

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 767 601**

51 Int. Cl.:

**H04W 12/02** (2009.01)

**H04W 8/24** (2009.01)

**H04M 1/725** (2006.01)

**H04W 12/12** (2009.01)

**H04W 4/14** (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **21.12.2012 PCT/CN2012/087166**

87 Fecha y número de publicación internacional: **26.06.2014 WO14094300**

96 Fecha de presentación y número de la solicitud europea: **21.12.2012 E 12890187 (3)**

97 Fecha y número de publicación de la concesión europea: **20.11.2019 EP 2849468**

54 Título: **Servidor y procedimiento para el control remoto del funcionamiento de un terminal de comunicación, y un terminal de comunicación**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**18.06.2020**

73 Titular/es:  
**HUAWEI TECHNOLOGIES CO., LTD (100.0%)  
Huawei Administration Building, Bantian,  
Longgang District  
Shenzhen, Guangdong 518129, CN**

72 Inventor/es:  
**FENG, YAXIA**

74 Agente/Representante:  
**PONS ARIÑO, Ángel**

ES 2 767 601 T3

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

## DESCRIPCIÓN

Servidor y procedimiento para el control remoto del funcionamiento de un terminal de comunicación, y un terminal de comunicación

5

### CAMPO TÉCNICO

La presente invención se refiere al campo técnico de las comunicación y, en particular, a un servidor y a un procedimiento para el control remoto del funcionamiento de un terminal de comunicación y un terminal de comunicación.

10

### ANTECEDENTES

Recientemente, los terminales de comunicación (como los teléfonos móviles) de las personas se pierden de vez en cuando y, por lo tanto, cómo controlar oportuna y efectivamente el funcionamiento de un teléfono móvil para garantizar la seguridad de la información personal es el problema más difícil para cada propietario. Por ejemplo, cómo obtener un mensaje de servicio de mensajes cortos (SMS) en un teléfono móvil perdido, cómo bloquear una pantalla del teléfono móvil para proteger la seguridad de los datos del teléfono móvil y cómo adquirir un número de teléfono móvil actual del teléfono móvil perdido (es decir, el ladrón cambia una tarjeta inmediatamente después de tomar el teléfono móvil). Las soluciones técnicas de un usuario para controlar el funcionamiento de un teléfono móvil perdido han existido en la técnica anterior.

15

20

Por ejemplo, en una solución técnica 1, se inserta una tarjeta SIM de un número original en un aparato de hardware de monitoreo de mensajes SMS, un mensaje SMS enviado al número puede transferirse automáticamente a un nuevo número designado, y después de que el nuevo número reciba el mensaje SMS, un remitente del mensaje SMS sigue siendo un número de un remitente original del mensaje SMS. El mensaje SMS se recibe usando un monitor de mensajes SMS, y el monitor de mensajes SMS analiza el mensaje SMS para adquirir información, como el contenido del mensaje SMS y un número de llamada, en el mensaje SMS, encapsula la información como el contenido del mensaje SMS, el número de llamada y un identificador de la parte llamada, y luego envía la información encapsulada a una plataforma de reenvío de mensajes SMS. La plataforma de reenvío de mensajes SMS analiza un paquete encapsulado enviado por el monitor de mensajes SMS, agrega un identificador de transferencia y luego encapsula el paquete en un paquete de datos de mensajes SMS, y envía el paquete de datos de mensajes SMS utilizando un número de una parte de reenvío como número de una parte llamada y un número de una parte llamante original del mensaje SMS como un número de una parte llamante.

25

30

35

Sin embargo, la solución técnica 1 tiene los siguientes problemas: cuando un usuario tiene la intención de implementar el reenvío de mensajes SMS, la tarjeta SIM del mismo debe insertarse en el hardware del monitor de mensajes SMS, de modo que el problema técnico de que «un mensaje SMS de un teléfono móvil perdido no puede reenviarse a un número de teléfono móvil designado» no puede resolverse, y el problema técnico de que «no se puede obtener un número de teléfono móvil actual del teléfono móvil perdido» tampoco puede resolverse, esto se debe a que el usuario no tiene el hardware del monitor de mensajes SMS, la tarjeta SIM no está en manos del propietario del teléfono móvil, un remitente de un mensaje SMS recibido es el remitente inicial del mensaje SMS original, en lugar de ser el número actual del teléfono móvil perdido, y el número del ladrón no se puede adquirir.

40

45

Por ejemplo, en una solución técnica 2: se utiliza un segundo terminal de comunicación para controlar de forma remota el reenvío de mensajes SMS de un primer terminal de comunicación (un teléfono móvil perdido), y el segundo terminal de comunicación incluye: un módulo para controlar de forma remota la configuración del formato de mensajes SMS, un módulo de filtrado de mensajes SMS y un módulo de reenvío de mensajes SMS, donde el módulo para controlar de forma remota la configuración del formato de mensajes SMS está configurado para establecer o iniciar un formato de mensaje de una función de reenvío de mensajes SMS, el módulo de filtrado de mensajes SMS está configurado para filtrar y monitorear un nuevo mensaje SMS entrante y el módulo de reenvío de mensajes SMS está configurado para implementar el reenvío del nuevo mensaje SMS.

50

Sin embargo, la solución técnica 2 tiene los siguientes problemas: primero se debe establecer un número de seguridad en el primer terminal de comunicación, se usa un teléfono móvil del número de seguridad como el segundo terminal de comunicación para enviar una instrucción de mensaje SMS al primer terminal de comunicación, y dado que muchos usuarios tienen cada uno un solo número de teléfono móvil, el número de seguridad es otro número que a menudo no es el suyo y puede ser un número de un pariente o un amigo, cuando un teléfono móvil se pierde o se olvida llevarlo, el teléfono móvil del número de seguridad no se puede obtener a tiempo para la operación; además, el reenvío de un mensaje SMS en el primer terminal de comunicación al número de seguridad puede causar una fuga de privacidad del propietario.

60

Por ejemplo, en una solución técnica 3: un aparato antirrobo de IMEI de teléfono móvil se implementa mediante el uso de un sistema de servidor de base de datos informático, el aparato antirrobo de IMEI de teléfono móvil se interconecta con una pasarela de mensajes SMS a través de una red de datos y se configura para gestionar y mantener un estado de IMEI de un teléfono móvil de un usuario; el aparato antirrobo de IMEI de teléfono móvil recibe además una solicitud de informe de pérdida de teléfono móvil del propietario, y establece un estado de IMEI de un teléfono móvil del usuario que informa la pérdida en un estado de bloqueo; el aparato antirrobo de IMEI del teléfono móvil recibe además una solicitud de servicio de eliminación de pérdida informada del usuario del teléfono móvil, y establece el estado de IMEI del teléfono móvil del usuario que ha eliminado la pérdida informada en un estado normal; el aparato antirrobo de IMEI de teléfono móvil recibe además un mensaje SMS de encendido iniciado por un usuario de un terminal antirrobo de teléfono móvil, y para un teléfono móvil de IMEI en estado de bloqueo, envía una instrucción de bloqueo de teléfono móvil a una pasarela de ejecución antirrobo de teléfono móvil; la pasarela de mensajes SMS es un elemento de red en una red de comunicación móvil y está interconectada con un centro de mensajes SMS SMSC, y si se recibe una solicitud de envío de mensaje SMS de la pasarela de ejecución antirrobo del teléfono móvil, el mensaje SMS se envía a un número de teléfono de destino a través del SMSC; si se recibe un mensaje SMS enviado a un número de acceso antirrobo de IMEI de teléfono móvil, el mensaje SMS se envía al aparato antirrobo de IMEI del teléfono móvil, y la pasarela de mensajes SMS puede conectarse con el centro de mensajes SMSC para recibir un mensaje SMS del SMSC. Sin embargo, la solución técnica 3 tiene los siguientes problemas: es necesario realizar modificaciones integradas en la pasarela de mensajes SMS y el centro de mensajes SMS, lo que implica ciertos costes; el propietario debe realizar una solicitud de informe de pérdida (a través de un operador) para realizar una operación de bloqueo de pantalla en el teléfono móvil perdido, la solicitud de informe de pérdida aumenta el coste de tiempo del propietario y el propietario tiene que establecer un número de teléfono móvil que se vincula a un número de IMEI en lugar de una cuenta aleatoria, tal como un correo electrónico, que tiene ciertas limitaciones.

