(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 914 087**

(51) Int. CI.:

G06F 21/31 (2013.01)
G06F 21/34 (2013.01)
G06F 21/45 (2013.01)
G06F 21/46 (2013.01)
H04L 9/08 (2006.01)
H04L 9/30 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.11.2015 PCT/CN2015/095447**

(87) Fecha y número de publicación internacional: **15.12.2016 WO16197555**

(96) Fecha de presentación y número de la solicitud europea: **24.11.2015 E 15894810 (9)**

(97) Fecha y número de publicación de la concesión europea: **20.04.2022 EP 3309997**

(54) Título: **Aparato de monitoreo de red y procedimiento de cifrado remoto y activación remota, dispositivo y sistema para el mismo**

(30) Prioridad:

11.06.2015 CN 201510320504

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.06.2022

(73) Titular/es:

HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD. (100.0%)
No. 555 Qianmo Road 700, Dongliu Road
Hikvision Technology Area Binjiang District
Hangzhou, Zhejiang 310051, CN

(72) Inventor/es:

ZHU, ZHENLEI;
PAN, YADONG;
LI, KUI;
SI, LUJIE y
ZHANG, XIAOYUAN

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Aparato de monitoreo de red y procedimiento de cifrado remoto y activación remota, dispositivo y sistema para el mismo

Campo técnico

La presente invención se refiere al campo técnico de la seguridad de la red, y en particular a un aparato de monitoreo de red, y un procedimiento, dispositivo y sistema de cifrado remoto y activación remota del mismo.

Antecedentes

En la actualidad, en una industria de monitoreo de seguridad, la configuración de fábrica de un aparato de monitoreo de red tiene los siguientes problemas.

La configuración de fábrica del aparato de monitoreo de red tiene un nombre de usuario y una contraseña predeterminados (por ejemplo, un nombre de usuario de administrador predeterminado: admin, y una contraseña de administrador predeterminada: 12345). Un procedimiento general actual para una situación de un nombre de usuario predeterminado y una contraseña predeterminada es recordarle al usuario que debe cambiar la contraseña predeterminada cuando inicie sesión. Sin embargo, este recordatorio puede ignorarse por el usuario. En realidad, pocos usuarios optarán por cambiar las contraseñas predeterminadas. En esta situación, es más probable que el aparato de monitoreo de red que adopta la contraseña predeterminada, en particular cuando se conecta a una World Wide Web, se controle ilegalmente. Los documentos CN101453325, US2004/073815, US2007/257768, US2015/067760 son documentos pertinentes de la técnica anterior.

Sumario

La invención se define por las reivindicaciones independientes y las realizaciones preferentes definidas por las reivindicaciones dependientes.

Al menos, algunas realizaciones de la presente invención proporcionan un aparato de monitoreo de red, y un procedimiento, dispositivo y sistema de cifrado remoto y activación remota del mismo.

En una realización de la presente invención, se proporciona un procedimiento de activación remota de un aparato de monitoreo de red. El procedimiento incluye: recibir una contraseña de activación cifrada enviada por un terminal de cliente; descifrar la contraseña de activación cifrada para obtener una contraseña de activación original; determinar si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado; cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, activar el aparato de monitoreo de red y establecer la contraseña de activación original como una contraseña de administrador; y devolver información que indica que el aparato de monitoreo de red se active con éxito al terminal de cliente.

En una realización ejemplar, recibir la contraseña de activación cifrada enviada por el terminal de cliente incluye: recibir una clave pública enviada por el terminal de cliente y generada a través de un primer algoritmo, cifrar una cadena aleatoria original generada por el aparato de monitoreo de red a través de la clave pública para generar una cadena aleatoria cifrada, que devuelve la cadena aleatoria cifrada al terminal de cliente; y recibir una contraseña de activación enviada por el terminal de cliente y cifrada a través de un segundo algoritmo, y la contraseña de activación se genera al cifrar una contraseña de activación original a través del segundo algoritmo, y una clave del segundo algoritmo es la cadena aleatoria original.

En una realización ejemplar, descifrar la contraseña de activación cifrada para obtener la contraseña de activación original incluye: descifrar la contraseña de activación a través de un segundo algoritmo para obtener la contraseña de activación original.

En una realización ejemplar, antes de recibir la clave pública enviada por el terminal de cliente y generada a través del primer algoritmo, que incluye, además: informar una dirección de control de acceso a medios (MAC) al terminal de cliente, y la dirección MAC se usa para identificar de forma única una identidad del aparato de monitoreo de red.

En una realización ejemplar, recibir la clave pública enviada por el terminal de cliente y generada a través del primer algoritmo incluye: recibir una clave pública que coincida con una dirección MAC del aparato de monitoreo de red, enviada por el terminal de cliente y generada a través del primer algoritmo.

En una realización ejemplar, devolver la cadena aleatoria cifrada al terminal de cliente incluye, además: informar una dirección MAC al terminal de cliente, y la dirección MAC se usa para identificar de manera única una identidad del aparato de monitoreo de red.

En una realización ejemplar, recibir la contraseña de activación enviada por el terminal de cliente y cifrada a través del segundo algoritmo incluye: recibir una contraseña de activación que coincida con una dirección MAC del aparato de monitoreo de red, enviada por el terminal de cliente y cifrada a través del segundo algoritmo.

En una realización ejemplar, el primer algoritmo es un algoritmo de cifrado asimétrico RSA.

En una realización ejemplar, el segundo algoritmo es un algoritmo de cifrado simétrico de Estándar de Cifrado Avanzado (AES).

En el procedimiento de activación remota del aparato de monitoreo de red provisto en, al menos, algunas realizaciones de la presente invención, no se establece una contraseña predeterminada para el aparato de monitoreo de red, y el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red puede usarse después de activarse por un usuario, de modo que se cambia el viejo mal hábito de usar siempre la contraseña predeterminada por parte del usuario. Además, una contraseña de activación original ingresada por el usuario se encuentra sujeta a verificación de seguridad, y no se permite usar una contraseña demasiado simple para activar el aparato de monitoreo de red, de modo que un usuario ilegal no puede controlar remotamente el aparato de monitoreo mediante el uso de la contraseña predeterminada o adivinar una contraseña actual que es demasiado simple, y mejora así la seguridad de la contraseña. Además, al menos, una realización de la presente invención combina un algoritmo de cifrado asimétrico RSA y un algoritmo de cifrado simétrico AES en un procedimiento de cifrado de una contraseña de activación original ingresada por un usuario, y es difícil descifrar la contraseña de activación ingresada por el usuario desde una red, y mejora así aún más la seguridad de un procedimiento de activación.

En otra realización de la presente invención, se proporciona un aparato de monitoreo de red. El aparato de monitoreo de red incluye: una interfaz, dispuesta para recibir una contraseña de activación cifrada enviada por un terminal de cliente; un elemento de cifrado y descifrado, dispuesto para descifrar la contraseña de activación cifrada para obtener una contraseña de activación original; un elemento de determinación, dispuesto para determinar si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado; un elemento de activación, dispuesto para activar, cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red y establecer la contraseña de activación original como una contraseña de administrador; y la interfaz, dispuesta además para devolver información que indique que el aparato de monitoreo de red se activó con éxito al terminal de cliente.

