el dispositivo ponible; la información de autenticación de enlace ascendente se genera por el dispositivo ponible de acuerdo con una clave de autenticación del dispositivo almacenada y la información de autenticación de enlace descendente.

El terminal recibe una instrucción de detección del servidor, extrae la identificación del dispositivo ponible y la información de autenticación de enlace descendente del mismo, y envía la información de autenticación de enlace descendente a un dispositivo ponible designado en la instrucción de detección (es decir, un dispositivo ponible que tiene la identificación del dispositivo ponible en la instrucción de detección). Si el dispositivo ponible designado en las instrucciones de detección aún no se ha conectado al terminal, el terminal debe completar primero una conexión con el dispositivo ponible de acuerdo con un protocolo de red de área local inalámbrica compatible con el dispositivo ponible.

Como se indicó anteriormente, el dispositivo ponible designado por el servidor almacena la clave de autenticación del dispositivo igual o correspondiente a la clave de autenticación del servidor. Después de que el dispositivo ponible recibe la información de autenticación de enlace descendente, para la información de autenticación de enlace descendente como texto sin formato, el dispositivo ponible cifra la información de autenticación de enlace descendente utilizando la clave de autenticación del dispositivo, para generar información de autenticación de enlace ascendente como un texto cifrado. Para la información de autenticación de enlace descendente como texto cifrado, el dispositivo ponible descifra la información de autenticación de enlace descendente utilizando la clave de autenticación del dispositivo, para generar información de autenticación de enlace ascendente como texto sin formato. La información de autenticación de enlace descendente como texto sin formato corresponde a la información de autenticación de enlace ascendente como texto cifrado, y la información de autenticación de enlace descendente como texto cifrado corresponde a la información de autenticación de enlace ascendente como texto sin formato. El dispositivo ponible devuelve la información de autenticación de enlace ascendente al terminal.

En el terminal, en la etapa 340, se envía al servidor un acuse de recibo de detección que porta la información de autenticación de enlace ascendente.

Después de recibir la información de autenticación de enlace ascendente devuelta por el dispositivo ponible, el terminal encapsula la información de autenticación de enlace ascendente en un acuse de recibo de detección y envía el acuse de recibo de detección al servidor. El acuse de recibo de detección generalmente porta además la identificación del dispositivo ponible.

En el servidor, en la etapa 230, se recibe un acuse de recibo de detección, devuelto por el terminal, que porta la información de autenticación de enlace ascendente.

En el servidor, en la etapa 240, la información de autenticación de enlace descendente se compara con la información de autenticación de enlace ascendente utilizando la clave de autenticación del servidor del usuario, en donde el usuario pasa la autenticación si la coincidencia tiene éxito.

El servidor recibe el acuse de recibo de detección devuelto por el terminal, extrae la información de autenticación de enlace ascendente del mismo y juzga si la información de autenticación de enlace ascendente coincide con la información de autenticación de enlace descendente utilizando la clave de autenticación del servidor del usuario, para determinar un resultado de autenticación del usuario. Específicamente, para la información de autenticación de enlace ascendente como texto sin formato, es posible comparar la información de autenticación de enlace ascendente con datos de autenticación para generar un texto cifrado o comparar la información de autenticación de enlace ascendente que se ha cifrado utilizando la clave de autenticación del servidor con la información de autenticación de enlace descendente, si son iguales, el usuario pasa la autenticación y, de lo contrario, la autenticación falla. Para la información de autenticación de enlace ascendente como texto cifrado, la información de autenticación de enlace ascendente se puede descifrar utilizando la clave de autenticación del servidor y luego se puede comparar con la información de autenticación de enlace descendente, si son iguales, el usuario pasa la autenticación y, de lo contrario, la autenticación falla.

El servidor devuelve al terminal un resultado de autenticación que indica si el usuario pasa la autenticación.

En el terminal, en la etapa 350, se recibe un resultado de autenticación de usuario determinado por el servidor de acuerdo con la información de autenticación de enlace ascendente, la información de autenticación de enlace descendente y la clave de autenticación del servidor.

En esta modalidad, una clave de autenticación del servidor y una clave de autenticación del dispositivo que son iguales o se corresponden entre sí se establecen en un servidor y un dispositivo ponible, el servidor autentica, mediante la interacción con un terminal, un dispositivo ponible designado mediante el uso de la clave de autenticación del dispositivo almacenada en el dispositivo ponible y la clave de autenticación del servidor almacenada en el servidor, logrando de esta manera la autenticación en un usuario correspondiente al dispositivo ponible. El usuario no necesita memorizar ninguna cuenta y contraseña ni necesita introducir ninguna cuenta y contraseña durante la autenticación, lo que reduce la carga para el usuario y mejora la eficiencia del usuario para adquirir un servicio de red.

En una implementación, una clave pública de usuario del usuario puede almacenarse en el servidor, una clave privada de usuario del usuario puede almacenarse en el terminal, una identificación de usuario diferente usa una clave pública de usuario diferente y una clave privada de usuario diferente, y la clave pública de usuario y la clave privada del usuario son un par de claves en cifrado asimétrico. La clave pública de usuario almacenada en el servidor corresponde a la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario. En tal implementación, el terminal firma los datos incluidos en el acuse de recibo de detección (que incluye la información de autenticación de enlace ascendente y también puede incluir la identificación del dispositivo ponible, la identificación del usuario y otros datos) utilizando la clave privada del usuario almacenada, y envía el acuse de recibo de detección firmado al servidor. El servidor realiza la verificación de la firma en el acuse de recibo de detección utilizando la clave pública de usuario del usuario. Si el acuse de recibo de detección pasa la verificación, se lleva a cabo la etapa 240 para hacer coincidir la información de autenticación de enlace ascendente con la información de autenticación de enlace descendente. Si el acuse de recibo de detección no pasa la verificación de la firma, se notifica al terminal que la autenticación falla. Tal implementación requiere que un terminal al que está conectado un dispositivo ponible debería almacenar una clave privada de usuario de un usuario cuando el usuario usa el dispositivo ponible para la autenticación, lo que puede lograr una mejor seguridad.

Además, se puede agregar una identificación de terminal a la relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario almacenada en el servidor, para restringir el terminal capaz de realizar la autenticación del usuario a través del dispositivo ponible conectado al mismo. En tal situación, el servidor almacena una relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario y la identificación del terminal. Una solicitud de autenticación enviada por el terminal al servidor porta una identificación de terminal del terminal. Después de recibir la solicitud de autenticación, el servidor encuentra, en la relación correspondiente almacenada, una identificación del terminal correspondiente a la identificación del usuario o la identificación del dispositivo ponible en la solicitud de autenticación, y compara la identificación del terminal con la identificación del terminal para enviar la solicitud de autenticación. Si son iguales, se lleva a cabo la etapa 220 para continuar el proceso de autenticación. Si son diferentes, se rechaza la solicitud de autenticación del terminal y falla la autenticación del usuario. Tal implementación es equivalente a vincular un dispositivo ponible a un terminal capaz de realizar la autenticación de usuario a través del dispositivo ponible. Como un terminal (especialmente un terminal móvil) generalmente también es específico para un usuario, la vinculación de un dispositivo ponible al terminal puede mejorar significativamente la seguridad de autenticación del usuario.

El proceso de autenticación anterior en esta modalidad es aplicable a cualquier escenario que requiera la autenticación de la identidad de un usuario, por ejemplo, autenticación de identidad de usuario en el caso de inicio de sesión, autenticación de identidad cuando un usuario accede a una cuenta personal, autenticación de identidad cuando un usuario realiza un pago a través de una plataforma de pago de terceros, etc. Una vez que el usuario pasa la autenticación, el servidor puede proporcionar un servicio posterior en el escenario y el terminal ejecuta una operación posterior en el escenario. Por ejemplo, cuando esta modalidad se usa para la autenticación de identidad en un escenario de pago, la solicitud de autenticación enviada por el terminal a un servidor de pago es una solicitud de pago.

Una vez que el usuario pasa la autenticación, el servidor de pago puede proporcionar un servicio de pago para el usuario que pasa la autenticación. Después de recibir, del servidor, un resultado de autenticación que indica que el usuario pasa la autenticación, el terminal puede cooperar con el servidor de pago para completar una operación de pago del usuario.

En esta modalidad, es posible preestablecer la relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario en el servidor y preestablecer la clave de autenticación del dispositivo correspondiente en el dispositivo ponible. También es posible generar primero la relación correspondiente anterior en el servidor y escribir la clave de autenticación del dispositivo en el dispositivo ponible a través de un proceso de registro antes del proceso de autenticación anterior.

Otra modalidad de la presente solicitud proporciona un método para registrar un dispositivo ponible. Un proceso del método en un servidor es como se muestra en la Figura 4, y un proceso del mismo en un terminal es como se muestra en la Figura 5.

En el terminal, en la etapa 510, se envía una solicitud de registro del dispositivo ponible a un servidor de acuerdo con una operación de un usuario.

En el servidor, en la etapa 410, se recibe una solicitud de registro del dispositivo ponible enviada por un usuario a través de un terminal.

El usuario registra un dispositivo ponible con el servidor en el terminal, y el terminal envía una solicitud de registro del dispositivo ponible al servidor de acuerdo con una operación del usuario. La solicitud de registro incluye una identificación de usuario y una identificación del dispositivo ponible del usuario.