El documento WO 2007027065 A1 describe un procedimiento para controlar de forma remota una operación de un terminal de telecomunicación móvil en preparación para un caso de pérdida o robo del terminal de telecomunicación móvil, que incluye las etapas de: (a) monitorear si una instrucción de configuración de bloqueo para ingresar al modo de configuración de bloqueo es recibida desde el servidor de control remoto; (b) controlar un microprocesador incluido en el terminal de telecomunicación móvil para entrar en el modo de configuración de bloqueo, cuando la instrucción de configuración de bloqueo se recibe en la etapa (a); (c) monitorear si una instrucción de liberación de bloqueo para ingresar al modo de liberación de bloqueo se recibe desde el servidor de control remoto; y (d) controlar el microprocesador para ingresar al modo de liberación de bloqueo cuando se recibe la instrucción de liberación de bloqueo en la etapa (c).

El documento WO 2010/067263 A2 proporciona un sistema para la protección y copia de seguridad de la información privada en una unidad celular móvil en la que el software de aplicación innovador se precarga en la memoria móvil. El software se activa tan pronto como se intenta cambiar la tarjeta SIM por parte de entidades no autorizadas y el nuevo número de teléfono o las ID del dispositivo se transmiten al usuario autorizado del dispositivo. Es posible enviar un mensaje SMS cifrado al dispositivo móvil perdido para fines de recuperación/manipulación de datos. La invención asegura que el nuevo usuario no tenga conocimiento o indicios sobre los procesos en funcionamiento. El software del sistema de la invención está estructurado en varios módulos; el primer módulo busca los SMS que contienen un código preasignado asociado con los comandos asignados. El segundo y el resto de los módulos analizan los mensajes para garantizar que los SMS recibidos provengan de un destinatario autorizado antes de ejecutar los comandos que ha recibido el dispositivo perdido.

#### 45 RESUMEN

La invención se describe en las reivindicaciones 1 a 11. Un problema técnico resuelto principalmente en la presente invención es proporcionar un servidor y un procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación, y un terminal de comunicación, de modo que sea capaz de controlar de manera flexible y conveniente el funcionamiento de un terminal de comunicación perdido a través del servidor para controlar de forma remota el funcionamiento de un terminal de comunicación, garantizando así la seguridad de los datos personales en el terminal de comunicación.

En un aspecto, se proporciona un servidor para controlar de forma remota el funcionamiento de un terminal de comunicación, el servidor para controlar de forma remota el funcionamiento de un terminal de comunicación implementa la comunicación con un terminal de comunicación a través de una red, y el servidor para controlar de forma remota el funcionamiento de un terminal de comunicación incluye: un módulo receptor, configurado para recibir información de operación generada por una operación de entrada de un usuario registrado en un terminal de red, donde la información de operación incluye información de comando e información adicional; un módulo de adquisición, configurado para adquirir, según la información sobre el usuario registrado, un identificador de dispositivo almacenado previamente que corresponde al terminal de comunicación; un módulo generador de instrucciones de gestión y control, configurado para convertir, según un formato de intercambio de datos predeterminado, la información de operación

recibida y el identificador de dispositivo adquirido en una instrucción de gestión y control; y un módulo de servicio push, configurado para proporcionar la instrucción de gestión y control para el terminal de comunicación en forma de servicio push, de modo que el terminal de comunicación funcione según la instrucción de gestión y control.

- 5 En una primera forma de implementación de este aspecto, el módulo de servicio push está configurado además para comenzar a proporcionar un servicio push para el terminal de comunicación en respuesta a una solicitud de registro del servicio push del terminal de comunicación.

- 10 En una segunda forma de implementación de este aspecto, el servidor para controlar de forma remota el funcionamiento de un terminal de comunicación incluye además un módulo de gestión de información de registro, y el módulo de gestión de información de registro está configurado para gestionar la información de registro correspondiente al terminal de comunicación.

- 15 En otro aspecto, se proporciona un procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación, el procedimiento se aplica en un servidor para controlar de forma remota el funcionamiento de un terminal de comunicación, y el procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación incluye las siguientes etapas: recibir información de operación generada por una operación de entrada de un usuario registrado en un terminal de red, donde la información de operación incluye información de comando e información adicional; adquirir, según la información sobre el usuario registrado, un identificador de dispositivo  
20 almacenado previamente que corresponde al terminal de comunicación; convertir, mediante el uso de un formato de intercambio de datos predeterminado, la información de operación recibida y el identificador de dispositivo adquirido en una instrucción de gestión y control; y proporcionar la instrucción de gestión y control para el terminal de comunicación en forma de servicio push, de modo que el terminal de comunicación funcione según la instrucción de gestión y control.

- 25 En una primera forma de implementación de este aspecto, el procedimiento incluye además las siguientes etapas: comenzar a proporcionar un servicio push para el terminal de comunicación en respuesta a una solicitud de registro push del terminal de comunicación.

- 30 En una segunda forma de implementación de este aspecto, el procedimiento incluye además la siguiente etapa: en respuesta a una solicitud de inicio de sesión del terminal de comunicación, comenzar a gestionar la información de registro correspondiente al terminal de comunicación.

- 35 En otro aspecto, se proporciona un terminal de comunicación, y el terminal de comunicación incluye: un módulo de cliente de servicio push, configurado para recibir, en forma de servicio push, una instrucción de gestión y control provista activamente por un servidor; un módulo de análisis de instrucciones, configurado para analizar, según un formato predeterminado de intercambio de datos, la instrucción de gestión y control recibida, con el fin de obtener información de operación correspondiente y adquirir un identificador de dispositivo, donde la información de operación incluye información de comando e información adicional; un módulo generador de instrucciones de funcionamiento,  
40 configurado para generar una instrucción de funcionamiento correspondiente según la información del comando y la información adicional que se obtiene mediante el análisis; y un módulo de ejecución de instrucciones de funcionamiento, configurado para ejecutar, según las instrucciones de funcionamiento, el funcionamiento correspondiente para proteger la seguridad de los datos.

- 45 En una primera forma de implementación de este aspecto, la información del comando es la información del comando de reenvío de mensajes SMS, la información adicional es un número de teléfono móvil de un receptor de un mensaje SMS reenviado, y el módulo generador de instrucciones de funcionamiento genera una instrucción de reenvío de mensajes SMS correspondiente según la información del comando y la información adicional que se obtiene mediante el análisis; y el módulo de ejecución de instrucciones de funcionamiento incluye una unidad de determinación, una  
50 unidad de monitoreo de mensajes SMS y una unidad de reenvío de mensajes SMS, donde la unidad de determinación está configurada para determinar un tipo de instrucción de funcionamiento, y al determinar que la instrucción de funcionamiento es una instrucción de reenvío de mensaje SMS, determinar el estado de una tarjeta SIM y, al determinar que el estado de la tarjeta SIM es un estado listo, controlar la unidad de monitoreo de mensajes SMS para que comience a funcionar; la unidad de monitoreo de mensajes SMS está configurada para monitorear un nuevo  
55 mensaje SMS entrante, y al monitorear un nuevo mensaje SMS entrante, controlar la unidad de reenvío de mensajes SMS para que funcione; y la unidad de reenvío de mensajes SMS está configurada para enviar el nuevo mensaje SMS entrante supervisado a un dispositivo de comunicación que corresponde al número de teléfono móvil del receptor del mensaje SMS reenviado.