En una realización ejemplar, la interfaz se dispone para recibir una clave pública enviada por el terminal de cliente y generada a través de un primer algoritmo, y devolver una cadena aleatoria cifrada al terminal de cliente, y la cadena aleatoria cifrada se obtiene al cifrar, mediante el elemento de cifrado y descifrado, una cadena aleatoria original generada por el aparato de monitoreo de red a través de la clave pública; y la interfaz se dispone además para recibir una contraseña de activación enviada por el terminal de cliente y cifrada a través de un segundo algoritmo, y la contraseña de activación se genera al cifrar, por parte del terminal de cliente, la contraseña de activación original a través del segundo algoritmo y una clave del segundo algoritmo es la cadena aleatoria original.

En una realización ejemplar, el elemento de cifrado y descifrado se dispone para descifrar la contraseña de activación cifrada a través de un segundo algoritmo para obtener la contraseña de activación original.

En una realización ejemplar, la interfaz se dispone además para, antes de recibir la clave pública enviada por el terminal de cliente y generada a través del primer algoritmo, informar una dirección de control de acceso a medios (MAC) al terminal de cliente, y la dirección MAC se usa para identificar de forma única una identidad del aparato de monitoreo de red.

En una realización ejemplar, la interfaz se configura para recibir una clave pública enviada por el terminal de cliente y generada a través del primer algoritmo que incluye el siguiente paso: recibir una clave pública que coincide con una dirección MAC del aparato de monitoreo de red, enviada por el terminal de cliente y generado a través del primer algoritmo.

En una realización ejemplar, la interfaz se dispone además para, además de devolver la cadena aleatoria cifrada al terminal de cliente, informar una dirección MAC al terminal de cliente, y la dirección MAC se usa para identificar de manera única una identidad del aparato de monitoreo de red.

En una realización ejemplar, la interfaz se configura para recibir la contraseña de activación enviada por el terminal de cliente y cifrada a través del segundo algoritmo que incluye el siguiente paso: recibir una contraseña de activación que coincida con una dirección MAC del aparato de monitoreo de red, enviada por el terminal de cliente y encriptado a través del segundo algoritmo.

En una realización ejemplar, el primer algoritmo es un algoritmo de cifrado asimétrico RSA.

En una realización ejemplar, el segundo algoritmo es un algoritmo de cifrado simétrico de Estándar de Cifrado Avanzado (AES).

En el aparato de monitoreo de red proporcionado en, al menos, algunas realizaciones de la presente invención, no se establece una contraseña predeterminada para el aparato de monitoreo de red, y el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red puede usarse después de activarse por un usuario, de modo que se cambia una vieja mala costumbre de usar siempre la contraseña predeterminada por parte del usuario. Además, una contraseña de activación original ingresada por el usuario se encuentra sujeta a una verificación de seguridad, y no se permite usar una contraseña demasiado simple para activar el dispositivo, de modo que un usuario ilegal no puede controlar de forma remota el aparato de monitoreo mediante el uso de la contraseña predeterminada o al adivinar una contraseña actual que es demasiado simple, lo que mejora la seguridad de la contraseña. Además, la presente invención combina un algoritmo de cifrado asimétrico RSA y un algoritmo de cifrado simétrico AES en un procedimiento de cifrado de una contraseña de activación original ingresada por un usuario, y es difícil descifrar la contraseña de activación ingresada por el usuario desde una red, por lo que se mejora la seguridad de un procedimiento de activación.

En otra realización de la presente invención, se proporciona un procedimiento de cifrado de un aparato de monitoreo de red en base a un terminal de cliente. El procedimiento incluye: recibir una contraseña de activación original de un aparato de monitoreo de red; cifrar la contraseña de activación original; enviar una contraseña de activación cifrada al aparato de monitoreo de red; y después de que el aparato de monitoreo de red se active con éxito de acuerdo con la contraseña de activación cifrada, recibir información, que indica que el aparato de monitoreo de red se activó con éxito, devuelta desde el aparato de monitoreo de red.

En una realización ejemplar, el envío de la contraseña de activación cifrada al aparato de monitoreo de red incluye: generar una clave pública y una clave privada a través de un primer algoritmo, enviar la clave pública al aparato de monitoreo de red y la clave pública se adopta por el aparato de monitoreo de red para cifrar la cadena aleatoria original generada por el aparato de monitoreo de red para generar una cadena aleatoria cifrada; recibir la cadena aleatoria cifrada enviada por el aparato de monitoreo de red, descifrar la cadena aleatoria cifrada a través de la clave privada para obtener la cadena aleatoria original y establecer la cadena aleatoria original como clave de un segundo algoritmo; y cifrar la contraseña de activación original a través del segundo algoritmo para obtener la contraseña de activación cifrada.

En una realización ejemplar, antes de enviar la clave pública al aparato de monitoreo de red, el procedimiento incluye, además: recibir una dirección de control de acceso a medios (MAC) enviada por el aparato de monitoreo de red, y la dirección MAC se usa para identificar de manera única una identidad del aparato de monitoreo de red.

En una realización ejemplar, enviar la clave pública al aparato de monitoreo de red incluye: enviar una clave pública que coincida con una dirección MAC del aparato de monitoreo de red al aparato de monitoreo de red.

En una realización ejemplar, recibir la cadena aleatoria cifrada enviada por el aparato de monitoreo de red incluye, además: recibir una dirección MAC enviada por el aparato de monitoreo de red, y la dirección MAC se usa para identificar de manera única una identidad del aparato de monitoreo de red.

En una realización ejemplar, enviar la contraseña de activación cifrada al aparato de monitoreo de red incluye: enviar una contraseña de activación que coincida con una dirección MAC del aparato de monitoreo de red al aparato de monitoreo de red.

En una realización ejemplar, el primer algoritmo es un algoritmo de cifrado asimétrico RSA, y el segundo algoritmo es un algoritmo de cifrado simétrico del Estándar de cifrado avanzado (AES).

En el procedimiento de cifrado del aparato de monitoreo de red en base al terminal de cliente provisto en, al menos, algunas realizaciones de la presente invención, no se establece una contraseña predeterminada para el aparato de monitoreo de red, y el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red puede usarse después de que un usuario lo active, de modo que se cambia el antiguo mal hábito de usar siempre la contraseña predeterminada por parte del usuario. Además, una contraseña de activación original ingresada por el usuario se encuentra sujeta a una verificación de seguridad, y no se permite usar una contraseña demasiado simple para activar el dispositivo, de modo que un usuario ilegal no puede controlar de forma remota el aparato de monitoreo mediante el uso de la contraseña predeterminada o al adivinar una contraseña actual que es demasiado simple, lo que mejora la seguridad de la contraseña. Además, la presente invención combina un algoritmo de cifrado asimétrico RSA y un algoritmo de cifrado simétrico AES en un procedimiento de cifrado de una contraseña de activación original ingresada por un usuario, y es difícil descifrar la contraseña de activación ingresada por el usuario desde una red, por lo que se mejora la seguridad de un procedimiento de activación.

En otra realización de la presente invención, se proporciona un terminal de cliente. El terminal de cliente incluye: una interfaz, dispuesta para recibir una contraseña de activación original de un aparato de monitoreo de red; un elemento de cifrado y descifrado, dispuesto para cifrar la contraseña de activación original; y la interfaz, dispuesta además

para enviar una contraseña de activación cifrada al aparato de monitoreo de red, y recibir, después de que el aparato de monitoreo de red se active con éxito de acuerdo con la contraseña de activación cifrada, información que indica que el aparato de monitoreo de red se activó con éxito, devuelta desde el aparato de monitoreo de red.