En el servidor, en la etapa 420, se adquieren una clave de autenticación del servidor del usuario y una clave de autenticación del dispositivo, y se emite al terminal una instrucción de escritura que porta la clave de autenticación del dispositivo y la identificación del dispositivo ponible del usuario.

Después de recibir la solicitud de registro del dispositivo ponible del terminal, el servidor adquiere, de acuerdo con un algoritmo de cifrado adoptado para la información de autenticación de enlace ascendente o la información de autenticación de enlace descendente en el proceso de autenticación, una clave de autenticación del servidor y una clave de autenticación del dispositivo que se utilizan para el algoritmo de cifrado y corresponden a la identificación del dispositivo ponible. La clave de autenticación del servidor y la clave de autenticación del dispositivo pueden ser una clave (por ejemplo, una clave de un algoritmo de cifrado simétrico) y también pueden ser un par de claves (por ejemplo, una clave pública y una clave privada de un algoritmo de cifrado asimétrico). El servidor puede generar la clave de autenticación del servidor y la clave de autenticación del dispositivo por sí mismo y también puede obtener la clave de autenticación del servidor y la clave de autenticación del dispositivo de otro servidor.

El servidor encapsula la clave de autenticación del dispositivo adquirida y la correspondiente identificación del dispositivo ponible en una instrucción de escritura, y envía la instrucción de escritura al terminal.

En el terminal, en la etapa 520, se recibe una instrucción de escritura del servidor, la instrucción de escritura que porta una clave de autenticación del dispositivo y la identificación del dispositivo ponible del usuario.

En el terminal, en la etapa 530, se ejecuta una operación de escritura de la clave de autenticación del dispositivo en un dispositivo ponible designado en la instrucción de escritura.

Una vez que el terminal recibe la instrucción de escritura del servidor, el terminal envía la clave de autenticación del dispositivo en la instrucción de escritura a un dispositivo ponible, para solicitarle que almacene la clave de autenticación del dispositivo. De acuerdo con un dispositivo ponible diferente y un permiso de configuración diferente del mismo, el dispositivo ponible puede completar el almacenamiento de la clave de autenticación del dispositivo solo después de que el usuario confirme la operación de escritura. Por ejemplo, para una pulsera, el usuario generalmente necesita tocar la pulsera para confirmar.

En el terminal, en la etapa 540, se envía un acuse de recibo de escritura al servidor, el acuse de recibo de escritura que porta un mensaje que indica si la clave de autenticación del dispositivo se ha escrito exitosamente. Después de completar la operación de escritura con el dispositivo ponible, el terminal encapsula un mensaje que indica si la clave de autenticación del dispositivo se escribió correctamente en un acuse de recibo de escritura y envía el acuse de recibo de escritura al servidor.

En el servidor, en la etapa 430, se recibe un acuse de recibo de escritura devuelto por el terminal, y si el acuse de recibo de escritura indica que la clave de autenticación del dispositivo se ha almacenado con éxito en un dispositivo ponible designado en la instrucción de escritura, se almacena una relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario, y el registro del dispositivo ponible se realiza exitosamente. Si el mensaje que se incluye en el acuse de recibo de escritura es que la

clave de autenticación del dispositivo no se ha escrito exitosamente, el proceso de registro falla. El servidor envía un resultado de registro al terminal.

El servidor puede requerir que el terminal proporcione una contraseña del usuario para mejorar la seguridad del registro del dispositivo ponible. Específicamente, el servidor recibe el acuse de recibo de escritura del terminal, y si el mensaje que se transmite en el acuse de recibo de escritura es que la clave de autenticación del dispositivo se ha almacenado exitosamente en el dispositivo ponible, el servidor emite una solicitud de confirmación de contraseña al terminal, para solicitar al terminal que proporcione una contraseña de la identificación del usuario correspondiente a la identificación del dispositivo ponible. El terminal recibe la solicitud de confirmación de contraseña del servidor y devuelve un acuse de recibo de confirmación de contraseña que porta una contraseña de usuario introducida por el usuario al servidor. El servidor recibe, desde el terminal, el acuse de recibo de confirmación de contraseña que porta la contraseña del usuario, y si la contraseña del usuario es correcta, almacena la relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario. El registro del dispositivo ponible se ha realizado exitosamente. Si la contraseña de usuario es incorrecta, la solicitud de registro del terminal se rechaza y el registro falla. El servidor envía un resultado de registro al terminal.

En una implementación, una clave pública de usuario y una clave privada de usuario del usuario pueden generarse automáticamente en el proceso de registro. Específicamente, después de que la operación de escritura de la clave de autenticación del dispositivo en el dispositivo ponible por parte del terminal sea exitosa, el terminal genera una clave pública de usuario y una clave privada de usuario del usuario de acuerdo con un algoritmo, almacena la clave privada de usuario generada localmente y encapsula la clave pública de usuario en un acuse de recibo de escritura y envía el acuse de recibo de escritura al servidor. Una vez que el terminal escribe correctamente la clave de autenticación del dispositivo en el dispositivo ponible o se verifica que la contraseña del usuario es correcta, el servidor almacena una relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible, la clave de autenticación del servidor y la clave pública de usuario del usuario.

En algunos escenarios de aplicación, una clave pública del servidor y una clave privada del servidor están preestablecidas en el servidor, y una clave privada del terminal y una clave pública del terminal están preestablecidas en el terminal, en donde la clave pública del servidor y la clave privada del terminal son un par de claves, y la clave privada del servidor y la clave pública del terminal son un par de claves. En estos escenarios, en la modalidad del método de autenticación, el servidor puede firmar la instrucción de detección utilizando la clave privada del servidor almacenada y enviar la instrucción de detección firmada al terminal. El terminal realiza la verificación de la firma en la instrucción de detección recibida utilizando la clave pública del terminal almacenada y rechaza la instrucción de detección si falla la verificación y, por lo tanto, falla la autenticación. En la modalidad del método de registro, el servidor puede firmar la instrucción de escritura utilizando la clave privada del servidor almacenada y enviar la instrucción de escritura firmada al terminal; el terminal realiza la verificación de la firma en la instrucción de escritura recibida utilizando la clave pública del terminal almacenada y rechaza la instrucción de escritura si falla la verificación y, por lo tanto, falla el registro. El terminal puede firmar el acuse de recibo de escritura utilizando la clave privada del terminal almacenada y enviar el acuse de recibo de escritura firmado al servidor; el servidor realiza la verificación de la firma en el acuse de recibo de escritura recibido utilizando la clave pública del servidor almacenada y rechaza la solicitud de registro del terminal si falla la verificación.

El servidor y el terminal pueden realizar la comunicación a través de un canal cifrado, para mejorar aún más la seguridad del registro del dispositivo ponible y la autenticación del usuario. Por ejemplo, la instrucción de detección y el acuse de recibo de detección en la modalidad del método de autenticación y la instrucción de escritura y el acuse de recibo de escritura en la modalidad del método de registro pueden transmitirse todos en un canal cifrado. Puede hacerse referencia a la técnica anterior para la implementación del canal cifrado y un método de cifrado adoptado, que no se repiten.

En una modalidad de la presente solicitud, un terminal de cliente de pago que se ejecuta en el terminal autentica la identidad de un usuario en un proceso de pago utilizando un dispositivo ponible conectado al terminal. Un proceso específico de esta modalidad es el siguiente:

En el dispositivo ponible, se recibe una solicitud de vinculación de pago del terminal de cliente de pago, la solicitud de vinculación de pago que incluye una clave de autenticación del dispositivo del dispositivo ponible. El dispositivo ponible almacena, en respuesta a la solicitud de vinculación de pago emitida por el usuario a través del terminal de cliente de pago, la clave de autenticación del dispositivo contenida en la solicitud de vinculación de pago en una memoria local.

Al realizar una operación de pago en el terminal de cliente de pago, el usuario selecciona el dispositivo ponible para realizar un pago, activa una respuesta del terminal de cliente de pago a la operación del usuario anterior y envía una solicitud de pago al servidor. La solicitud de pago porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario.

Después de recibir la solicitud de pago enviada por el usuario a través del terminal de cliente de pago, el servidor adquiere la información de autenticación de enlace descendente y emite al terminal de cliente de pago una instrucción

de autenticación que incluye la información de autenticación de enlace descendente y la identificación del dispositivo ponible.

El terminal de cliente de pago recibe la instrucción de autenticación emitida por el servidor y porta la información de autenticación de enlace descendente en la información de autenticación de pago y envía la información de autenticación de pago a un dispositivo ponible designado en la instrucción de autenticación.

El dispositivo ponible recibe la información de autenticación de pago enviada por el terminal de cliente de pago, extrae, de la información de autenticación de pago, la información de autenticación de enlace descendente emitida por el servidor en base a la solicitud de pago del usuario enviada por el terminal de cliente de pago; y genera la información de autenticación de enlace ascendente de acuerdo con la clave de autenticación del dispositivo almacenada y la información de autenticación de enlace descendente, y envía la información de autenticación de enlace ascendente al terminal de cliente de pago.