- 60 En una segunda forma de implementación de este aspecto, el módulo de ejecución de instrucciones de funcionamiento incluye además una unidad de informe de resultados, y la unidad de determinación está configurada además para, al determinar que el estado de la tarjeta SIM es un estado no listo, controlar que la unidad de informe de resultados

funcione; y la unidad de informe de resultados está configurada para generar información de error de configuración y transmitir la información de error de configuración a un servidor remoto, de modo que el servidor proporcione un terminal de red con información rápida sobre un error de configuración.

- 5 En una tercera forma de implementación de este aspecto, la información del comando es información del comando de bloqueo de pantalla, la información adicional es información de contraseña, y el módulo generador de instrucciones de funcionamiento está configurado para generar una instrucción de bloqueo de pantalla correspondiente según la información del comando y la información adicional que se obtienen mediante análisis; el módulo de ejecución de instrucciones de funcionamiento incluye una unidad de determinación y una unidad de bloqueo de pantalla, donde la
- 10 unidad de determinación está configurada para determinar un tipo de instrucción de funcionamiento, y al determinar que la instrucción de funcionamiento es una instrucción de bloqueo de pantalla, controlar que la unidad de bloqueo de pantalla funcione; y la unidad de bloqueo de pantalla está configurada para ejecutar una operación de bloqueo de pantalla para proteger la seguridad de los datos.
- 15 En una cuarta forma de implementación de este aspecto, la unidad de determinación, al determinar que la instrucción de funcionamiento es una instrucción de bloqueo de pantalla, determina si un conjunto de gestión de dispositivos del terminal de comunicación está activado, y al determinar que el conjunto de gestión de dispositivos del terminal de comunicación está en estado activado, controla que la unidad de bloqueo de pantalla funcione; y la unidad de bloqueo de pantalla funciona, según la información adicional en las instrucciones de bloqueo de pantalla, para realizar una
- 20 operación de bloqueo de pantalla para proteger la seguridad de los datos.

En una quinta forma de implementación de este aspecto, la unidad de bloqueo de pantalla, al determinar que la información adicional no está vacía, realiza una operación de bloqueo de pantalla para proteger la seguridad de los datos; y la unidad de bloqueo de pantalla desbloquea una pantalla al determinar que la información adicional está

25 vacía.

En otro aspecto, se proporciona un procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación, el procedimiento se aplica en un terminal de comunicación que tiene una conexión establecida con un servidor remoto, y el procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación

30 incluye las siguientes etapas: recibir, en forma de servicio push, una instrucción de gestión y control provista activamente por el servidor; analizar, según el formato de intercambio de datos predeterminado, la instrucción de gestión y control recibida, para obtener la información de operación correspondiente y adquirir un identificador de dispositivo, donde la información de operación incluye información de comando e información adicional; generar una instrucción de funcionamiento correspondiente según la información del comando y la información adicional que se

35 obtiene mediante el análisis; y ejecutar, según las instrucciones de funcionamiento, el funcionamiento para proteger la seguridad de los datos.

En una primera implementación de este aspecto, la información del comando es información del comando de reenvío de mensajes SMS, la información adicional es un número de teléfono móvil de un receptor de un mensaje SMS

40 reenviado, y se genera una instrucción de reenvío de mensajes SMS correspondiente según la información del comando y la información adicional que se obtiene mediante el análisis; y la etapa de ejecutar, según la instrucción de funcionamiento, el funcionamiento para proteger la seguridad de los datos incluye específicamente: determinar un tipo de instrucción de funcionamiento; cuando se determina que la instrucción de funcionamiento es una instrucción de reenvío de mensajes SMS, determinar un estado de una tarjeta SIM; cuando se determina que el estado de la tarjeta

45 SIM es un estado listo, monitorear un nuevo mensaje SMS entrante; y enviar el nuevo mensaje SMS entrante a un dispositivo de comunicación que corresponde al número de teléfono móvil del receptor del mensaje SMS reenviado.

En una segunda forma de implementación de este aspecto, cuando se determina que el estado de la tarjeta SIM es un estado no listo, se genera información de error de configuración; y la información de error de configuración se transmite al servidor remoto, de modo que el servidor proporcione un terminal de red con información inmediata sobre

50 un error de configuración.

En una tercera forma de implementación de este aspecto, la información del comando es información del comando de bloqueo de pantalla, la información adicional es una información de contraseña, y se genera una instrucción de bloqueo de pantalla correspondiente según la información del comando y la información adicional que se obtiene mediante

55 análisis; y la etapa de ejecutar, según las instrucciones de funcionamiento, el funcionamiento para proteger la seguridad de los datos incluye específicamente: determinar un tipo de instrucción de funcionamiento; y cuando se determina que la instrucción de funcionamiento es una instrucción de bloqueo de pantalla, se ejecuta una operación de bloqueo de pantalla para proteger la seguridad de los datos.

60 En una cuarta forma de implementación de este aspecto, cuando se determina que la instrucción de funcionamiento es una instrucción de bloqueo de pantalla, se determina si un conjunto de gestión de dispositivo del terminal de comunicación está activado; y cuando se determina que el conjunto de gestión de dispositivo del terminal de

comunicación está en estado activado, se realiza una operación de bloqueo de pantalla según la información adicional en la instrucción de bloqueo de pantalla para proteger la seguridad de los datos.

5 En una quinta forma de implementación de este aspecto, cuando se determina que la información adicional no está vacía, se realiza una operación de bloqueo de pantalla para proteger la seguridad de los datos; y cuando se determina que la información adicional está vacía, se desbloquea una pantalla.

Los efectos beneficiosos de la presente invención radican en que: a diferencia de la situación en la técnica anterior, por medio del servidor y el procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación y el terminal de comunicación según la presente invención, cuando un terminal de comunicación (por ejemplo, un teléfono móvil) se pierde o se olvida llevarlo, el propietario solo necesita iniciar sesión en un terminal de red para controlar de forma inmediata y remota que el terminal de comunicación que el propietario no lleva consigo funcione, lo que garantiza la seguridad de los datos personales en el terminal de comunicación, por ejemplo, reenviar un mensaje SMS en el terminal de comunicación a cualquier teléfono móvil que pueda recibir el mensaje SMS y 15 bloquear de forma remota una pantalla del terminal de comunicación para garantizar que no se use el teléfono móvil perdido. Mientras tanto, los modos de implementación de la presente invención no necesitan modificar elementos de red en la red existente o red móvil, ahorrando así en costes.

### 20 **BREVE DESCRIPCIÓN DE LOS DIBUJOS**

La figura 1 es un diagrama esquemático de la arquitectura de la aplicación de un sistema para controlar de forma remota el funcionamiento de un terminal de comunicación según una realización ejemplar;

la figura 2 es un diagrama de bloques funcional de un servidor para controlar de forma remota el funcionamiento de un terminal de comunicación en la figura 1;

la figura 3 es un diagrama de bloques funcional de un terminal de comunicación en la figura 1;

la figura 4 es un diagrama de bloques funcional de un módulo de ejecución de instrucción de funcionamiento en la figura 3;

la figura 5 es otro diagrama de bloques funcional de un módulo de ejecución de instrucción de funcionamiento en la figura 3;

35 la figura 6 es un diagrama de flujo de un procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación según una realización ejemplar; y

la figura 7 es un diagrama de flujo de un procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación según otra realización ejemplar.

### 40 **DESCRIPCIÓN DE LAS REALIZACIONES**

Lo siguiente describe de forma clara y completa las soluciones técnicas en las realizaciones de la presente invención con referencia a los dibujos adjuntos en las realizaciones de la presente invención. Aparentemente, las realizaciones 45 descritas son solamente una parte y no todas las realizaciones de la presente invención. Todas las demás realizaciones obtenidas por expertos en la técnica basándose en las realizaciones de la presente invención sin esfuerzos creativos estarán dentro del alcance de protección de la presente invención.