En una realización ejemplar, el elemento de cifrado y descifrado se dispone para generar una clave pública y una clave privada a través de un primer algoritmo, y envía la clave pública al aparato de monitoreo de red a través de la interfaz, y la clave pública se adopta por el aparato de monitoreo de red para cifrar la cadena aleatoria original generada por el aparato de monitoreo de red para generar una cadena aleatoria cifrada; la interfaz se dispone para recibir la cadena aleatoria cifrada enviada por el aparato de monitoreo de red, descifrar la cadena aleatoria cifrada a través de la clave privada para obtener la cadena aleatoria original y establecer la cadena aleatoria original obtenida como clave de un segundo algoritmo; y el elemento de cifrado y descifrado se dispone para cifrar la contraseña de activación original a través del segundo algoritmo para obtener la contraseña de activación cifrada.

En una realización ejemplar, la interfaz se configura además para, antes de enviar la clave pública al aparato de monitoreo de red, recibir una dirección de control de acceso a medios (MAC) enviada por el aparato de monitoreo de red, y la dirección MAC se usa para identificar de manera única una identidad del aparato de monitoreo de red.

En una realización ejemplar, la interfaz se dispone para enviar la clave pública al aparato de monitoreo de red e incluye el siguiente paso: enviar una clave pública que coincida con una dirección MAC del aparato de monitoreo de red al aparato de monitoreo de red.

En una realización ejemplar, la interfaz se dispone para recibir la cadena aleatoria cifrada enviada por el aparato de monitoreo de red e incluye además el siguiente paso: recibir una dirección MAC enviada por el aparato de monitoreo de red, y la dirección MAC se usa para identificar de manera única una identidad del aparato de monitoreo de red.

En una realización ejemplar, la interfaz se configura para enviar la contraseña de activación cifrada al aparato de monitoreo de red e incluye el siguiente paso: enviar una contraseña de activación que coincida con una dirección MAC del aparato de monitoreo de red al aparato de monitoreo de red.

En una realización ejemplar, el primer algoritmo es un algoritmo de cifrado asimétrico RSA, y el segundo algoritmo es un algoritmo de cifrado simétrico del estándar de cifrado avanzado (AES).

En el terminal de cliente provisto en, al menos, algunas realizaciones de la presente invención, no se establece una contraseña predeterminada para el aparato de monitoreo de red, y el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red puede usarse después de activarse por un usuario, por lo que se cambia un viejo mal hábito de usar siempre la contraseña predeterminada por el usuario. Además, una contraseña de activación original ingresada por el usuario se encuentra sujeta a una verificación de seguridad, y no se permite usar una contraseña demasiado simple para activar el dispositivo, de modo que un usuario ilegal no puede controlar de forma remota el aparato de monitoreo mediante el uso de la contraseña predeterminada o al adivinar una contraseña actual que es demasiado simple, lo que mejora la seguridad de la contraseña. Además, la presente invención combina un algoritmo de cifrado asimétrico RSA y un algoritmo de cifrado simétrico AES en un procedimiento de cifrado de una contraseña de activación original ingresada por un usuario, y es difícil descifrar la contraseña de activación ingresada por el usuario desde una red, por lo que se mejora la seguridad de un procedimiento de activación.

En otra realización de la presente invención, se proporciona un sistema de activación remota en base a un aparato de monitoreo de red. El sistema incluye: un terminal de cliente, dispuesto para recibir una contraseña de activación original de un aparato de monitoreo de red, y cifrar la contraseña de activación original; y el aparato de monitoreo de red, dispuesto para recibir una contraseña de activación cifrada desde el terminal de cliente, descifrar la contraseña de activación cifrada para obtener la contraseña de activación original, determinar si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado, activar, cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red y establece la contraseña de activación original como una contraseña de administrador, y devuelve información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente; el terminal de cliente, dispuesto además para enviar, después de recibir la información que indica que el aparato de monitoreo de red se activó con éxito, un aviso que indica que el aparato de monitoreo de red se activó con éxito.

En una realización ejemplar, el terminal de cliente se dispone para recibir la contraseña de activación original de un aparato de monitoreo de red y cifrar la contraseña de activación original que incluye el siguiente paso: enviar una clave pública generada a través de un primer algoritmo al aparato de monitoreo de red, y la clave pública se adopta por el aparato de monitoreo de red para cifrar la cadena aleatoria original generada por el aparato de monitoreo de red para generar una cadena aleatoria cifrada; y desencriptar la cadena aleatoria cifrada devuelta por el aparato de monitoreo de red mediante el uso de una clave privada generada a través del primer algoritmo para obtener la cadena aleatoria original, y establecer la cadena aleatoria original como clave de un segundo algoritmo, al encriptar la contraseña de activación original a través del segundo algoritmo para obtener una contraseña de activación cifrada, y enviar la contraseña de activación cifrada al aparato de monitoreo de red.

En el sistema de activación remota en base al aparato de monitoreo de red provisto en, al menos, algunas realizaciones de la presente invención, no se establece una contraseña predeterminada para el aparato de monitoreo de red, y el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red puede usarse después de activarse por un usuario, de modo que se cambia el antiguo mal hábito de usar siempre la contraseña predeterminada por parte del usuario. Además, una contraseña de activación original ingresada por el usuario se encuentra sujeta a verificación de seguridad, y no se permite usar una contraseña demasiado simple para activar el dispositivo, de modo que un usuario ilegal no puede controlar de forma remota el aparato de monitoreo mediante el uso de la contraseña predeterminada o al adivinar una contraseña actual que es demasiado simple, lo que mejora la seguridad de la contraseña. Además, la presente invención combina un algoritmo de cifrado asimétrico RSA y un algoritmo de cifrado simétrico AES en un procedimiento de cifrado de una contraseña de activación original ingresada por un usuario, y es difícil descifrar la contraseña de activación ingresada por el usuario desde una red, por lo que se mejora la seguridad de un procedimiento de activación.

Breve descripción de los dibujos

Con el fin de ilustrar más claramente las soluciones técnicas en las realizaciones de la presente invención o la técnica relacionada, simplemente se presentarán los dibujos que es necesario usar en las realizaciones. Obviamente, los dibujos descritos a continuación son solamente algunas de las realizaciones de la presente descripción. Bajo la premisa de que no hay trabajo creativo, una persona con conocimientos ordinarios en la técnica también puede obtener otros dibujos de acuerdo con estos dibujos. Como se muestra en los dibujos, los propósitos, características y ventajas mencionados anteriormente y otros de la presente invención serán más claros. La misma marca de dibujo en todos los dibujos indica la misma parte. Los dibujos no se dibujan a escala igual de acuerdo con los tamaños reales a propósito. Se enfoca la demostración de la sustancia de la presente invención.