El terminal de cliente de pago recibe la información de autenticación de enlace ascendente devuelta por el dispositivo ponible y porta la información de autenticación de enlace ascendente en la información de respuesta de autenticación y envía la información de respuesta de autenticación al servidor.

El servidor recibe la información de respuesta de autenticación que porta la información de autenticación de enlace ascendente devuelta por el terminal de cliente de pago, hace coincidir la información de autenticación de enlace descendente con la información de autenticación de enlace ascendente mediante el uso de la clave de autenticación del servidor del usuario, en donde el usuario pasa la autenticación si la coincidencia tiene éxito y realiza una operación de pago después de que la autenticación sea exitosa. La clave de autenticación del servidor del usuario es la misma o corresponde a la clave de autenticación del dispositivo del dispositivo ponible designado en la instrucción de autenticación.

En esta modalidad, una clave de autenticación del servidor y una clave de autenticación del dispositivo que son iguales o se corresponden entre sí se establecen en un servidor y un dispositivo ponible, y el dispositivo ponible se autentica mediante el uso de la clave de autenticación del dispositivo y la clave de autenticación del servidor, completando de esta manera la autenticación de pago en un usuario correspondiente al dispositivo ponible, de modo que el usuario pueda realizar un pago en un terminal de cliente de pago utilizando el dispositivo ponible, y el usuario no necesita memorizar ninguna cuenta ni contraseña ni necesita introducir ninguna cuenta y ninguna contraseña durante la autenticación, lo que reduce la carga para el usuario y mejora la eficiencia del pago.

En un ejemplo de aplicación de la presente aplicación, después de registrar una pulsera con un servidor de pago a través de una aplicación (App) del terminal de cliente que se ejecuta en un terminal de teléfono móvil, el usuario puede completar el pago de la red a través de la pulsera sin introducir ninguna cuenta ni contraseña. Una clave pública de servidor y una clave privada de terminal en un par, así como también una clave privada del servidor y una clave pública del terminal en un par, están preestablecidas en el servidor de pago y la aplicación de terminal de cliente. En donde el servidor de pago puede ser un servidor que ejecuta un programa de terminal del servidor correspondiente a la aplicación de terminal de cliente, y también puede ser un servidor de una plataforma de pago de terceros que admita la aplicación de terminal de cliente. Un proceso específico es el siguiente:

Un usuario envía una solicitud de registro del dispositivo ponible a un servidor de pago a través de una aplicación de terminal de cliente (en adelante, terminal de cliente) que se ejecuta en un terminal de teléfono móvil, para solicitar la apertura del pago de pulsera, y el terminal de cliente carga una identificación de usuario (una cuenta del usuario en el servidor de pago), una identificación de terminal de teléfono móvil (un IMEI) y una identificación de pulsera (una dirección MAC de pulsera) en la solicitud de registro al servidor.

El servidor de pago genera, a través de un algoritmo predeterminado, una clave simétrica para autenticar una pulsera (es decir, una clave de autenticación del servidor y una clave de autenticación del dispositivo que son iguales), firma la clave simétrica, la identificación del usuario y la identificación de la pulsera juntas a través de una clave privada del servidor preestablecida, encapsula la clave simétrica firmada, la identificación del usuario y la identificación de la pulsera en una instrucción de escritura, y envía la instrucción de escritura al terminal de cliente a través de un canal cifrado entre el servidor de pago y el terminal de cliente.

Después de recibir la instrucción de escritura del terminal del servidor, el terminal de cliente primero verifica la validez de los datos en la instrucción de escritura de acuerdo con una clave pública del terminal preestablecida y rechaza directamente la instrucción de escritura si los datos no son válidos. Una vez que la verificación de validez tiene éxito, el terminal de cliente se conecta a una pulsera designada en la instrucción de escritura y, una vez que la conexión sea exitosa, escribe la clave simétrica emitida por el servidor de pago en la pulsera. En el proceso de escribir la clave simétrica en la pulsera, el usuario debe tocar la pulsera para confirmar la operación de escritura, y después de que el usuario toque la pulsera, la clave simétrica se escribe en un área de almacenamiento de la pulsera.

Una vez que la operación de escritura sea exitosa, el terminal de cliente genera un par de claves asimétricas de acuerdo con la identificación del usuario, es decir, una clave pública de usuario y una clave privada de usuario

correspondiente a la identificación del usuario. El terminal de cliente firma un resultado que indica si la operación de escritura es exitosa, la identificación de la pulsera y la clave pública de usuario generada a través de una clave privada del terminal preestablecida, encapsula la información firmada en un acuse de recibo de escritura y envía el acuse de recibo de escritura al servidor de pago a través de un canal encriptado. La clave privada del usuario se almacena localmente en el terminal de cliente.

Después de recibir el acuse de recibo de escritura del terminal de cliente, el servidor de pago verifica la firma del terminal de cliente a través de una clave pública de servidor preestablecida, y rechaza la solicitud de registro del terminal de cliente si la verificación falla. Una vez que la verificación de la firma tiene éxito, el servidor de pago emite una solicitud de confirmación de contraseña al terminal de cliente, para solicitar al terminal de cliente que proporcione una contraseña de una cuenta del usuario en el servidor de pago.

El terminal de cliente muestra al usuario información de solicitud de introducir una contraseña, y el usuario introduce la contraseña de su cuenta en el servidor de pago. El terminal de cliente envía un acuse de recibo de confirmación de contraseña que porta la contraseña recibida al servidor de pago.

El servidor de pago verifica la contraseña del usuario en el acuse de recibo de confirmación de la contraseña, después de que la verificación tiene éxito, almacena una relación correspondiente entre la clave simétrica (la clave de autenticación del servidor), la identificación del usuario, la identificación del teléfono móvil, la identificación de la pulsera y la clave pública de usuario generada por el terminal de cliente, y notifica al terminal de cliente que la pulsera se registró exitosamente. Finaliza el proceso de registro.

Una vez que la pulsera se registra con éxito en el servidor de pago, el usuario envía, cuando espera realizar un pago a través de la pulsera, una solicitud de autenticación de pago al servidor a través del terminal de cliente. La solicitud de autenticación incluye la información de un pedido a pagar, una identificación de usuario, una identificación de terminal de teléfono móvil y una identificación de pulsera.

Después de recibir la solicitud de autenticación del terminal de cliente, el servidor de pago compara la identificación del terminal del teléfono móvil en la solicitud de autenticación con la identificación del terminal del teléfono móvil en la relación correspondiente almacenada que corresponde a la identificación de la pulsera en la solicitud de autenticación. Si son diferentes, la solicitud de autenticación se rechaza y el pago falla. Si son iguales, el servidor de pago genera datos de texto sin formato aleatorios y utiliza los datos de texto sin formato como información de autenticación de enlace descendente. El servidor de pago firma la información de autenticación de enlace descendente, la identificación del usuario y la identificación de la pulsera mediante el uso de una clave privada del servidor preestablecida, los encapsula en una instrucción de detección y envía la instrucción de detección al terminal de cliente a través de un canal cifrado entre el servidor de pago y el terminal de cliente.

Después de recibir la instrucción de detección del servidor de pago, el terminal de cliente primero verifica la validez de los datos de la firma en la instrucción de detección de acuerdo con una clave pública del terminal preestablecida. Si los datos no son válidos, la instrucción de detección se rechaza y el pago falla. Una vez que la verificación de validez de la firma sea exitosa, el terminal de cliente se conecta a una pulsera designada en la instrucción de detección y, una vez que la conexión sea exitosa, envía la información de autenticación de enlace descendente en la instrucción de detección a la pulsera. La pulsera cifra la información de autenticación de enlace descendente utilizando la clave simétrica almacenada para generar información de autenticación de enlace ascendente y devuelve la información de autenticación de enlace ascendente al terminal de cliente. El proceso de cifrar la información de autenticación de enlace descendente mediante la pulsera no requiere que el usuario toque para confirmar, lo que puede reducir aún más las operaciones del usuario y optimizar las experiencias del usuario.

Después de recibir la información de autenticación de enlace ascendente generada por la pulsera, el terminal de cliente firma la información de autenticación de enlace ascendente utilizando una clave privada de usuario almacenada localmente, encapsula los datos firmados y la identificación de pulsera firmada en un acuse de recibo de detección y envía el acuse de recibo de detección al servidor de pago a través de un canal cifrado entre el terminal de cliente y el servidor de pago.

Después de recibir el acuse de recibo de detección cargado por el terminal de cliente, el servidor de pago puede realizar la verificación de la firma en el acuse de recibo de detección de acuerdo con la clave pública de usuario correspondiente a la identificación de la pulsera en el acuse de recibo de detección. Si la verificación de la firma falla, la solicitud de autenticación falla. Una vez que la verificación de la firma tiene éxito, el servidor de pago cifra la información de autenticación de enlace descendente utilizando una clave simétrica correspondiente a la identificación de la pulsera, compara los datos cifrados con la información de autenticación de enlace ascendente en el acuse de recibo de detección, es decir, compara si la información de autenticación de enlace descendente cifrada por el servidor de pago es el mismo que la información de autenticación de enlace descendente cifrada por la pulsera, y si son iguales, devuelve un mensaje de autenticación exitosa al terminal de cliente y continúa pagando un pedido. Si son diferentes, el servidor de pago devuelve un mensaje de autenticación fallida al terminal de cliente. Después de recibir el mensaje de autenticación exitosa, el terminal de cliente completa una operación de pago de la orden de usuario junto con el

servidor de pago. Si recibe el mensaje de autenticación incorrecta, el terminal de cliente notifica al usuario que este pago no se puede completar debido a una autenticación incorrecta.