En este modo de implementación, se usa un terminal de comunicación (por ejemplo, un teléfono móvil) para establecer una conexión de red con un servidor, y un propietario envía información de operación al servidor, de modo que el servidor realiza el control remoto en un terminal de comunicación que no lleva consigo el propietario, lo que garantiza la seguridad de los datos personales en el terminal de comunicación. Con referencia a la figura 1, un sistema 10 para controlar de forma remota el funcionamiento de un terminal de comunicación incluye un servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación, un terminal de comunicación 30 y un terminal de red 40. El terminal de comunicación 30, el terminal de red 40 y el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación están conectados a través de una red, tal como una red inalámbrica y una red cableada, y el terminal de comunicación 30 puede ser un teléfono móvil. El terminal de red 40 puede ser un ordenador personal, un asistente digital personal (PDA, por sus siglas en inglés) y similares.

60 El terminal de comunicación del propietario 30 solo necesita establecer una conexión de red con el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación, implementar una operación de registro en el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación para convertirse

en un usuario registrado, y suscribirse a un servicio push al mismo tiempo, con el fin de implementar la garantía de seguridad de los datos personales en el terminal de comunicación 30, tales como: configurar remotamente el reenvío de mensajes SMS y bloquear remotamente una pantalla del terminal de comunicación 30.

- 5 Las soluciones de implementación del servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación, y el terminal de comunicación 30 se describen específicamente a continuación, de modo que un experto en la técnica entienda e implemente la presente invención.

10 Con referencia a la figura 2, el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación incluye los siguientes módulos:

15 Un módulo receptor 21 está configurado para recibir información de operación generada por una operación de entrada de un usuario registrado en el terminal de red 40, donde la información de operación incluye información de comando e información adicional. Por ejemplo, el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación proporciona al usuario registrado una interfaz de entrada para controlar el terminal de comunicación 30, y el usuario registrado puede acceder a la interfaz de entrada e ingresar la información de operación en la interfaz de entrada.

20 Un módulo de adquisición 22 está configurado para adquirir, según la información sobre el usuario registrado, un identificador de dispositivo almacenado correspondiente al terminal de comunicación 30, donde el identificador de dispositivo es un símbolo identificador utilizado por el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación para identificar el terminal de comunicación 30 después de que el usuario registrado se registre en el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación a través del terminal de comunicación 30, por ejemplo, cuando se registra un servicio push, el identificador del dispositivo es un autenticador de dispositivo.

30 Un módulo generador de instrucciones de gestión y control 23 está configurado para convertir, según un formato de intercambio de datos predeterminado, la información de operación recibida y el identificador de dispositivo adquirido en una instrucción de gestión y control, donde el formato de intercambio de datos predeterminado puede ser un formato de intercambio de datos ligero, por ejemplo, JSON (notación de objetos JavaScript).

35 Un módulo de servicio push 24 está configurado para proporcionar, en forma de servicio push, la instrucción de gestión y control para el terminal de comunicación 30, de modo que el terminal de comunicación 30 funcione según la instrucción de gestión y control, donde el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación genera una identificación de sesión única (ID de sesión) cada vez que se envían las instrucciones de gestión y control, y la identificación de sesión se utiliza para coincidir con un resultado devuelto por el terminal de comunicación 30. Además, el módulo de servicio push 24 está configurado además para comenzar a proporcionar un servicio push para el terminal de comunicación 30 en respuesta a una solicitud de registro de servicio push del terminal de comunicación 30; el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación incluye además un módulo de gestión de información de registro 25, y el módulo de gestión de información de registro 40 25 está configurado para gestionar la información de registro correspondiente al terminal de comunicación 30.

Con referencia a la figura 3, el terminal de comunicación 30 incluye los siguientes módulos:

45 Un módulo de cliente de servicio push 31 está configurado para recibir, en forma de servicio push, una instrucción de gestión y control provista activamente por el servidor 20. Por ejemplo, el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación envía la instrucción de gestión y control en forma de difusión, y el módulo de cliente de servicio push 31 puede recibir, en forma de recepción de difusión, la instrucción de gestión y control.

50 Un módulo de análisis de instrucciones 32 está configurado para analizar, según un formato de intercambio de datos predeterminado, la instrucción de gestión y control recibida, con el fin de obtener información de operación correspondiente y adquirir un identificador de dispositivo, donde la información de operación incluye información de comando e información adicional. El formato de intercambio de datos predeterminado puede ser un formato de intercambio de datos ligero, por ejemplo, JSON (notación de objetos JavaScript).

60 El módulo generador de instrucciones de funcionamiento 33 está configurado para generar una instrucción de funcionamiento correspondiente según la información del comando y la información adicional que se obtiene a través del análisis por el módulo de análisis de instrucciones 32.

El módulo de ejecución de instrucciones de funcionamiento 34 está configurado para ejecutar, según la instrucción de funcionamiento, el funcionamiento correspondiente para proteger la seguridad de los datos.

Por ejemplo, en una realización del reenvío de mensajes SMS, con referencia a la figura 4, la información del comando es información del comando de reenvío de mensajes SMS, la información adicional es un número de teléfono móvil de un receptor de un mensaje SMS reenviado, y el módulo generador de instrucciones de funcionamiento 33 genera una instrucción de reenvío de mensajes SMS correspondiente según la información del comando e información adicional que se obtiene mediante el análisis; además, el módulo de ejecución de instrucciones de funcionamiento 34 incluye una unidad de determinación 340, una unidad de monitoreo de mensajes SMS 341 y una unidad de reenvío de mensajes SMS 342.

10 La unidad de determinación 340 está configurada para determinar un tipo de instrucción de funcionamiento, al determinar que la instrucción de funcionamiento es una instrucción de reenvío de mensajes SMS, determinar el estado de una tarjeta SIM y al determinar que el estado de la tarjeta SIM es un estado listo, controlar la unidad de monitoreo de mensajes SMS 341 para que comience a funcionar; la unidad de monitoreo de mensajes SMS 341 está configurada para monitorear un nuevo mensaje SMS entrante, y cuando se monitorea un nuevo mensaje SMS entrante, controlar que la unidad de reenvío de mensajes SMS 342 funcione; y la unidad de reenvío de mensajes SMS 342 está configurada para enviar, según la información adicional, el nuevo mensaje SMS entrante monitorizado y un número de teléfono móvil actual a un dispositivo de comunicación correspondiente al número de teléfono móvil del receptor del mensaje SMS reenviado. De esta manera, si una tarjeta del terminal de comunicación perdido 30 no se cambia, todos los mensajes SMS enviados a un número original A se reenvían, y si el terminal de comunicación 30 se ha cambiado a un número B, cuando se envía un mensaje SMS al número B, el terminal de comunicación 30 todavía reenvía el mensaje SMS enviado al número B y el número B a un teléfono móvil, capaz de recibirlos, del usuario cuyo teléfono móvil se ha perdido. Además, el módulo de ejecución de instrucciones de funcionamiento 34 incluye además una unidad de informe de resultados 343, la unidad de determinación 340 se configura además para, cuando se determina que el estado de la tarjeta SIM es un estado no preparado, controlar que la unidad de informe de resultados 343 funcione; y la unidad de informe de resultados 343 está configurada para generar información de error de configuración y transmitir la información de error de configuración al servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación, de modo que el servidor 20 para controlar de forma remota el funcionamiento de un terminal de comunicación provea al terminal de red 40 información inmediata sobre un error de configuración.