La Figura 1 es un diagrama de flujo de un procedimiento de activación remota de un aparato de monitoreo de red de acuerdo con una realización ejemplar de la presente invención.
La Figura 2 es un diagrama de flujo de activación remota en base a una dirección de Protocolo de Internet (IP) de acuerdo con una realización ejemplar de la presente invención.
La Figura 3 es un diagrama de flujo de activación remota en base a una dirección MAC de acuerdo con una realización ejemplar de la presente invención.
La Figura 4 es un diagrama de bloques estructural de un aparato de monitoreo de red de acuerdo con una realización ejemplar de la presente invención.
La Figura 5 es un diagrama de flujo de un procedimiento de cifrado de un aparato de monitoreo de red en base a un terminal de cliente de acuerdo con una forma de realización ejemplar de la presente invención.
La Figura 6 es un diagrama de bloques estructural de un terminal de cliente de acuerdo con una realización ejemplar de la presente invención.
La Figura 7 es un diagrama de bloques estructural de un sistema de activación remota en base a un aparato de monitoreo de red de acuerdo con una realización ejemplar de la presente invención.
La Figura 8 es un diagrama de flujo de activación de un sistema de activación remota en base a un aparato de monitoreo de red de acuerdo con una realización ejemplar de la presente invención.

Descripción detallada

Para que un experto en la técnica comprenda mejor las soluciones de la presente invención, las soluciones técnicas en las realizaciones de la presente invención se describirán clara y completamente en la presente memoria con referencia a los dibujos en las realizaciones de la presente invención. Obviamente, las realizaciones descritas son una parte de las realizaciones de la presente invención, no todas las realizaciones. Sobre la base de las realizaciones de la presente invención, todas las demás realizaciones obtenidas bajo la premisa de que no hay trabajo creativo de una persona con conocimientos ordinarios en la técnica entran dentro del ámbito de protección de la presente invención.

Es importante señalar que la descripción y las reivindicaciones de la presente invención y los términos "primero", "segundo" y similares en los dibujos pretenden distinguir objetos similares y no necesitan describir una secuencia específica o un orden de precedencia. Debe entenderse que los datos usados de tal manera pueden intercambiarse en condiciones apropiadas, para que las realizaciones de la presente invención descritas aquí puedan implementarse en una secuencia excepto las secuencias mostradas o descritas gráficamente aquí. Además, los términos "incluir" y "tener" y cualquier variación de los términos pretenden cubrir inclusiones no exclusivas. Por ejemplo, los procesos, procedimientos, sistemas, productos o dispositivos que contengan una serie de pasos o elementos no necesitan enumerar claramente esos pasos o elementos, y pueden incluir otros pasos o elementos inherentes a estos procesos, procedimientos, productos o dispositivos, que se enumeran claramente.

Para resolver problemas en la técnica relacionada, en la presente invención se proporcionan un aparato de monitoreo de red y un procedimiento, dispositivo y sistema de cifrado remota y activación remota del aparato de monitoreo de red. Al volver a cifrar una contraseña de activación original ingresada por un usuario, es difícil descifrar la contraseña de activación original en una red, y mejora así la seguridad de un procedimiento de activación. En la presente memoria, el aparato de monitoreo de red se refiere a un aparato de monitoreo de seguridad que se

proporciona con un componente de red y se accede a través de una dirección IP, como una grabadora de video digital (DVR), un servidor de video digital (DVS), una grabadora de video en red (NVR), una grabadora de video central (CVR), una cámara IP (IPC) y un dispositivo de transmisión y visualización.

La Figura 1 es un diagrama de flujo de un procedimiento de activación remota de un aparato de monitoreo de red de acuerdo con una realización ejemplar de la presente invención. Es importante señalar que un objeto ejecutado del procedimiento de activación remota del aparato de monitoreo de red es el aparato de monitoreo de red. Es decir, el aparato de monitoreo de red completa los pasos de la siguiente manera.

En el paso S11, se recibe una contraseña de activación cifrada enviada por un terminal de cliente.

Después de arrancar, el usuario accede al aparato de monitoreo de red a través del terminal de cliente. Dado que el aparato de monitoreo de red aún no se encuentra activado en este momento, un dispositivo no activado no puede ejecutar ninguna otra operación, como la modificación de una dirección IP. Cuando el aparato de monitoreo de red se activa por completo, pueden realizarse operaciones de red.

El aparato de monitoreo de red informa al terminal de cliente que el aparato de monitoreo de red puede usarse después de que se active el aparato de monitoreo de red. Y después de que el usuario ingrese una contraseña de activación original, el terminal de cliente cifra la contraseña de activación original y luego envía una contraseña de activación cifrada al aparato de monitoreo de red.

En el paso S12, la contraseña de activación cifrada se descifra para obtener la contraseña de activación original.

El aparato de monitoreo de red descifra la contraseña de activación cifrada recibida en el paso S11, para obtener la contraseña de activación original introducida por el usuario.

En el paso S13, se determina si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado, y cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red se activa y la contraseña de activación original se establece como contraseña de administrador.

El aparato de monitoreo de red analiza la complejidad de la contraseña de activación original descifrada, es decir, comprueba si la complejidad (es decir, la seguridad de la contraseña) de una contraseña establecida por el usuario cumple el requisito de seguridad de contraseña predeterminado. Por ejemplo, el requisito de seguridad de contraseña predeterminado satisface las siguientes condiciones: combinación de números, letras mayúsculas y minúsculas, y una longitud de contraseña de, al menos, 8 bits. En este momento, cuando una contraseña de activación original ingresada por el usuario es U0123CRRT, se determina que la contraseña califica debido al hecho de que la contraseña no tiene letras minúsculas y la longitud de la contraseña no alcanza los 8 bits.

Cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, se activa el aparato de monitoreo de red. Y la contraseña de activación original se configura como una contraseña de administrador del aparato de monitoreo de red. Cuando la contraseña de activación original no cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red devuelve información al terminal de cliente, y esta información se usa para indicar que el aparato de monitoreo de red no se activó con éxito.

En el paso S14, la información que indica que el aparato de monitoreo de red se activó con éxito se devuelve al terminal de cliente.

Después de activarse con éxito, el aparato de monitoreo de red envía información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente. El terminal de cliente le recuerda al usuario que el aparato de monitoreo de red se activó con éxito. Y luego el usuario inicia sesión en el aparato de monitoreo de red como administrador mediante el uso de la contraseña de activación original establecida y realiza otras operaciones de red.

Es importante señalar que el procedimiento de activación remota del aparato de monitoreo de red de la presente invención incluye: un modo de activación en base a una dirección IP y un modo de activación en base a una dirección MAC de acuerdo con diferentes modos de interacción de red. La diferencia entre los dos modos de activación radica en la interacción de la red y los modos de cifrado de los dos modos de activación son consistentes.

Los dos modos de activación se ilustran en la presente memoria con referencia a la Figura 2 y la Figura 3 respectivamente.

La Figura 2 es un diagrama de flujo de activación remota en base a una dirección IP de acuerdo con una realización ejemplar de la presente invención. El modo de activación en base a la dirección IP se refiere a la activación a través de una conexión de red direccional a un determinado aparato de monitoreo de red.

En el paso S21, un terminal de cliente solicita un primer algoritmo para generar una clave pública y una clave privada, y el terminal de cliente envía la clave pública a un aparato de monitoreo de red no activado.

En el paso S22, el aparato de monitoreo de red recibe la clave pública generada por el terminal de cliente a través del primer algoritmo y cifra una cadena aleatoria original generada por el aparato de monitoreo de red a través de la clave pública para generar una cadena aleatoria cifrada. El aparato de monitoreo de red devuelve la cadena aleatoria cifrada al terminal de cliente. Específicamente, el aparato de monitoreo de red cifra una cadena aleatoria original (una cadena aleatoria generada sin ninguna operación de cifrado) a través de la clave pública para obtener una cadena aleatoria cifrada y devuelve la cadena aleatoria cifrada al terminal de cliente.