En correspondencia con la implementación del proceso anterior, las modalidades de la presente solicitud proporcionan además un aparato para autenticar a un usuario aplicado a un servidor, un aparato para autenticar a un usuario aplicado a un terminal conectado a un dispositivo ponible del usuario, un aparato para registrar un dispositivo ponible aplicado a un servidor, un aparato para registrar un dispositivo ponible aplicado a un terminal, un aparato de pago aplicado a un servidor, un aparato de pago aplicado a un terminal y un aparato de pago aplicado a un dispositivo ponible. Todos estos aparatos pueden implementarse mediante software y también pueden implementarse mediante hardware o mediante una combinación de software y hardware. Tomando la implementación del software como ejemplo, se forma un aparato en un sentido lógico al leer una instrucción de programa informático correspondiente en una memoria a través de una CPU de un servidor, un terminal o un dispositivo ponible y al ejecutar la instrucción del programa informático. En términos del nivel de hardware, además de la CPU, la memoria y la memoria no volátil mostradas en la Figura 6, el terminal o dispositivo ponible donde se encuentra el aparato generalmente incluye además otro hardware, tal como un chip para enviar y recibir señales inalámbricas, y el servidor donde se encuentra el aparato generalmente incluye además otro hardware, tal como una tarjeta de placa para implementar una función de comunicación de red.

La Figura 7 muestra un aparato para autenticar a un usuario de acuerdo con esta modalidad. El aparato se aplica a un servidor y el servidor almacena una relación correspondiente entre una identificación de usuario, una identificación del dispositivo ponible y una clave de autenticación del servidor del usuario. El aparato incluye una unidad receptora de solicitud de autenticación, una unidad de emisión de instrucción de detección, una unidad receptora de acuse de recibo de detección y una unidad de coincidencia, en donde la unidad receptora de solicitud de autenticación está configurada para recibir una solicitud de autenticación enviada por el usuario a través de un terminal, la solicitud de autenticación que porta la identificación del usuario y/o la identificación del dispositivo ponible del usuario; la unidad de emisión de instrucciones de detección está configurada para adquirir información de autenticación de enlace descendente y emitir al terminal una instrucción de detección que porta la información de autenticación de enlace descendente y la identificación del dispositivo ponible del usuario; la unidad receptora de acuse de recibo de detección está configurada para recibir un acuse de recibo de detección, devuelto por el terminal, que porta la información de autenticación de enlace ascendente, la información de autenticación de enlace ascendente se genera, mediante un dispositivo ponible designado en la instrucción de detección, de acuerdo con una clave de autenticación del dispositivo y el enlace descendente la información de autenticación, y la clave de autenticación del dispositivo es la misma o corresponde a la clave de autenticación del servidor; y la unidad de coincidencia está configurada para hacer coincidir la información de autenticación de enlace descendente con la información de autenticación de enlace ascendente utilizando la clave de autenticación del servidor del usuario, en donde el usuario pasa la autenticación si la coincidencia tiene éxito.

Opcionalmente, el servidor almacena además una clave pública de usuario del usuario, la clave pública de usuario corresponde a la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario, y la clave pública de usuario y una clave privada del usuario almacenada en el terminal son un par de claves. El acuse de recibo de detección devuelto por el terminal se firma utilizando la clave privada del usuario almacenada en el terminal. El aparato incluye, además: una unidad de verificación de acuse de recibo de detección configurada para realizar la verificación de firma en el acuse de recibo de detección del terminal de acuerdo con la clave pública de usuario del usuario, en donde la autenticación del usuario falla si falla la verificación.

Opcionalmente, el servidor almacena además una identificación del terminal, y la identificación del terminal corresponde a la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario. La solicitud de autenticación incluye, además: una identificación de terminal para enviar la solicitud de autenticación. El aparato incluye, además: una unidad de verificación de identificación del terminal configurada para, cuando la identificación del terminal correspondiente a la identificación del usuario o la identificación del dispositivo ponible en la solicitud de autenticación es diferente de la identificación del terminal para enviar la solicitud de autenticación, verificar que la autenticación en el usuario falla.

Opcionalmente, el servidor almacena además una clave privada del servidor, y la clave privada del servidor y una clave pública del terminal almacenadas en el terminal son un par de claves; El aparato incluye, además: una unidad de firma de instrucciones de detección configurada para firmar la instrucción de detección utilizando la clave privada del servidor.

Opcionalmente, el servidor es un servidor de pago y la solicitud de autenticación es una solicitud de pago. El aparato incluye, además: una unidad de servicio de pago configurada para proporcionar un servicio de pago para un usuario que pasa la autenticación.

La Figura 8 muestra un aparato para autenticar a un usuario de acuerdo con esta modalidad. El aparato se aplica a un terminal conectado a un dispositivo ponible del usuario. El aparato incluye una unidad de envío de solicitud de autenticación, una unidad receptora de instrucciones de detección, una unidad de información de autenticación de enlace ascendente, una unidad de envío de acuse de recibo de detección y una unidad receptora de resultados de

autenticación, en donde la unidad de envío de solicitud de autenticación está configurada para enviar una solicitud de autenticación a un servidor de acuerdo con una operación del usuario, la solicitud de autenticación que porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario; la unidad receptora de instrucciones de detección está configurada para recibir una instrucción de detección del servidor, la instrucción de detección que porta la información de autenticación de enlace descendente y la identificación del dispositivo ponible; la unidad de información de autenticación de enlace ascendente está configurada para enviar la información de autenticación de enlace descendente a un dispositivo ponible designado en la instrucción de detección y recibir la información de autenticación de enlace ascendente devuelta por el dispositivo ponible; la información de autenticación de enlace ascendente se genera por el dispositivo ponible de acuerdo con una clave de autenticación del dispositivo almacenada y la información de autenticación de enlace descendente, la clave de autenticación del dispositivo es la misma o correspondiente a una clave de autenticación del servidor almacenada en el servidor; la unidad de envío de acuse de recibo de detección está configurada para enviar al servidor un acuse de recibo de detección que porta la información de autenticación de enlace ascendente; y la unidad receptora de resultados de autenticación está configurada para recibir un resultado de autenticación de usuario determinado por el servidor de acuerdo con la información de autenticación de enlace ascendente, la información de autenticación de enlace descendente y la clave de autenticación del servidor.

Opcionalmente, el terminal almacena una clave privada de usuario del usuario, y la clave privada de usuario y una clave pública de usuario almacenada en el servidor son un par de claves. El aparato incluye, además: una unidad de firma de acuse de recibo de detección configurada para firmar el acuse de recibo de detección utilizando la clave privada de usuario del usuario.

Opcionalmente, el terminal almacena una clave pública del terminal, y la clave pública del terminal y una clave privada del servidor almacenadas en el servidor son un par de claves. La instrucción de detección emitida por el servidor se firma utilizando la clave privada del servidor. El aparato incluye, además: una unidad de verificación de instrucción de detección configurada para realizar la verificación de firma en la instrucción de detección del servidor de acuerdo con la clave pública del terminal, y rechazar la instrucción de detección si falla la verificación.

Opcionalmente, la solicitud de autenticación es una solicitud de pago, y el terminal completa una operación de pago del usuario después de que el resultado de la autenticación del usuario es que la autenticación sea exitosa.

La Figura 9 muestra un aparato para registrar un dispositivo ponible de acuerdo con esta modalidad. El aparato se aplica a un servidor. Cuando se divide en términos de funciones, el aparato incluye además una unidad receptora de solicitud de registro, una unidad de emisión de instrucción de escritura y una unidad receptora de acuse de recibo de escritura, en donde la unidad receptora de solicitud de registro está configurada para recibir una solicitud de registro del dispositivo ponible enviada por un usuario a través de un terminal, la solicitud de registro que porta una identificación de usuario y una identificación del dispositivo ponible del usuario; la unidad de emisión de instrucciones de escritura está configurada para adquirir una clave de autenticación del servidor del usuario y una clave de autenticación del dispositivo, y emitir al terminal una instrucción de escritura que porta la clave de autenticación del dispositivo y la identificación del dispositivo ponible del usuario; y la unidad receptora de acuse de recibo de escritura está configurada para recibir un acuse de recibo de escritura devuelto por el terminal, y si el acuse de recibo de escritura indica que la clave de autenticación del dispositivo se ha almacenado con éxito en un dispositivo ponible designado en la instrucción de escritura, almacena una relación correspondiente entre el usuario identificación, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario.

Opcionalmente, la unidad receptora de acuse de recibo de escritura incluye: un módulo de emisión de solicitud de confirmación de contraseña configurado para emitir una solicitud de confirmación de contraseña al terminal cuando el acuse de recibo de escritura indica que la clave de autenticación del dispositivo se ha almacenado con éxito en el dispositivo ponible designado en la instrucción de escritura; y un módulo de recepción de acuse de recibo de confirmación de contraseña configurado para recibir, desde el terminal, un acuse de recibo de confirmación de contraseña que porta una contraseña de usuario, y si la contraseña de usuario es correcta, almacenar la relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y el servidor clave de autenticación del usuario.