30 Por ejemplo, en una realización de bloqueo de pantalla, con referencia a la figura 5, la información de comando es información de comando de bloqueo de pantalla, la información adicional es información de contraseña, y el módulo generador de instrucciones de funcionamiento 33 está configurado para generar una instrucción de bloqueo de pantalla correspondiente según la información de comando y la información adicional que se obtiene mediante análisis; y el módulo de ejecución de instrucciones de funcionamiento 34 incluye una unidad de determinación 340' y una unidad de bloqueo de pantalla 341'.

La unidad de determinación 340' está configurada para determinar un tipo de instrucción de funcionamiento, y al determinar que la instrucción de funcionamiento es una instrucción de bloqueo de pantalla, controlar que la unidad de bloqueo de pantalla 341' funcione; y la unidad de bloqueo de pantalla 341' está configurada para ejecutar una operación de bloqueo de pantalla para proteger la seguridad de los datos.

Además, la unidad de determinación 340' determina, al determinar que la instrucción de funcionamiento es la instrucción de bloqueo de pantalla, si un conjunto de gestión de dispositivos del terminal de comunicación 30 está activado, y al determinar que el conjunto de gestión de dispositivos del terminal de comunicación 30 está en estado activado, controla que la unidad de bloqueo de pantalla 341' funcione; la unidad de bloqueo de pantalla 341' funciona según la información adicional en la instrucción de bloqueo de pantalla, con el fin de realizar la operación de bloqueo de pantalla para proteger la seguridad de los datos, es decir, la unidad de bloqueo de pantalla 341' realiza, al determinar que la información adicional no está vacía, la operación de bloqueo de pantalla para proteger la seguridad de los datos; y la unidad de bloqueo de pantalla 341' desbloquea una pantalla al determinar que la información adicional está vacía.

Con referencia a la figura 6, se aplica un procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación en un servidor de control remoto del funcionamiento de un terminal de comunicación, de modo que el servidor realiza el control remoto en un terminal de comunicación que no es transportado por un propietario, garantizando así la seguridad de los datos personales en el terminal de comunicación. El procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación incluye las siguientes etapas:

etapa S301: recibir información de operación generada por una operación de entrada de un usuario registrado en el terminal de red, donde la información de operación incluye información de comando e información adicional;

etapa S303: adquirir, según la información sobre el usuario registrado, un identificador de dispositivo almacenado

previamente correspondiente al terminal de comunicación;

etapa S305: convertir, mediante el uso de un formato de intercambio de datos predeterminado, la información de operación recibida y el identificador de dispositivo adquirido en una instrucción de gestión y control, donde el formato de intercambio de datos predeterminado puede ser un formato de intercambio de datos ligero, por ejemplo, JSON (notación de objetos JavaScript); y

etapa S307: proporcionar, en forma de servicio push, la instrucción de gestión y control para el terminal de comunicación, de modo que el terminal de comunicación funcione según la instrucción de gestión y control.

El procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación incluye además las siguientes etapas: comenzar a proporcionar un servicio push para el terminal de comunicación en respuesta a una solicitud de registro push del terminal de comunicación; y en respuesta a una solicitud de inicio de sesión del terminal de comunicación, comenzar a gestionar la información de registro correspondiente al terminal de comunicación.

Con referencia a la figura 7, se aplica un procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación en un terminal de comunicación que tiene una conexión establecida con un servidor remoto, y el procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación incluye las siguientes etapas:

etapa S401: recibir, en forma de servicio push, una instrucción de gestión y control provista activamente por un servidor;

etapa S403: analizar, según un formato de intercambio de datos predeterminado, la instrucción de gestión y control recibida, para obtener la información de operación correspondiente y adquirir un identificador de dispositivo, donde la información de operación incluye información de comando e información adicional, y el formato de intercambio de datos predeterminado puede ser un formato de intercambio de datos ligero, por ejemplo, JSON (notación de objetos JavaScript Object);

etapa S405: generar una instrucción de funcionamiento correspondiente según la información del comando y la información adicional que se obtiene mediante el análisis; y

etapa S407: ejecutar, según la instrucción de funcionamiento, el funcionamiento para proteger la seguridad de los datos.

Por ejemplo, en una realización del reenvío de mensajes SMS, la información del comando es información del comando de reenvío de mensajes SMS, la información adicional es un número de teléfono móvil de un receptor de un mensaje SMS reenviado, y se genera una instrucción de reenvío de mensaje SMS correspondiente según información de comando y la información adicional que se obtiene mediante el análisis; y la etapa de ejecutar, según la instrucción de funcionamiento, el funcionamiento para proteger la seguridad de los datos incluye específicamente:

determinar un tipo de instrucción de funcionamiento;

cuando se determina que la instrucción de funcionamiento es una instrucción de reenvío de mensaje SMS, determinar el estado de una tarjeta SIM;

cuando se determina que el estado de la tarjeta SIM es un estado listo, monitorear un nuevo mensaje SMS entrante;

enviar el nuevo mensaje SMS entrante a un dispositivo de comunicación que corresponde al número de teléfono móvil del receptor del mensaje SMS reenviado;

cuando se determina que el estado de la tarjeta SIM es un estado no listo, generar la información de error de configuración; y

transmitir la información de error de configuración al servidor, de modo que el servidor proporcione un terminal de red con información inmediata sobre un error de configuración.

Por ejemplo, en una realización del bloqueo de pantalla, la información del comando es información del comando de bloqueo de pantalla, la información adicional es información de contraseña, y se genera una instrucción de bloqueo de pantalla correspondiente según la información de comando y la información adicional que se obtienen mediante el análisis; y la etapa de ejecutar, según la instrucción de funcionamiento, el funcionamiento para proteger la seguridad de los datos incluye específicamente:

determinar un tipo de instrucción de funcionamiento; y

cuando se determina que la instrucción de funcionamiento es una instrucción de bloqueo de pantalla, ejecutar una operación de bloqueo de pantalla para proteger la seguridad de los datos, que incluye específicamente: cuando se  
 5 determina que la instrucción de funcionamiento es la instrucción de bloqueo de pantalla, determinar si un conjunto de gestión de dispositivos del terminal de comunicación está activado; cuando se determina que el conjunto de gestión de dispositivos del terminal de comunicación está en estado activado, realizar, según la información adicional en la instrucción de bloqueo de pantalla, una operación de bloqueo de pantalla para proteger la seguridad de los datos, es decir, cuando se determina que la información no está vacía, realizar la operación de bloqueo de pantalla para proteger  
 10 la seguridad de los datos; y desbloquear una pantalla cuando se determina que la información adicional está vacía.

Por medio de descripciones de las realizaciones anteriores, en comparación con la técnica anterior, la presente invención tiene las siguientes ventajas: por medio del servidor y el procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación y el terminal de comunicación según la presente invención, cuando  
 15 un terminal de comunicación (por ejemplo, un teléfono móvil) se pierde o se olvida llevarlo consigo, el propietario solo necesita iniciar sesión en un terminal de red para controlar de forma inmediata y remota que el funcionamiento del terminal de comunicación que el propietario no lleva consigo funcione, lo que garantiza la seguridad de los datos personales en el terminal de comunicación, por ejemplo, reenviar un mensaje SMS en el terminal de comunicación a cualquier teléfono móvil que pueda recibir el mensaje SMS y bloquear de forma remota una pantalla del terminal de  
 20 comunicación para garantizar que no se use el teléfono móvil perdido. Mientras tanto, los modos de implementación de la presente invención no necesitan modificar elementos de red en la red existente o red móvil, ahorrando así en costes.