En el paso S23, el terminal de cliente descifra la cadena aleatoria cifrada a través del primer algoritmo para obtener la cadena aleatoria original.

En el paso S24, el terminal de cliente establece la cadena aleatoria original descifrada como clave de cifrado de un segundo algoritmo y cifra una contraseña de activación original a través del segundo algoritmo para obtener una contraseña de activación. Luego, la contraseña de activación se envía al aparato de monitoreo de red.

En el paso S25, el aparato de monitoreo de red recibe la contraseña de activación cifrada por el terminal de cliente a través del segundo algoritmo. Dado que la contraseña de cifrado es la cadena aleatoria original generada por el aparato de monitoreo de red, el aparato de monitoreo de red descifra la contraseña de activación a través del segundo algoritmo para obtener la contraseña de activación original.

En el paso S26, el aparato de monitoreo de red determina si la complejidad de la contraseña de activación original descifrada cumple con un requisito de seguridad de contraseña predeterminado. Cuando una complejidad de la contraseña de activación original descifrada cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red se activa y la información que indica que el aparato de monitoreo de red se activó con éxito se devuelve al terminal de cliente.

En el paso S27, el terminal de cliente indica al usuario que el aparato de monitoreo de red se activó con éxito.

La Figura 3 es un diagrama de flujo de activación remota en base a una dirección MAC de acuerdo con una realización ejemplar de la presente invención. Dado que la configuración de fábrica de un aparato de monitoreo de red incluye normalmente una dirección IP fija, las direcciones IP son idénticas cuando se juntan muchos dispositivos. En este caso, un modo de activación en base a una dirección IP no puede determinar visualmente el aparato de monitoreo de red activado en este modo. Una dirección MAC es única para cada aparato de monitoreo de red. Es decir, la dirección MAC se usa para identificar de manera única una identidad de cada aparato de monitoreo de red. Por lo tanto, el modo de activación en base a la dirección MAC resuelve el problema mencionado anteriormente y la interacción de la red se realiza a través de multidifusión.

Es importante señalar que, en los pasos siguientes, dado que hay múltiples aparatos de monitoreo de red, la interacción de red entre un terminal de cliente y múltiples aparatos de monitoreo de red se realiza en forma de multidifusión. La multidifusión es un modo de comunicación de uno a múltiples puntos, la información enviada entre los aparatos de monitoreo de red y el terminal de cliente se envía primero a un grupo de multidifusión específico, y cualquier dispositivo de red que se una a este grupo de multidifusión recibe datos. La dirección MAC se establece como base de coincidencia de cada aparato de monitoreo de red, de modo que el terminal de cliente pueda determinar visualmente el aparato de monitoreo de red que se encuentra activado actualmente. El modo se aplica particularmente a un escenario donde los aparatos de monitoreo de red se activan en lotes y se ahorra ancho de banda de red.

En el paso S31, se comunica una dirección MAC de un aparato de monitoreo de red a un terminal de cliente.

Cada aparato de monitoreo de red envía una dirección MAC propia al terminal de cliente en forma de multidifusión.

En el paso S32, el terminal de cliente genera una clave pública y una clave privada a través de un primer algoritmo y envía la clave pública y una dirección MAC al aparato de monitoreo de red.

En el paso S33, el aparato de monitoreo de red determina si la dirección MAC recibida coincide con la dirección MAC del aparato de monitoreo de red. Y cuando la dirección MAC recibida se compara con la dirección MAC del aparato de monitoreo de red, se ejecuta el paso S34. En otras palabras, el aparato de monitoreo de red recibe la clave pública que coincide con la dirección MAC del aparato de monitoreo de red, y se ejecuta el paso S34.

En el paso S34, el aparato de monitoreo de red genera una cadena aleatoria original, cifra la cadena aleatoria original a través de la clave pública para obtener una cadena aleatoria cifrada y envía la cadena aleatoria cifrada y la dirección MAC al terminal de cliente.

En el paso S35, el terminal de cliente descifra la cadena aleatoria cifrada a través de la clave privada del primer algoritmo para obtener la cadena aleatoria original, establece la cadena aleatoria original como clave de un segundo algoritmo, cifra una contraseña de activación original para obtener una contraseña de activación, y envía la contraseña de activación cifrada a través del segundo algoritmo y la dirección MAC al aparato de monitoreo de red.

En el paso S36, el aparato de monitoreo de red determina si la dirección MAC recibida se compara nuevamente con la dirección MAC del aparato de monitoreo de red, y cuando la dirección MAC recibida se compara con la dirección MAC del aparato de monitoreo de red, se ejecuta el paso S37. En otras palabras, el aparato de monitoreo de red recibe la clave pública que coincide con la dirección MAC del aparato de monitoreo de red, y se ejecuta el paso S37.

En el paso S37, el aparato de monitoreo de red descifra la contraseña de activación a través del segundo algoritmo. Dado que la contraseña de cifrado es la cadena aleatoria original generada por el aparato de monitoreo de red, el aparato de monitoreo de red descifra la contraseña de activación para obtener la contraseña de activación original.

En el paso S38, el aparato de monitoreo de red determina si la complejidad de la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado. Cuando la complejidad de la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red se activa y la información que indica que el aparato de monitoreo de red se activó con éxito se devuelve al terminal de cliente.

En el paso S39, el terminal de cliente indica al usuario que el aparato de monitoreo de red se activó con éxito.

En resumen, el modo de activación en base a la dirección MAC es idéntico al modo de activación en base a la dirección IP en términos de algoritmos de cifrado y contraseñas y son ligeramente diferentes en la interacción de la red. El modo de activación en base a la dirección MAC realiza una interacción de red uno a múltiple en forma de multidifusión.

En una realización de la presente invención, en el modo de activación en base a la dirección IP y el modo de activación en base a la dirección MAC, el primer algoritmo es un algoritmo RSA de cifrado asimétrico y el segundo algoritmo es un algoritmo de cifrado simétrico AES.

El algoritmo RSA es un algoritmo de cifrado asimétrico, un par de contraseñas que incluyen una clave pública y una clave privada se generan mediante el uso del algoritmo RSA. La clave pública se encuentra abierta al público y la clave privada se guarda por un generador. En la presente invención, la clave privada generada por el algoritmo RSA se guarda por un terminal de cliente generador. Durante el cifrado, los datos se cifran mediante el uso de la clave pública y los datos cifrados se descifran con la clave privada. Siempre que una contraseña sea lo suficientemente larga, la contraseña no puede descifrarse. Cuando el aparato de monitoreo de red se activa cada vez, se generará un nuevo par de contraseñas RSA, y la clave privada se almacena en la memoria de un terminal de cliente y es poco probable que se capture.

El algoritmo AES es un algoritmo de cifrado simétrico. Una parte de cifrado o una parte de descifrado, cifra o descifra los datos mediante el uso de la misma contraseña. Aunque el modo de cifrado simétrico no es seguro, dado que la divulgación preventiva realiza el procesamiento de cifrado del algoritmo RSA en la contraseña del algoritmo AES por adelantado, la contraseña no puede obtenerse mediante rastreo y otros medios, lo que mejora la seguridad del aparato de monitoreo de red.