Opcionalmente, el acuse de recibo de escritura devuelto por el terminal incluye además una clave pública de usuario generada por el terminal; y la unidad receptora de acuse de recibo de confirmación de contraseña está configurada específicamente para: recibir, desde el terminal, un acuse de recibo de confirmación de contraseña que porta una contraseña de usuario, y si la contraseña de usuario es correcta, almacenar una relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible, la clave de autenticación del servidor y la clave pública de usuario del usuario.

Opcionalmente, el servidor almacena además una clave privada del servidor y una clave pública de servidor. La clave privada del servidor y una clave pública del terminal almacenadas en el terminal son un par de claves; y la clave pública del servidor y una clave privada del terminal almacenadas en el terminal son un par de claves. El aparato incluye, además: una unidad de firma de instrucciones de escritura configurada para firmar la instrucción de escritura utilizando la clave privada del servidor. El aparato incluye, además: una unidad de verificación de acuse de recibo de escritura

configurada para realizar la verificación de firma en el acuse de recibo de escritura del terminal utilizando la clave pública del servidor y rechazar la solicitud de registro si la verificación falla.

La Figura 10 muestra un aparato para registrar un dispositivo ponible de acuerdo con esta modalidad. El aparato se aplica a un terminal. Al dividir en términos de funciones, el aparato incluye además una unidad de envío de solicitud de registro, una unidad receptora de instrucción de escritura, una unidad de ejecución de operación de escritura y una unidad de envío de acuse de recibo de escritura, en donde la unidad de envío de solicitud de registro está configurada para enviar una solicitud de registro del dispositivo ponible a un servidor de acuerdo con una operación de un usuario, la solicitud de registro que porta una identificación de usuario y una identificación del dispositivo ponible del usuario; la unidad receptora de instrucciones de escritura está configurada para recibir una instrucción de escritura del servidor, la instrucción de escritura porta una clave de autenticación del dispositivo y la identificación del dispositivo ponible del usuario; la unidad de ejecución de la operación de escritura está configurada para ejecutar una operación de escritura de la clave de autenticación del dispositivo en un dispositivo ponible designado en la instrucción de escritura; y la unidad de envío de acuse de recibo de escritura está configurada para enviar un acuse de recibo de escritura al servidor, el acuse de recibo de escritura que porta un mensaje que indica si la clave de autenticación del dispositivo se ha escrito exitosamente.

Opcionalmente, el aparato incluye además una unidad receptora de solicitud de confirmación de contraseña configurada para, después de que se envía el acuse de recibo de escritura al servidor, recibir una solicitud de confirmación de contraseña del servidor y devolver al servidor un acuse de recibo de confirmación de contraseña que porta una contraseña de usuario introducida por el usuario.

Opcionalmente, el aparato incluye además una unidad de generación de clave de usuario configurada para, después de que la operación de escritura de la clave de autenticación del dispositivo sea exitosa, generar una clave privada de usuario y una clave pública de usuario del usuario, y almacenar la clave privada de usuario; y el acuse de recibo de escritura porta además la clave pública de usuario del usuario.

Opcionalmente, el terminal almacena una clave pública del terminal y una clave privada de terminal. La clave pública del terminal y una clave privada del servidor almacenada en el servidor son un par de claves; y la clave privada del terminal y una clave pública del servidor almacenadas en el servidor son un par de claves. El aparato incluye, además: una unidad de verificación de la instrucción de escritura configurada para realizar la verificación de la firma en la instrucción de escritura del servidor utilizando la clave pública del terminal y rechazar la instrucción de escritura si falla la verificación. El aparato incluye, además: una unidad de firma de acuse de recibo de escritura configurada para firmar el acuse de recibo de escritura utilizando la clave privada del terminal.

Una modalidad de la presente solicitud proporciona un aparato de pago aplicado a un servidor. Al dividir en términos de funciones, el aparato incluye una unidad receptora de solicitud de pago, una unidad de emisión de instrucción de autenticación, una unidad receptora de respuesta de autenticación y una unidad de coincidencia de pago, en donde la unidad receptora de solicitud de pago está configurada para recibir una solicitud de pago enviada por un usuario a través de un terminal de cliente de pago, la solicitud de pago que porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario; la unidad de emisión de instrucciones de autenticación está configurada para adquirir información de autenticación de enlace descendente y emitir al terminal de cliente de pago una instrucción de autenticación que incluye la información de autenticación de enlace descendente y la identificación del dispositivo ponible; la unidad receptora de respuesta de autenticación está configurada para recibir la información de respuesta de autenticación, devuelta por el terminal de cliente de pago, que porta la información de autenticación de enlace ascendente, la información de autenticación de enlace ascendente se genera, mediante un dispositivo ponible designado en la instrucción de autenticación, de acuerdo con una clave de autenticación del dispositivo y la información de autenticación de enlace descendente y la clave de autenticación del dispositivo es la misma o correspondiente a una clave de autenticación del servidor; y la unidad de coincidencia de pago está configurada para hacer coincidir la información de autenticación de enlace descendente con la información de autenticación de enlace ascendente utilizando la clave de autenticación del servidor del usuario, en donde el usuario pasa la autenticación si la coincidencia tiene éxito, y se lleva a cabo una operación de pago después de que la autenticación sea exitosa.

Opcionalmente, la solicitud de pago se activa mediante información que selecciona el usuario en el terminal de cliente de pago e indica que se realiza un pago mediante un dispositivo ponible.

Una modalidad de la presente solicitud proporciona un aparato de pago, aplicado a un terminal. Al dividir en términos de funciones, el aparato incluye una unidad de envío de solicitud de pago, una unidad receptora de instrucciones de autenticación y una unidad de envío de respuesta de autenticación, en donde la unidad de envío de solicitud de pago está configurada para enviar una solicitud de pago a un servidor en respuesta a una operación de pago de un usuario en un terminal de cliente de pago, la solicitud de pago que porta una identificación de usuario y/o una identificación del dispositivo ponible del usuario; la unidad receptora de instrucciones de autenticación está configurada para recibir una instrucción de autenticación, emitida por el servidor, que incluye la información de autenticación de enlace descendente y la identificación del dispositivo ponible, y envía la información de autenticación de enlace descendente a un dispositivo ponible, de modo que el dispositivo ponible genera la información de autenticación de enlace ascendente mediante el uso de una clave de autenticación del dispositivo almacenada por el dispositivo ponible y la

información de autenticación de enlace descendente; y la unidad de envío de respuesta de autenticación está configurada para recibir la información de autenticación de enlace ascendente devuelta por el dispositivo ponible y enviar la información de autenticación de enlace ascendente al servidor, de modo que el servidor autentica al usuario de acuerdo con la información de autenticación de enlace ascendente y realiza una operación de pago después de la autenticación sea exitosa.

Opcionalmente, la operación de pago del usuario en el terminal de cliente de pago es específicamente una operación que es seleccionada por el usuario e indica la modalidad de un pago mediante un dispositivo ponible.

Una modalidad de la presente solicitud proporciona un aparato de pago para un dispositivo ponible, aplicado al dispositivo ponible. Al dividir en términos de funciones, el aparato de pago incluye una unidad receptora de información de autenticación de pago y una unidad de generación de información de autenticación de enlace ascendente, en donde la unidad receptora de información de autenticación de pago está configurada para recibir la información de autenticación de pago enviada por un terminal de cliente de pago, la información de autenticación de pago que incluye la información de autenticación de enlace descendente emitida por un servidor en base a una solicitud de pago de un usuario enviada por el terminal de cliente de pago; y la unidad de generación de información de autenticación de enlace ascendente está configurada para generar información de autenticación de enlace ascendente de acuerdo con una clave de autenticación del dispositivo almacenada y la información de autenticación de enlace descendente, y enviar la información de autenticación de enlace ascendente al terminal de cliente de pago, de modo que el terminal de cliente de pago envía la información de autenticación de enlace ascendente al servidor, de modo que el servidor pueda autenticar al usuario en base a la información de autenticación de enlace ascendente y realizar una operación de pago después de que la autenticación sea exitosa.

Opcionalmente, el aparato incluye, además: una unidad de vinculación de pago configurada para almacenar, en respuesta a una solicitud de vinculación de pago emitida por el usuario a través del terminal de cliente de pago, una clave de autenticación del dispositivo incluida en la solicitud de vinculación de pago.

Lo anterior son simplemente modalidades preferidas de la presente solicitud, que no se usan para limitar la presente solicitud.

En una configuración típica, el dispositivo informático incluye uno o más procesadores (CPU), una interfaz de entrada/salida, una interfaz de red y una memoria.

La memoria puede incluir una memoria volátil, una memoria de acceso aleatorio (RAM) y/o una memoria no volátil o similar en un medio legible por ordenador, por ejemplo, una memoria de solo lectura (ROM) o una RAM flash. La memoria es un ejemplo del medio legible por ordenador.