En las varias realizaciones proporcionadas en la presente solicitud, se debe entender que el sistema, aparato y  
 25 procedimiento descritos se pueden implementar de otras maneras. Por ejemplo, la realización del aparato descrito es solo a modo de ejemplo. Por ejemplo, la división de los módulos o unidades es solo la división de la función lógica y puede ser otra división en la implementación real. Por ejemplo, se pueden combinar o integrar una pluralidad de unidades o componentes en otro sistema, o algunas funciones se pueden ignorar o no ejecutar. Además, los acoplamientos mutuos o acoplamientos directos o conexiones de comunicación que se muestran o se analizan, se  
 30 pueden implementar a través de algunas interfaces. Los acoplamientos indirectos o conexiones de comunicación entre los aparatos o unidades se pueden implementar en formas electrónicas, mecánicas u otras formas.

Las unidades descritas como partes separadas pueden estar o no físicamente separadas, y las partes exhibidas como unidades pueden ser o no unidades físicas, pueden estar situadas en una posición, o pueden estar distribuidas en una  
 35 pluralidad de unidades de red. Una parte o todas las unidades pueden seleccionarse según los requisitos reales para lograr los objetivos de las soluciones de las realizaciones.

Además, las unidades funcionales en las realizaciones de la presente invención se pueden integrar en una unidad de procesamiento, o cada una de las unidades puede existir solo físicamente, o se pueden integrar en una unidad dos o  
 40 más unidades. La unidad integrada se puede implementar en forma de hardware, o se puede implementar en forma de una unidad funcional de software.

Cuando la unidad integrada se implementa en forma de una unidad funcional de software y se vende o se usa como un producto independiente, la unidad integrada se puede almacenar en un medio de almacenamiento legible por  
 45 ordenador. Basándose en dicho entendimiento, las soluciones técnicas de la presente invención esencialmente, o la parte que contribuye a la técnica anterior, o todas o una parte de las soluciones técnicas, se pueden implementar en forma de un producto de software. El producto de software informático se almacena en un medio de almacenamiento e incluye varias instrucciones para dar instrucciones a un dispositivo informático (que puede ser un ordenador personal, un servidor o un dispositivo de red) o un procesador (procesador) para realizar todas o una parte de las etapas de los  
 50 procedimientos descritos en las realizaciones de la presente invención. El medio de almacenamiento anterior incluye: cualquier medio que pueda almacenar códigos de programa, tal como un disco flash USB, un disco duro extraíble, una memoria de solo lectura (ROM, memoria de solo lectura), una memoria de acceso aleatorio (RAM, memoria de acceso aleatorio), un disco magnético o un disco óptico.

55 Debe observarse que las realizaciones anteriores están destinadas simplemente a describir las soluciones técnicas de la presente invención además de limitar la presente invención. Aunque la presente invención se describe en detalle con referencia a las realizaciones anteriores, los expertos en la técnica deben comprender que aún pueden hacer modificaciones a las soluciones técnicas descritas en las realizaciones anteriores o hacer reemplazos equivalentes a algunas características técnicas de las mismas, sin apartarse del alcance de las soluciones técnicas de las  
 60 realizaciones de la presente invención.

**REIVINDICACIONES**

1. Un servidor (20) para controlar de forma remota el funcionamiento de un terminal de comunicación, implementar la comunicación con un terminal de comunicación a través de una red y que comprende:
- 5 un módulo receptor (21), configurado para recibir información de operación generada por una operación de entrada de un usuario registrado en un terminal de red, donde la información de operación comprende información de comando e información adicional; la información de comando es información del comando de bloqueo de pantalla, la información adicional es una información de contraseña;
- 10 un módulo de adquisición (22), configurado para adquirir, según la información sobre el usuario registrado, un identificador de dispositivo almacenado previamente que corresponde al terminal de comunicación;
- un módulo generador de instrucciones de gestión y control (23), configurado para convertir, según un formato de intercambio de datos predeterminado, la información de operación recibida y el identificador de dispositivo adquirido
- 15 en una instrucción de gestión y control, donde la instrucción de gestión y control es una instrucción de bloqueo de pantalla; y
- un módulo de servicio push (24), configurado para proporcionar la instrucción de gestión y control para el terminal de comunicación en forma de servicio push.
- 20
2. El servidor para controlar de forma remota el funcionamiento de un terminal de comunicación según la reivindicación 1, donde el módulo de servicio push (24) está configurado además para comenzar a proporcionar un servicio push para el terminal de comunicación en respuesta a una solicitud de registro del servicio push del terminal
- 25 de comunicación.
3. El servidor para controlar de forma remota el funcionamiento de un terminal de comunicación según la reivindicación 1 o 2, donde el servidor para controlar de forma remota el funcionamiento de un terminal de comunicación comprende además un módulo de gestión de información de registro (25), y el módulo de gestión de
- 30 información de registro está configurado para gestionar la información de registro que corresponde al terminal de comunicación.
4. Un terminal de comunicación (30), que comprende:
- 35 un módulo de cliente de servicio push (31), configurado para recibir, en forma de servicio push, una instrucción de gestión y control provista activamente por un servidor;
- un módulo de análisis de instrucciones (32), configurado para analizar, según un formato de intercambio de datos predeterminado, la instrucción de gestión y control recibida, obtener información de operación correspondiente y
- 40 adquirir un identificador de dispositivo, donde la información de operación comprende información de comando e información adicional;
- un módulo generador de instrucciones de funcionamiento (33), configurado para generar una instrucción de funcionamiento correspondiente según la información de comando y la información adicional que se obtienen mediante
- 45 el análisis;
- un módulo de ejecución de instrucciones de funcionamiento (34), configurado para ejecutar, según la instrucción de funcionamiento, el funcionamiento correspondiente para proteger la seguridad de los datos,
- 50 donde la información de comando es información del comando de bloqueo de pantalla, la información adicional es información de contraseña;
- el módulo generador de instrucciones de funcionamiento (33) está configurado específicamente para generar una instrucción de bloqueo de pantalla correspondiente según la información de comando de bloqueo de pantalla y la
- 55 información de contraseña que se obtienen mediante el análisis; y
- el módulo de ejecución de instrucciones de funcionamiento (34) comprende una unidad de determinación (340') y una unidad de bloqueo de pantalla (341'), donde
- 60 la unidad de determinación (340') está configurada para determinar un tipo de instrucción de funcionamiento, y al determinar que la instrucción de funcionamiento es la instrucción de bloqueo de pantalla, controlar que la unidad de bloqueo de pantalla funcione; y

la unidad de bloqueo de pantalla (341') está configurada para ejecutar una operación de bloqueo de pantalla para proteger la seguridad de los datos.

5 5. El terminal de comunicación según la reivindicación 4, donde la unidad de determinación (340') configurada además para, al determinar que la instrucción de funcionamiento es una instrucción de bloqueo de pantalla, determinar si un conjunto de gestión de dispositivos del terminal de comunicación está activado, y al determinar que el conjunto de gestión de dispositivos del terminal de comunicación está en estado activado, controlar que la unidad de bloqueo de pantalla (341') funcione; y

10 la unidad de bloqueo de pantalla (341') está configurada específicamente para, según la información adicional en la instrucción de bloqueo de pantalla, realizar la operación de bloqueo de pantalla para proteger la seguridad de los datos.

6. El terminal de comunicación según la reivindicación 5, donde la unidad de bloqueo de pantalla (341'), al  
15 determinar que la información adicional no está vacía, realiza una operación de bloqueo de pantalla para proteger la seguridad de los datos; y la unidad de bloqueo de pantalla (341') desbloquea una pantalla al determinar que la información adicional está vacía.