En el procedimiento de activación remota de un aparato de monitoreo de red provisto en, al menos, algunas realizaciones de la presente invención, no se establece una contraseña predeterminada para el aparato de monitoreo de red, y el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red puede utilizarse después de activarse por el usuario, de modo que se cambia el antiguo mal hábito de usar siempre la contraseña predeterminada por parte del usuario. Además, una contraseña de activación original ingresada por el usuario se encuentra sujeta a verificación de seguridad, y no se permite usar una contraseña demasiado simple para activar el aparato de monitoreo de red, de modo que un usuario ilegal no puede controlar remotamente el aparato de monitoreo mediante el uso de la contraseña predeterminada o adivinar una contraseña actual que es demasiado simple, y mejora así la seguridad de la contraseña. Además, la presente invención combina un algoritmo de cifrado asimétrico RSA y un algoritmo de cifrado simétrico AES en un procedimiento de cifrado de la contraseña de activación original ingresada por el usuario, y es difícil descifrar la contraseña de activación ingresada por el usuario desde una red, y mejora así la seguridad de un procedimiento de activación.

La Figura 4 es un diagrama de bloques estructural de un aparato de monitoreo de red de acuerdo con una realización ejemplar de la presente invención.

Como se muestra en la Figura 4, el aparato de monitoreo de red proporcionado en la presente invención incluye: una interfaz 41, un elemento de cifrado y descifrado 42, un elemento de determinación 43 y un elemento de activación 44.

Específicamente, la interfaz 41 se dispone para recibir una contraseña de activación cifrada enviada por un terminal de cliente. Es decir, después de que el usuario ingresa una contraseña de activación original, el terminal de cliente cifra la contraseña de activación original y luego envía la contraseña de activación cifrada a la interfaz 41.

El elemento de cifrado y descifrado 42 se dispone para descifrar la contraseña de activación cifrada para obtener la contraseña de activación original.

El elemento de determinación 43 se dispone para determinar si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado. El elemento de determinación 43 analiza la complejidad de la contraseña de activación original descifrada, es decir, comprueba si la complejidad (es decir, la seguridad de la contraseña) de una contraseña establecida por el usuario cumple el requisito de seguridad de contraseña predeterminado. Por ejemplo, el requisito de seguridad de contraseña predeterminado satisface las siguientes condiciones: combinación de números, letras mayúsculas y minúsculas, y una longitud de contraseña de, al menos, 8 bits. En este momento, cuando una contraseña de activación original ingresada por el usuario es U0123CRRT, se determina que la contraseña no califica debido al hecho de que la contraseña no tiene letras minúsculas y la longitud de la contraseña no alcanza los 8 bits.

El elemento de activación 44 se dispone para activar, cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red y establecer la contraseña de activación original como una contraseña de administrador. Luego, la interfaz 41 devuelve información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente. Cuando la contraseña de activación original no cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red devuelve información al terminal de cliente, y esta información se usa para indicar que el aparato de monitoreo de red no se activó con éxito.

Es importante notar que el procedimiento de activación remota de un aparato de monitoreo de red de la presente invención incluye: un modo de activación en base a una dirección IP y un modo de activación en base a una dirección MAC de acuerdo con diferentes modos de interacción de red, y la diferencia entre los dos modos de activación radican en la interacción de la red, y los modos de cifrado de los dos modos de activación son consistentes.

Los dos modos de activación se ilustran en la presente memoria a continuación respectivamente. (1) Un modo de activación en base a una dirección IP: activación a través de una conexión de red direccional a un cierto aparato de monitoreo de red.

El terminal de cliente llama a un primer algoritmo para generar una clave pública y una clave privada, y el terminal de cliente envía la clave pública a la interfaz 41 no activada. La interfaz 41 recibe la clave pública generada por el terminal de cliente a través del primer algoritmo y devuelve una cadena aleatoria cifrada a través de la clave pública al terminal de cliente. La cadena aleatoria cifrada se obtiene al cifrar, mediante el elemento de cifrado y descifrado 42, una cadena aleatoria original generada por el aparato de monitoreo de red a través de la clave pública.

El terminal de cliente descifra la cadena aleatoria cifrada a través de la clave privada del primer algoritmo para obtener la cadena aleatoria original, establece la cadena aleatoria original descifrada como clave de cifrado de un segundo algoritmo, cifra una contraseña de activación original ingresada por un usuario a través del segundo algoritmo para obtener una contraseña de activación, y luego envía la contraseña de activación a la interfaz 41. La interfaz 41 recibe la contraseña de activación cifrada por el terminal de cliente a través del segundo algoritmo. El elemento de cifrado y descifrado 42 descifra la contraseña de activación a través del segundo algoritmo para obtener la contraseña de activación original. El elemento de determinación 43 determina si la complejidad de la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado. El elemento de activación 44 activa, cuando la complejidad de la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red y devuelve información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente. El terminal de cliente avisa además al usuario de que el aparato de monitoreo de red se activó con éxito.

(2) Un modo de activación en base a una dirección MAC: la dirección MAC es única para cada aparato de monitoreo de red. Es decir, la dirección MAC se usa para identificar de manera única la identidad del aparato de monitoreo de red. Por lo tanto, el modo de activación en base a una dirección MAC resuelve el problema mencionado anteriormente y la interacción de la red se realiza a través de multidifusión. Dado que existen múltiples aparatos de monitoreo de red, la interacción de red entre un terminal de cliente y múltiples aparatos de monitoreo de red se realiza en forma de multidifusión. La multidifusión es un modo de comunicación de uno a múltiples puntos, la información enviada entre los aparatos de monitoreo de red y el terminal de cliente se envía primero a un grupo de multidifusión específico, y cualquier dispositivo de red que se una a este grupo de multidifusión recibe datos. La dirección MAC se establece como base de coincidencia de cada aparato de monitoreo de red, de modo que el terminal de cliente pueda determinar visualmente el aparato de monitoreo de red que se encuentra activado actualmente. El modo se aplica particularmente a un escenario donde los aparatos de monitoreo de red se activan en lotes y se ahorra ancho de banda de red.

Cada aparato de monitoreo de red envía una dirección MAC al terminal de cliente en forma de multidifusión. El terminal de cliente genera una clave pública y una clave privada a través de un primer algoritmo y envía la clave pública y una dirección MAC a la interfaz 41. La interfaz 41 recibe la clave pública devuelta y la dirección MAC generada a través del primer algoritmo, y devuelve una cadena aleatoria cifrada a través de la clave pública al terminal de cliente después de determinar que la dirección MAC recibida coincide con la dirección MAC del presente aparato de monitoreo de red. Es decir, después de que el aparato de monitoreo de red recibe la clave pública que coincide con la dirección MAC del aparato de monitoreo de red, y el terminal de cliente descifra la cadena aleatoria cifrada a través de la clave privada del primer algoritmo para obtener una cadena aleatoria original, configura la cadena aleatoria original como clave de un segundo algoritmo, y cifra una contraseña de activación original ingresada por un usuario para obtener una contraseña de activación.