El medio legible por ordenador incluye medios no volátiles o volátiles, y medios móviles o no móviles, y puede implementar el almacenamiento de información por medio de cualquier método o tecnología. La información puede ser una instrucción legible por ordenador, una estructura de datos y un módulo de un programa u otros datos. Un medio de almacenamiento de un ordenador incluye, por ejemplo, pero no se limita a, una memoria de cambio de fase (PRAM), una memoria estática de acceso aleatorio (SRAM), una memoria dinámica de acceso aleatorio (DRAM), otros tipos de memorias de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable eléctricamente (EEPROM), una memoria flash u otras tecnologías de memoria, una memoria de solo lectura de disco compacto (CD-ROM), un disco versátil digital (DVD) u otros almacenamientos ópticos, una cinta de casete, una cinta magnética/almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio sin transmisión, y pueden usarse para almacenar información accesible al dispositivo informático. De acuerdo con la definición en este texto, el medio legible por ordenador no incluye medios transitorios, tal como una señal de datos modulada y una portadora.

Debe observarse además que, los términos "incluir", "comprender" o cualquier variante de los mismos están destinados a cubrir una inclusión no exclusiva, de modo que un proceso, un método, un producto o un dispositivo que incluya una serie de elementos no solo incluye tales elementos, sino que también incluye otros elementos no especificados expresamente, o puede incluir además elementos inherentes del proceso, método, producto o dispositivo. Sin más restricciones, un elemento limitado por la frase "incluye un/una..." no excluye otros elementos iguales existentes en el proceso, método, producto o dispositivo que incluye el elemento.

Los expertos en la técnica deben comprender que las modalidades de la presente solicitud pueden proporcionarse como un método, un sistema o un producto de programa informático. Por lo tanto, la presente solicitud puede implementarse en forma de una modalidad de hardware completa, una modalidad de software completa o una modalidad que combina software y hardware. Además, la presente solicitud puede emplear la forma de un producto de programa informático implementado en uno o más medios de almacenamiento utilizables por ordenador (que incluyen, pero no se limitan a, una memoria de disco magnético, un CD-ROM, una memoria óptica y similares) que incluyen código de programa utilizable por ordenador.

**REIVINDICACIONES**

1. Un método para autenticar a un usuario, llevado a cabo en un servidor, en donde el servidor almacena una relación correspondiente entre una identificación de usuario de un usuario, una identificación del dispositivo ponible de un dispositivo ponible del usuario y una clave de autenticación del servidor del usuario, el método que comprende:
recibir una solicitud del usuario en un terminal para un servicio, desde el servidor, que requiere autenticación de identidad;
recibir una solicitud de autenticación enviada por el terminal de acuerdo con una operación del usuario, la solicitud de autenticación que porta la identificación del usuario y/o la identificación del dispositivo ponible (210);
adquirir información de autenticación de enlace descendente y emitir al terminal una instrucción de detección que porta la información de autenticación de enlace descendente y la identificación del dispositivo ponible del usuario (220);
recibir un acuse de recibo de detección, devuelto por el terminal, que porta la información de autenticación de enlace ascendente, la información de autenticación de enlace ascendente que se genera, por un dispositivo ponible designado en la instrucción de detección, de acuerdo con una clave de autenticación del dispositivo y la información de autenticación de enlace descendente, y la clave de autenticación del dispositivo que es la misma o corresponde a la clave de autenticación del servidor (230);
hacer coincidir la información de autenticación de enlace descendente con la información de autenticación de enlace ascendente utilizando la clave de autenticación del servidor del usuario, para determinar un resultado de autenticación de usuario para el usuario, en donde el usuario pasa la autenticación si la coincidencia tiene éxito (240);
enviar, al terminal, el resultado de la autenticación del usuario; y
realizar el servicio solicitado para el usuario en el terminal si el usuario pasa la autenticación.

2. El método de acuerdo con la reivindicación 1, en donde el servidor almacena además una clave pública de usuario del usuario, la clave pública de usuario corresponde a la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario, y la clave pública de usuario y una clave privada del usuario almacenada en el terminal son un par de claves;
el acuse de recibo de detección devuelto por el terminal se firma utilizando la clave privada del usuario almacenada en el terminal; y
el método comprende, además:
realizar la verificación de la firma en el acuse de recibo de detección del terminal de acuerdo con la clave pública de usuario del usuario, en donde la autenticación del usuario falla si falla la verificación.

3. El método de acuerdo con la reivindicación 1, en donde el servidor almacena además una identificación de terminal, y la identificación de terminal corresponde a la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario;
la solicitud de autenticación comprende, además:
una identificación de terminal para enviar la solicitud de autenticación; y
el método comprende, además:
si la identificación del terminal correspondiente a la identificación del usuario o la identificación del dispositivo ponible en la solicitud de autenticación es diferente de la identificación del terminal para enviar la solicitud de autenticación, la autenticación del usuario falla.

4. El método de acuerdo con cualquiera de las reivindicaciones 1 a 3, en donde el servidor almacena además una clave privada del servidor, y la clave privada del servidor y una clave pública del terminal almacenada en el terminal son un par de claves; y
el método comprende, además:
firmar la instrucción de detección utilizando la clave privada del servidor.

5. El método de acuerdo con cualquiera de las reivindicaciones 1 a 3, en donde la instrucción de detección y el acuse de recibo de detección se transmiten a través de un canal cifrado entre el servidor y el terminal.

6. El método de acuerdo con cualquiera de las reivindicaciones 1 a 3, en donde el servidor es un servidor de pago y la solicitud de autenticación es una solicitud de pago; y
el método comprende, además:
proporcionar un servicio de pago para un usuario que pasa la autenticación.

7. El método de acuerdo con cualquiera de las reivindicaciones 1 a 6, que comprende además registrar el dispositivo ponible, que comprende:
recibir una solicitud de registro del dispositivo ponible enviada por el terminal de acuerdo con una operación del usuario, la solicitud de registro que porta una identificación de usuario y una identificación del dispositivo ponible del usuario (410);

adquirir una clave de autenticación del servidor del usuario y una clave de autenticación del dispositivo, y emitir al terminal una instrucción de escritura que porta la clave de autenticación del dispositivo y la identificación del dispositivo ponible del usuario (420); y
recibir un acuse de recibo de escritura devuelto por el terminal, y si el acuse de recibo de escritura indica que la clave de autenticación del dispositivo se ha almacenado con éxito en un dispositivo ponible designado en la instrucción de escritura, almacenar una relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario (430).

8. El método de acuerdo con la reivindicación 7, en donde almacenar una relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario comprende:
emitir una solicitud de confirmación de contraseña al terminal; y
recibir, desde el terminal, un acuse de recibo de confirmación de contraseña que porta una contraseña de usuario, y si la contraseña de usuario es correcta, almacenar la relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario.

9. El método de acuerdo con la reivindicación 7 u 8, en donde el acuse de recibo de escritura devuelto por el terminal comprende además una clave pública de usuario generada por el terminal; y
el almacenamiento de una relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible y la clave de autenticación del servidor del usuario comprende, además:
almacenar una relación correspondiente entre la identificación del usuario, la identificación del dispositivo ponible, la clave de autenticación del servidor y la clave pública de usuario del usuario.

10. El método de acuerdo con la reivindicación 7 u 8, en donde el servidor almacena además una clave privada del servidor y una clave pública de servidor;
la clave privada del servidor y una clave pública del terminal almacenada en el terminal son un par de claves; y
la clave pública del servidor y una clave privada del terminal almacenadas en el terminal son un par de claves;
el método comprende, además:
firmar la instrucción de escritura utilizando la clave privada del servidor; y
el método comprende, además:
realizar la verificación de la firma en el acuse de recibo de escritura del terminal utilizando la clave pública del servidor y rechazar la solicitud de registro si falla la verificación.

11. Un método para autenticar a un usuario, llevado a cabo en un terminal conectado a un dispositivo ponible del usuario, el método que comprende:
enviar una solicitud del usuario en el terminal para un servicio, desde un servidor, que requiere autenticación de identidad;
enviar una solicitud de autenticación al servidor de acuerdo con una operación del usuario, la solicitud de autenticación que porta una identificación de usuario y/o una identificación de dispositivo ponible del dispositivo ponible del usuario (310);
recibir una instrucción de detección del servidor, la instrucción de detección que porta la información de autenticación de enlace descendente y la identificación del dispositivo ponible (320);
enviar la información de autenticación de enlace descendente al dispositivo ponible designado en la instrucción de detección y recibir la información de autenticación de enlace ascendente devuelta por el dispositivo ponible;
la información de autenticación de enlace ascendente que se genera por el dispositivo ponible de acuerdo con una clave de autenticación del dispositivo almacenada y la información de autenticación de enlace descendente, y la clave de autenticación del dispositivo que es la misma o corresponde a una clave de autenticación del servidor almacenada en el servidor (330);
enviar al servidor un acuse de recibo de detección que porta la información de autenticación de enlace ascendente (340);
autenticar al usuario, que incluye la recepción de un resultado de autenticación de usuario determinado por el servidor de acuerdo con la información de autenticación de enlace ascendente, la información de autenticación de enlace descendente y la clave de autenticación del servidor (350); y
ejecutar operaciones del servicio solicitado en el terminal para el usuario si el usuario pasa la autenticación.

12. El método de acuerdo con la reivindicación 11, en donde el terminal almacena una clave privada de usuario del usuario, y la clave privada de usuario y una clave pública de usuario almacenada en el servidor son un par de claves; y
el método comprende, además:
firmar el acuse de recibo de detección mediante el uso de la clave privada de usuario del usuario.