7. Un procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación,  
20 aplicado en un terminal de comunicación que tiene una conexión establecida con un servidor remoto, que comprende las siguientes etapas:

recibir, en forma de servicio push, una instrucción de gestión y control provista activamente por el servidor remoto;

25 analizar, según un formato de intercambio de datos predeterminado, la instrucción de gestión y control recibida; obtener información de operación y adquirir un identificador de dispositivo, donde la información de operación comprende información de comando e información adicional;

30 generar una instrucción de funcionamiento correspondiente según la información del comando y la información adicional que se obtienen mediante el análisis; y

ejecutar, según la instrucción de funcionamiento, el funcionamiento para proteger la seguridad de los datos,

35 donde la información de comando es información de comando de bloqueo de pantalla, la información adicional es información de contraseña, se genera una instrucción de bloqueo de pantalla correspondiente según la información de comando y la información de contraseña; y la etapa de ejecutar, según la instrucción de funcionamiento, el funcionamiento para proteger la seguridad de los datos comprende específicamente:

determinar un tipo de instrucción de funcionamiento; y

40 cuando se determina que la instrucción de funcionamiento es la instrucción de bloqueo de pantalla, ejecutar una operación de bloqueo de pantalla para proteger la seguridad de los datos.

8. El procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación  
45 según la reivindicación 7, donde la información de operación se genera mediante una operación de entrada de un usuario en un terminal de red.

9. El procedimiento según la reivindicación 8, donde el usuario accede a una interfaz de entrada proporcionada por el servidor remoto e ingresa la información de operación en la interfaz de entrada.

50 10. El procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación según cualquiera de las reivindicaciones 7 a 9, donde antes de ejecutar una operación de bloqueo de pantalla para proteger la seguridad de los datos, el procedimiento comprende además:

55 determinar si un conjunto de gestión de dispositivos del terminal de comunicación está activado;

donde la etapa de ejecutar una operación de bloqueo de pantalla para proteger la seguridad de los datos comprende:

60 cuando se determina que el conjunto de gestión de dispositivos del terminal de comunicación está en un estado activado, ejecutar, según la información adicional en la instrucción de bloqueo de pantalla, una operación de bloqueo de pantalla para proteger la seguridad de los datos.

11. El procedimiento para controlar de forma remota el funcionamiento de un terminal de comunicación según la reivindicación 10, donde:

cuando se determina que la información adicional no está vacía, se realiza una operación de bloqueo de pantalla para  
5 proteger la seguridad de los datos; y

cuando se determina que la información adicional está vacía, se desbloquea una pantalla.