La interfaz 41 recibe una contraseña de activación cifrada por el terminal de cliente a través del segundo algoritmo y la dirección MAC, y la contraseña del segundo algoritmo es una cadena aleatoria original. Después de determinar que la dirección MAC recibida nuevamente coincide con la dirección MAC del presente aparato de monitoreo de red, es decir, después de que el aparato de monitoreo de red recibe la contraseña de activación que coincide con la dirección MAC del aparato de monitoreo de red, el elemento de cifrado y descifrado 42 descifra la contraseña de activación a través del segundo algoritmo para obtener la contraseña de activación original. El elemento de determinación 43 determina si la complejidad de la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado. El elemento de activación 44 activa, cuando la complejidad de la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red y devuelve información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente. El terminal de cliente avisa además al usuario de que el aparato de monitoreo de red se activó con éxito.

Es importante señalar que la interfaz 41, el elemento de cifrado y descifrado 42, el elemento de determinación 43 y el elemento de activación 44 se ejecutan en una terminal de computadora como parte del aparato, las funciones implementadas por los elementos pueden ejecutarse a través de un procesador en el terminal de computadora, y la terminal de computadora es un dispositivo de terminal como un teléfono inteligente (como un teléfono Android y un teléfono iOS), una tableta, una computadora de mano, dispositivos móviles de internet (MID) y un PAD.

En una realización de la presente invención, en un modo de activación en base a una dirección IP y un modo de activación en base a una dirección MAC, el primer algoritmo es un algoritmo de cifrado asimétrico RSA y el segundo algoritmo es un algoritmo de cifrado simétrico AES.

En el aparato de monitoreo de red proporcionado en, al menos, algunas realizaciones de la presente invención, no se establece una contraseña predeterminada para un aparato de monitoreo de red, y el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red puede utilizarse después de activarse por un usuario, de modo que se cambia una vieja mala costumbre de usar siempre la contraseña predeterminada por parte del usuario. Además, una contraseña de activación original ingresada por el usuario se encuentra sujeta a una verificación de seguridad, y no se permite usar una contraseña demasiado simple para activar el dispositivo, de modo que un usuario ilegal no puede controlar de forma remota el aparato de monitoreo mediante el uso de la contraseña predeterminada o al adivinar una contraseña actual que es demasiado simple, lo que mejora la seguridad de la contraseña. Además, la presente invención combina un algoritmo de cifrado asimétrico RSA y un algoritmo de cifrado simétrico AES en un procedimiento de cifrado de una contraseña de activación original ingresada por un usuario, y es difícil descifrar la contraseña de activación ingresada por el usuario desde una red, por lo que se mejora la seguridad de un procedimiento de activación.

La Figura 5 es un diagrama de flujo de un procedimiento de cifrado de un aparato de monitoreo de red en base a un terminal de cliente de acuerdo con un ejemplo de la presente invención. Es importante señalar que un objeto ejecutado del procedimiento de cifrado del aparato de monitoreo de red en base al terminal de cliente es el terminal de cliente, es decir, el terminal de cliente completa los pasos de la siguiente manera.

En el paso S51, se recibe una contraseña de activación original de un aparato de monitoreo de red.

En el paso S52, se cifra la contraseña de activación original.

Específicamente, el terminal de cliente envía además la contraseña de activación cifrada al aparato de monitoreo de red, y el aparato de monitoreo de red determina si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado, se activa, cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red, establece la contraseña de activación original como una contraseña de administrador y devuelve información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente.

Cuando se usa para activar el aparato de monitoreo de red, el procedimiento de cifrado del aparato de monitoreo de red en base al terminal de cliente de la presente invención incluye: un modo de activación en base a una dirección IP y un modo de activación en base a una dirección MAC de acuerdo con diferentes modos de interacción de red. La

diferencia entre dos modos de activación radica en la interacción de la red y los modos de cifrado de los dos modos de activación son consistentes.

(1) Modo de activación en base a la dirección IP

El terminal de cliente adopta un primer algoritmo para generar una clave pública y una clave privada y envía la clave pública al aparato de monitoreo de red. El aparato de monitoreo de red cifra una cadena aleatoria original generada por el aparato de monitoreo de red a través de la clave pública para generar una cadena aleatoria cifrada. El terminal de cliente recibe la cadena aleatoria cifrada enviada por el aparato de monitoreo de red, descifra la cadena aleatoria devuelta por el aparato de monitoreo de red y cifrada a través de la clave pública, y establece una cadena aleatoria original obtenida como clave de un segundo algoritmo. Luego, una entrada de contraseña de activación original por parte de un usuario se cifra a través del segundo algoritmo para obtener una contraseña de activación, y la contraseña de activación cifrada se envía al aparato de monitoreo de red.

(2) Modo de activación en base a la dirección MAC

El terminal de cliente recibe direcciones MAC notificadas por múltiples aparatos de monitoreo de red. Las direcciones MAC se usan para identificar de manera única la identidad del aparato de monitoreo de red. El terminal de cliente adopta un primer algoritmo para generar una clave pública y una clave privada, y envía la clave pública y la dirección MAC al aparato de monitoreo de red. Específicamente, el terminal de cliente envía la clave pública emparejada con la dirección MAC del aparato de monitoreo de red al aparato de monitoreo de red. El aparato de monitoreo de red cifra una cadena aleatoria original generada por el aparato de monitoreo de red a través de la clave pública para generar una cadena aleatoria cifrada. Luego, el terminal de cliente recibe la cadena aleatoria cifrada enviada por el aparato de monitoreo de red. Además, el paso de recibir, por parte del terminal de cliente, la cadena aleatoria cifrada enviada por el aparato de monitoreo de red incluye, además: recibir una dirección MAC enviada por el aparato de monitoreo de red, y la dirección MAC se usa para identificar de manera única la identidad del aparato de monitoreo de red.

El terminal de cliente descifra la cadena aleatoria cifrada a través de la clave privada y establece la cadena aleatoria original como clave de un segundo algoritmo. Una entrada de contraseña de activación original por parte de un usuario se cifra a través del segundo algoritmo para obtener una contraseña de activación, y la contraseña de activación cifrada se envía al aparato de monitoreo de red. Específicamente, el terminal de cliente envía una contraseña de activación que coincide con la dirección MAC del aparato de monitoreo de red al aparato de monitoreo de red.

En una realización de la presente invención, en el modo de activación en base a la dirección IP y el modo de activación en base a la dirección MAC, el primer algoritmo es un algoritmo de cifrado asimétrico RSA y el segundo algoritmo es un algoritmo de cifrado simétrico AES.

En el paso S53, la contraseña de activación cifrada se envía al aparato de monitoreo de red.

Dado que la contraseña de cifrado es la cadena aleatoria original generada por el aparato de monitoreo de red, el aparato de monitoreo de red descifra la contraseña de activación a través del segundo algoritmo para obtener la contraseña de activación original introducida por el usuario.

En el paso S54, después de que el aparato de monitoreo de red se active con éxito de acuerdo con la contraseña de activación cifrada, se recibe la información que indica que el aparato de monitoreo de red se activó con éxito.

El aparato de monitoreo de red determina si la complejidad de la contraseña de activación original descifrada cumple con un requisito de seguridad de contraseña predeterminado. Cuando la complejidad de la contraseña de activación original descifrada cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red se activa y la información que indica que el aparato de monitoreo de red se activó con éxito se devuelve al terminal de cliente. De lo contrario, la información que indica que el aparato de monitoreo de red no se activó con éxito se devuelve al terminal de cliente. El terminal de cliente avisa al usuario de que el aparato de monitoreo de red se activó con éxito.