13. El método de acuerdo con la reivindicación 11 o 12, en donde el terminal almacena una clave pública del terminal, y la clave pública del terminal y una clave privada del servidor almacenadas en el servidor son un par de claves;
la instrucción de detección emitida por el servidor se firma utilizando la clave privada del servidor; y

el método comprende, además:
realizar la verificación de la firma en la instrucción de detección del servidor de acuerdo con la clave pública del terminal, y rechazar la instrucción de detección si la verificación falla.

14. El método de acuerdo con la reivindicación 11 o 12, en donde la solicitud de autenticación es una solicitud de pago, y el terminal completa una operación de pago del usuario después de que el resultado de la autenticación del usuario es que la autenticación es exitosa.

15. El método de acuerdo con una cualquiera de las reivindicaciones 11 a 14, que comprende además registrar el dispositivo ponible, que comprende:
enviar una solicitud de registro del dispositivo ponible a un servidor de acuerdo con una operación de un usuario, la solicitud de registro que porta una identificación de usuario y una identificación del dispositivo ponible del usuario (510);
recibir una instrucción de escritura del servidor, la instrucción de escritura que porta una clave de autenticación del dispositivo y la identificación del dispositivo ponible del usuario (520);
ejecutar una operación de escritura de la clave de autenticación del dispositivo en un dispositivo ponible designado en la instrucción de escritura (530); y
enviar un acuse de recibo de escritura al servidor, el acuse de recibo de escritura que porta un mensaje que indica si la clave de autenticación del dispositivo se ha escrito correctamente (540).

16. El método de acuerdo con la reivindicación 15, en donde el método comprende, además:
después de que se envía el acuse de recibo de escritura al servidor, recibir una solicitud de confirmación de contraseña del servidor y devolver al servidor un acuse de recibo de confirmación de contraseña que porta una contraseña de usuario introducida por el usuario.

17. El método de acuerdo con la reivindicación 15 o 16, en donde el método comprende, además:
después de que la operación de escritura de la clave de autenticación del dispositivo es exitosa, generar una clave privada de usuario y una clave pública de usuario del usuario, y almacenar la clave privada de usuario; y el acuse de recibo de escritura porta además la clave pública de usuario del usuario.

18. El método de acuerdo con la reivindicación 15 o 16, en donde el terminal almacena una clave pública del terminal y una clave privada del terminal;
la clave pública del terminal y una clave privada del servidor almacenadas en el servidor son un par de claves; y
la clave privada del terminal y una clave pública del servidor almacenadas en el servidor son un par de claves;
el método comprende, además:
realizar la verificación de la firma en la instrucción de escritura del servidor utilizando la clave pública del terminal, y rechazar la instrucción de escritura si falla la verificación; y
el método comprende, además:
firmar el acuse de recibo de escritura utilizando la clave privada del terminal.

19. Un aparato para autenticar a un usuario y registrar un dispositivo ponible para un servidor, en donde el servidor almacena una relación correspondiente entre una identificación de usuario, una identificación del dispositivo ponible y una clave de autenticación del servidor del usuario, el aparato que comprende múltiples módulos configurados para llevar a cabo cualquiera de las reivindicaciones 1-10.

20. Un aparato para autenticar a un usuario y registrar un dispositivo ponible para un terminal conectado a un dispositivo ponible del usuario, en donde el aparato comprende múltiples módulos configurados para llevar a cabo cualquiera de las reivindicaciones 11 - 18.