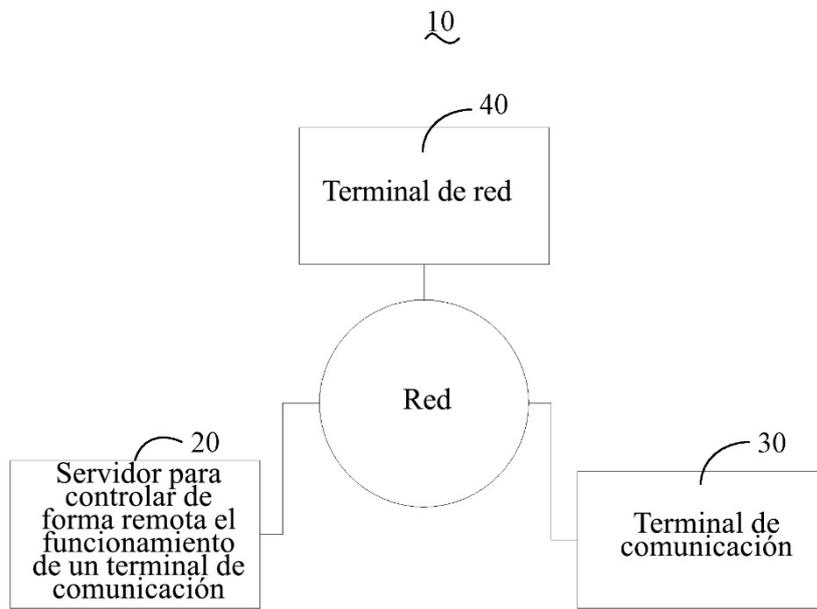


FIG. 1

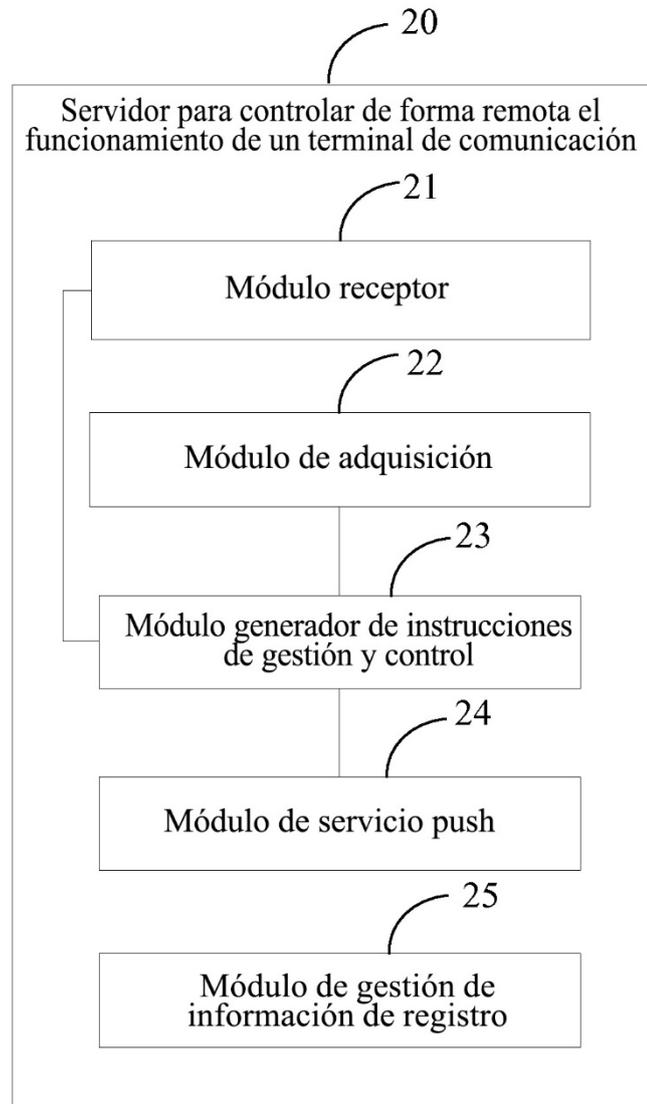


FIG. 2

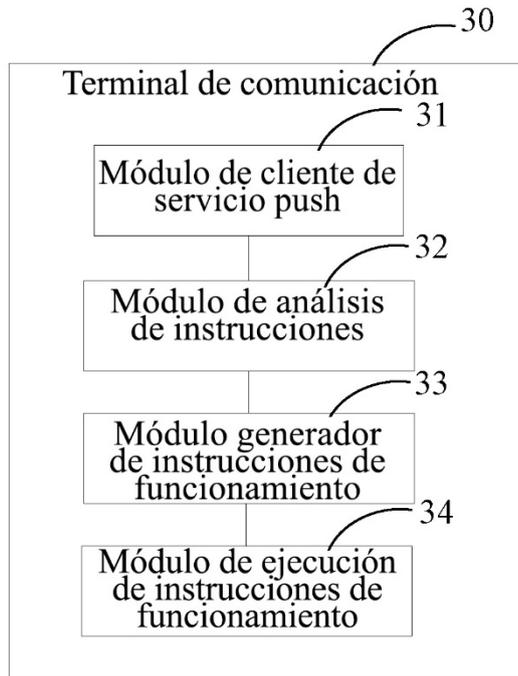


FIG. 3

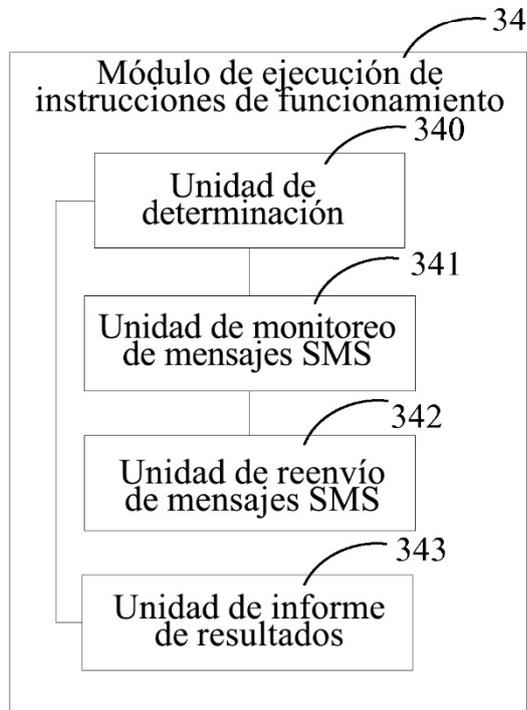


FIG. 4

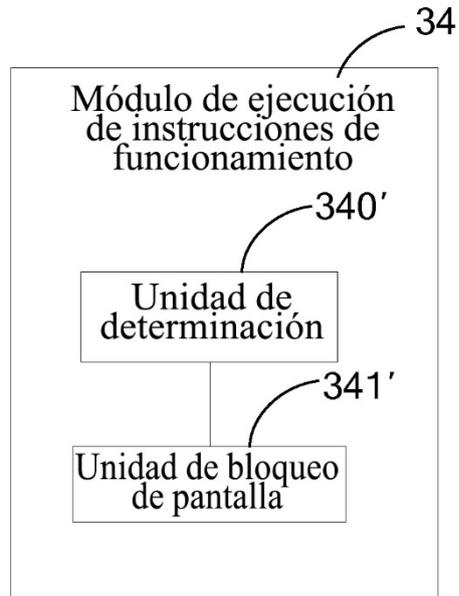


FIG. 5

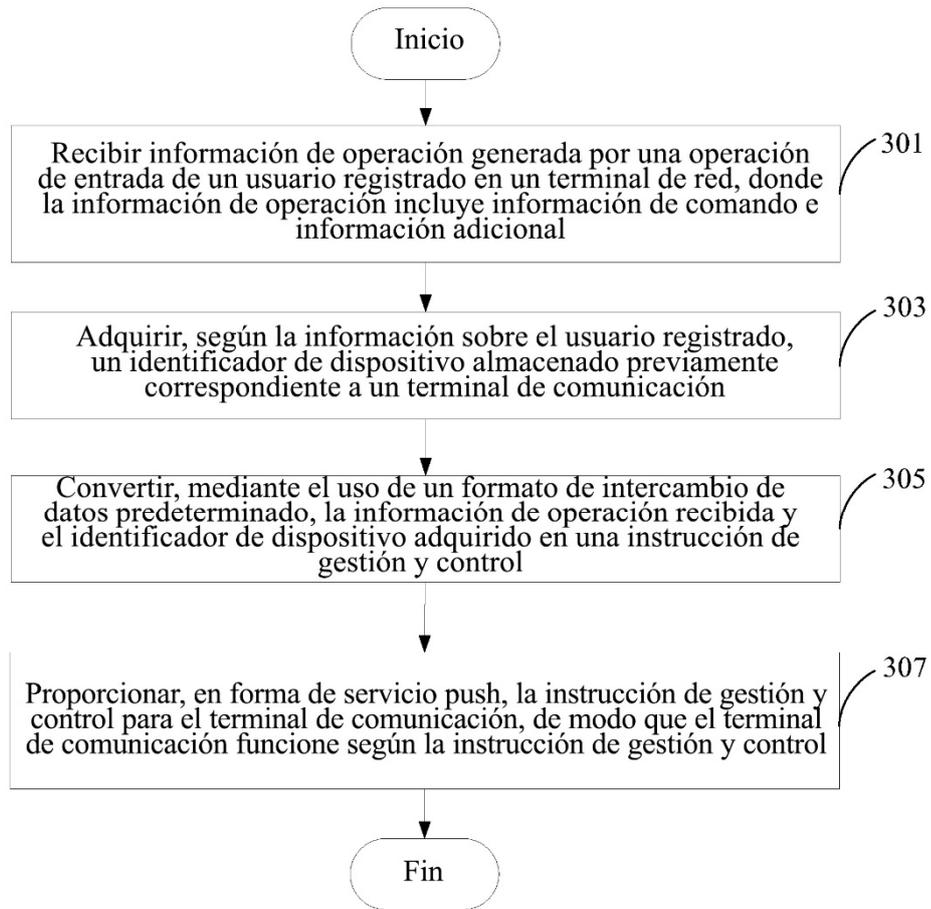


FIG. 6

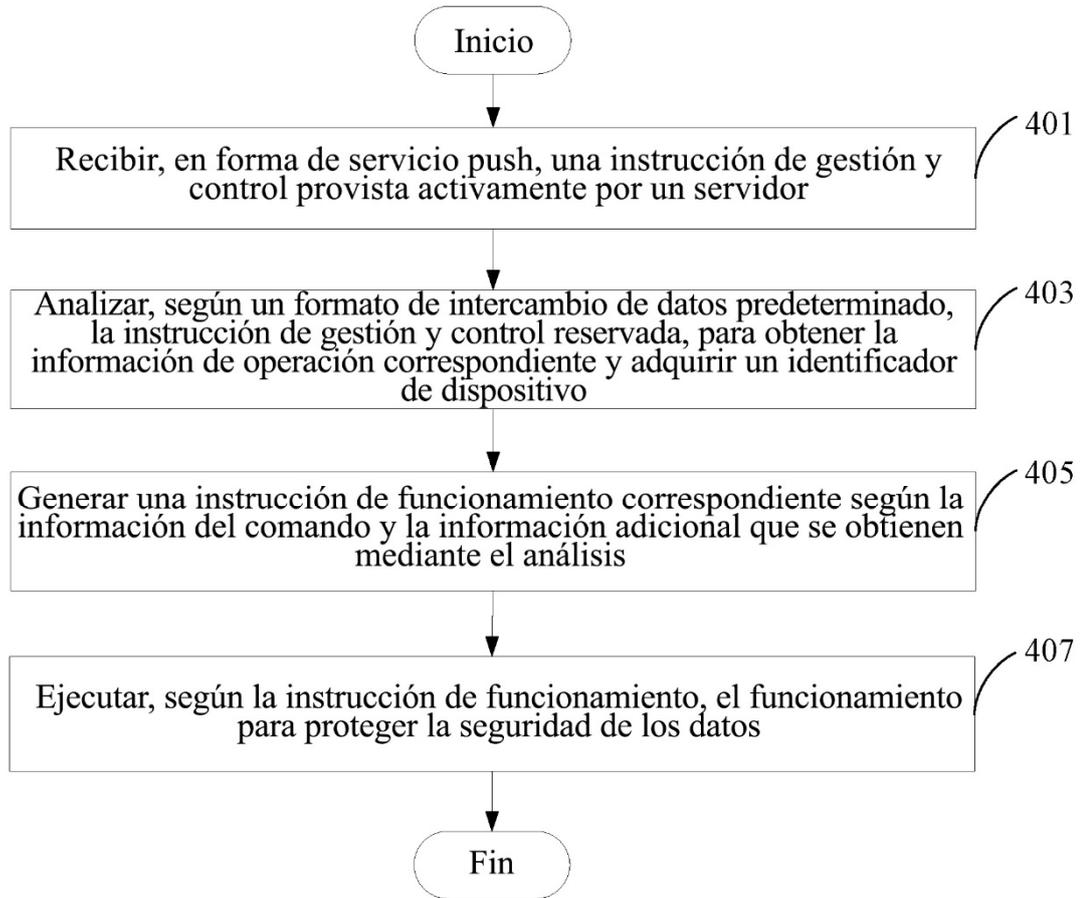


FIG. 7