**Dibujos**

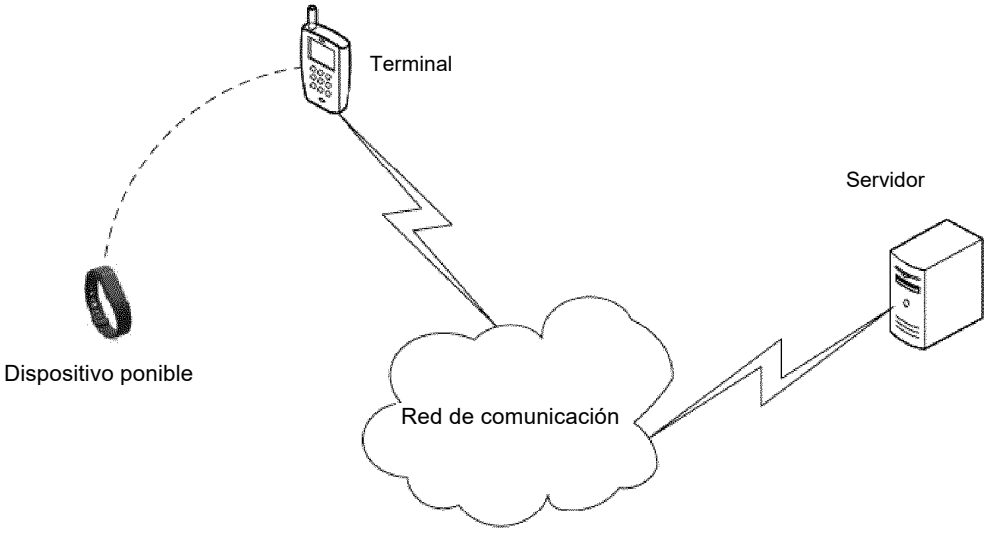


**FIGURA 1**

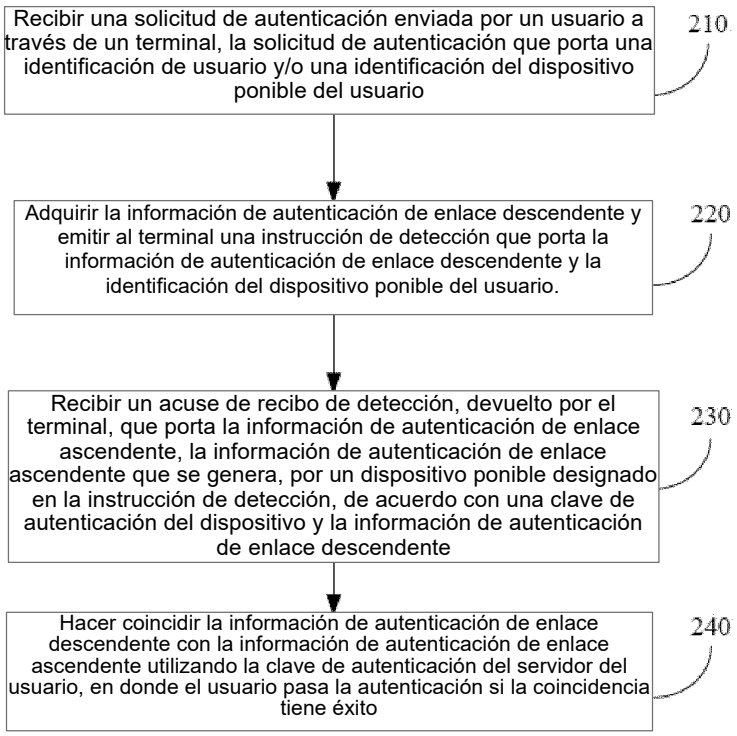


**FIGURA 2**

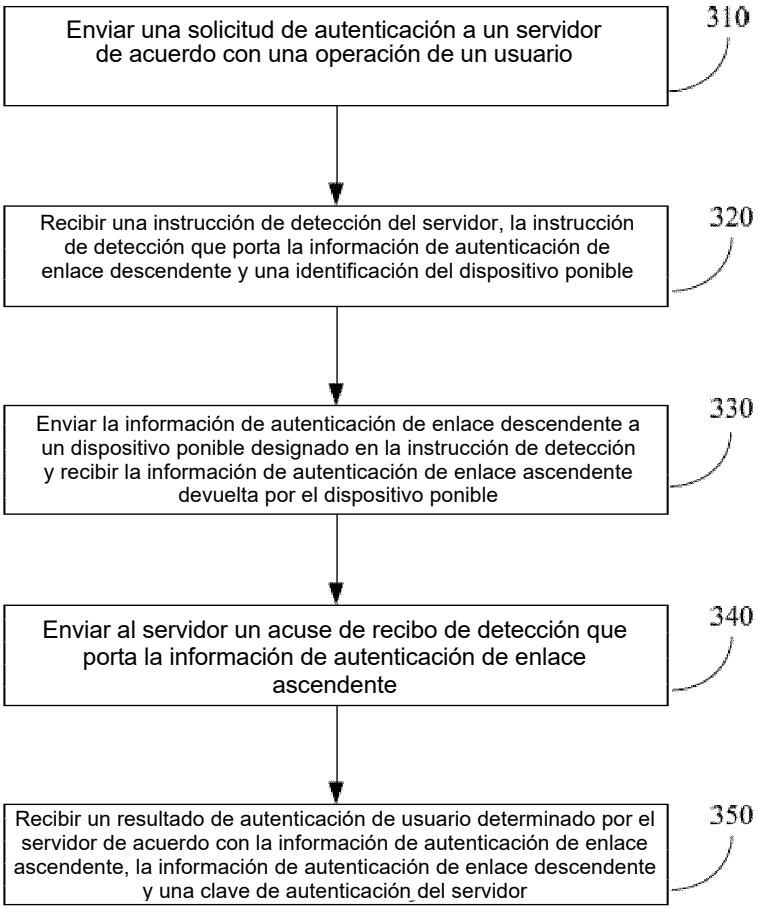


**FIGURA 3**

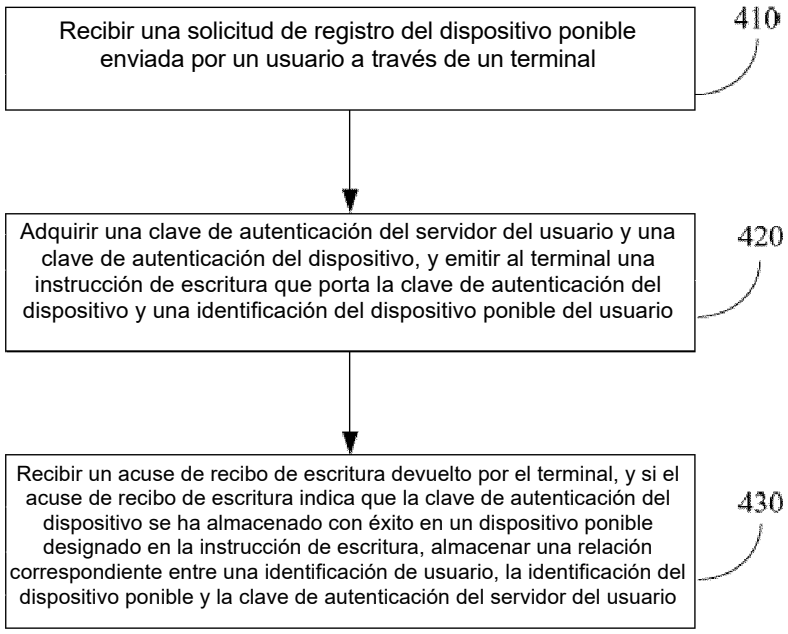


**FIGURA 4**

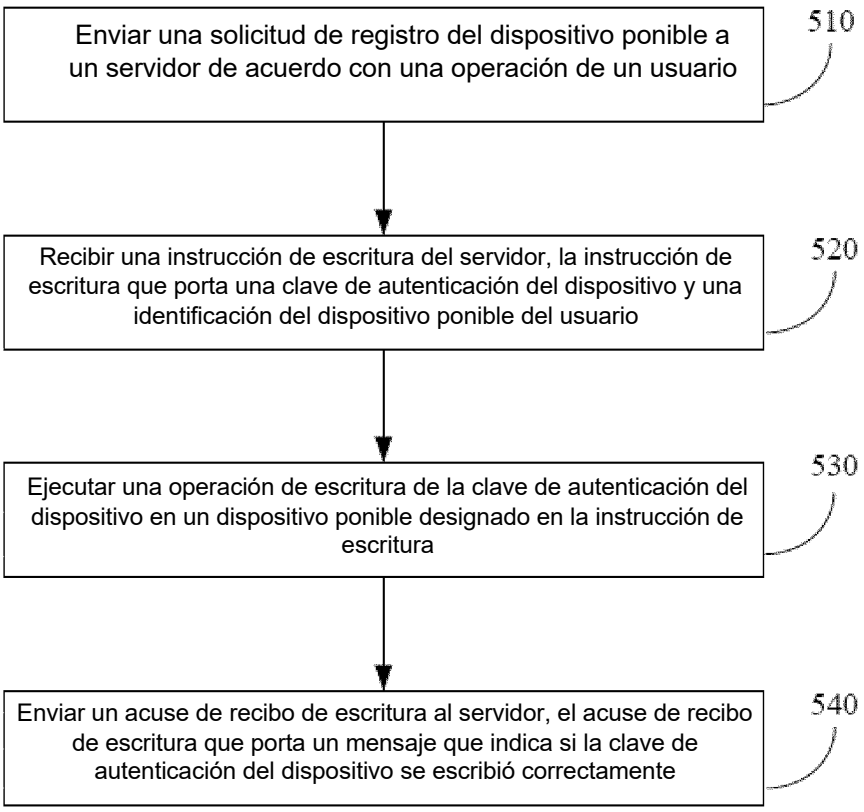


**FIGURA 5**

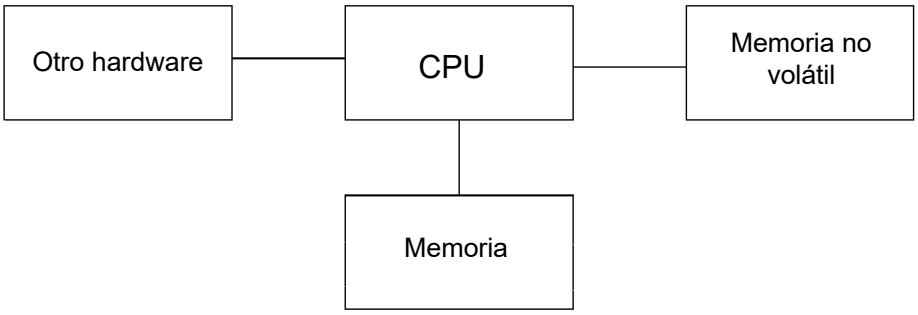


**FIGURA 6**

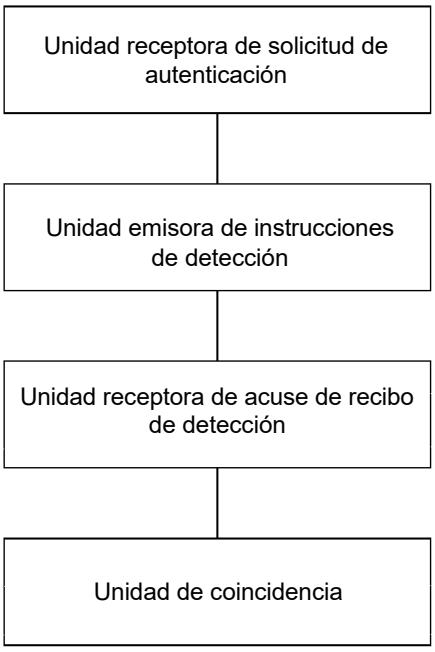


**FIGURA 7**

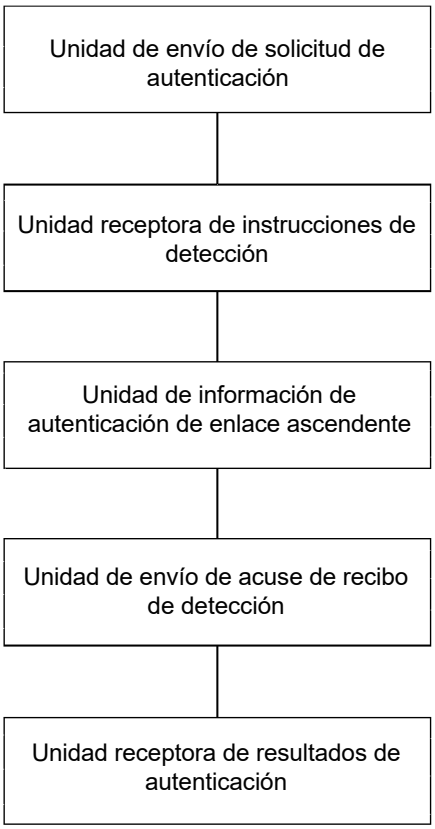


**FIGURA 8**

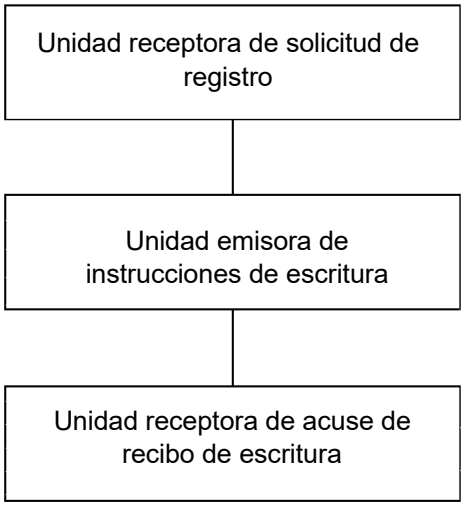


**FIGURA 9**

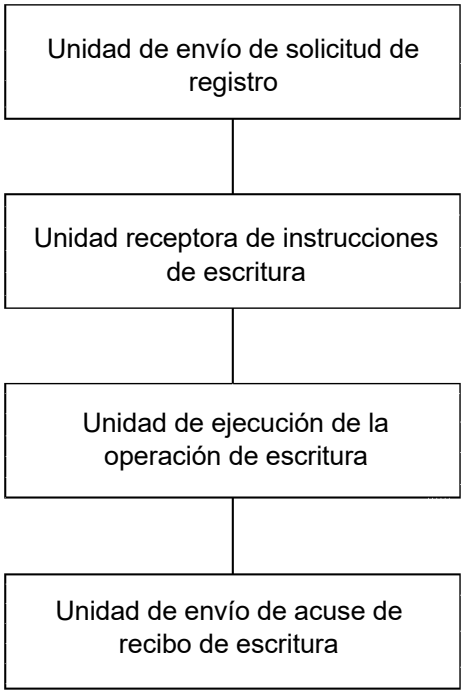


**FIGURA 10**