En el procedimiento de cifrado del aparato de monitoreo de red en base al terminal de cliente provisto en, al menos, algunas realizaciones de la presente invención, no se establece una contraseña predeterminada para el aparato de monitoreo de red, y el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red puede usarse después de que un usuario lo active, de modo que se cambia el antiguo mal hábito de usar siempre la contraseña predeterminada por parte del usuario. Además, una contraseña de activación original ingresada por el usuario se encuentra sujeta a una verificación de seguridad, y no se permite usar una contraseña demasiado simple para activar el dispositivo, de modo que un usuario ilegal no puede controlar de forma remota el aparato de monitoreo mediante el uso de la contraseña predeterminada o al adivinar una contraseña actual que es demasiado simple, lo que mejora la seguridad de la contraseña. Además, la presente invención combina un algoritmo de cifrado asimétrico RSA y un algoritmo de cifrado simétrico AES en un procedimiento de cifrado de una

contraseña de activación original ingresada por un usuario, y es difícil descifrar la contraseña de activación ingresada por el usuario desde una red, por lo que se mejora la seguridad de un procedimiento de activación.

La Figura 6 es un diagrama de bloques estructural de un terminal de cliente de acuerdo con una realización ejemplar de la presente invención.

Como se muestra en la Figura 6, el terminal de cliente en esta realización ejemplar de la presente invención incluye: una interfaz 61 y un elemento de cifrado y descifrado 62.

Específicamente, la interfaz 61 se dispone para recibir una contraseña de activación original de un aparato de monitoreo de red.

El elemento de cifrado y descifrado 62 se dispone para cifrar la contraseña de activación original. La interfaz 61 envía además la contraseña de activación cifrada al aparato de monitoreo de red, y el aparato de monitoreo de red determina si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado, se activa, cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red, establece la contraseña de activación original como una contraseña de administrador y devuelve información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente.

Cuando se usa para activar el aparato de monitoreo de red, el terminal de cliente en esta realización ejemplar de la presente invención incluye: un modo de activación en base a una dirección IP y un modo de activación en base a una dirección MAC de acuerdo con diferentes modos de interacción de red. La diferencia entre dos modos de activación radica en la interacción de la red y los modos de cifrado de los dos modos de activación son consistentes.

(1) Modo de activación en base a una dirección IP

El elemento de cifrado y descifrado 62 adopta un primer algoritmo para generar una clave pública y una clave privada, y envía la clave pública al aparato de monitoreo de red. El aparato de monitoreo de red cifra una cadena aleatoria original generada por el aparato de monitoreo de red a través de la clave pública para generar una cadena aleatoria cifrada. La interfaz 61 recibe la cadena aleatoria cifrada enviada por el aparato de monitoreo de red, descifra la cadena aleatoria que se devuelve por el aparato de monitoreo de red y cifrada a través de la clave pública, y establece una cadena aleatoria original obtenida como clave de un segundo algoritmo. Luego, el elemento de cifrado y descifrado 62 cifra una contraseña de activación original a través del segundo algoritmo para obtener una contraseña de activación y envía la contraseña de activación cifrada al aparato de monitoreo de red.

(2) Modo de activación en base a una dirección MAC

La interfaz 61 recibe direcciones MAC notificadas por múltiples aparatos de monitoreo de red, y las direcciones MAC se usan respectivamente para identificar de forma única una identidad de cada aparato de monitoreo de red. El elemento de cifrado y descifrado 62 adopta un primer algoritmo para generar una clave pública y una clave privada, y envía la clave pública y la dirección MAC al aparato de monitoreo de red. Específicamente, la interfaz 61 envía la clave pública emparejada con la dirección MAC del aparato de monitoreo de red al aparato de monitoreo de red. El aparato de monitoreo de red cifra una cadena aleatoria original generada por el aparato de monitoreo de red a través de la clave pública para generar una cadena aleatoria cifrada. Luego, la interfaz 61 recibe la cadena aleatoria cifrada enviada por el aparato de monitoreo de red. Además, la operación de recibir, por la interfaz 61, la cadena aleatoria cifrada enviada por el aparato de monitoreo de red incluye, además: recibir una dirección MAC enviada por el aparato de monitoreo de red, y la dirección MAC se usa para identificar de manera única la identidad del aparato de monitoreo de red. El elemento de cifrado y descifrado 62 descifra la cadena aleatoria cifrada a través de la clave privada para obtener una contraseña de activación y establece la cadena aleatoria original como clave de un segundo algoritmo. El elemento de cifrado y descifrado 62 cifra una contraseña de activación original a través del segundo algoritmo para obtener la contraseña de activación cifrada. Específicamente, la interfaz 61 envía una contraseña de activación que coincide con la dirección MAC del aparato de monitoreo de red al aparato de monitoreo de red.

En una realización de la presente invención, en el modo de activación en base a la dirección IP y el modo de activación en base a la dirección MAC, el primer algoritmo es un algoritmo de cifrado asimétrico RSA y el segundo algoritmo es un algoritmo de cifrado simétrico AES.

La interfaz 61 envía la contraseña de activación cifrada al aparato de monitoreo de red. Dado que la contraseña de cifrado es la cadena aleatoria original generada por el aparato de monitoreo de red, el aparato de monitoreo de red descifra la contraseña de activación a través del segundo algoritmo para obtener la contraseña de activación original.

El aparato de monitoreo de red determina si la complejidad de la contraseña de activación original descifrada cumple con un requisito de seguridad de contraseña predeterminado. Cuando la complejidad de la contraseña de activación

original descifrada cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red se activa y la información que indica que el aparato de monitoreo de red se activó con éxito se devuelve a la interfaz 61. De lo contrario, la información que indica que el aparato de monitoreo de red no se activó con éxito se devuelve a la interfaz 61. El terminal de cliente avisa al usuario de que el aparato de monitoreo de red se activó con éxito.

En el terminal de cliente provisto en, al menos, algunas realizaciones de la presente invención, no se establece una contraseña predeterminada para el aparato de monitoreo de red, y el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red puede usarse después de activarse por un usuario, por lo que se cambia un viejo mal hábito de usar siempre la contraseña predeterminada por el usuario. Además, una contraseña de activación original se encuentra sujeta a verificación de seguridad, y no se permite usar una contraseña demasiado simple para activar el dispositivo, de modo que un usuario ilegal no puede controlar de forma remota el aparato de monitoreo mediante el uso de la contraseña predeterminada o al adivinar una contraseña actual que es demasiado simple, lo que mejora la seguridad de las contraseñas. Además, la presente invención combina un algoritmo de cifrado asimétrico RSA y un algoritmo de cifrado simétrico AES en un procedimiento de cifrado de una contraseña de activación original, y es difícil descifrar la contraseña de activación ingresada por el usuario desde una red, y mejora así aún más la seguridad de un procedimiento de activación.

La Figura 7 es un diagrama de bloques estructural de un sistema de activación remota en base a un aparato de monitoreo de red de acuerdo con una realización ejemplar de la presente invención.

Específicamente, el sistema de activación remota en base al aparato de monitoreo de red en esta realización ejemplar de la presente invención incluye: un terminal de cliente 1 y un aparato de monitoreo de red 2.

El terminal de cliente 1 se dispone para recibir una contraseña de activación original del aparato de monitoreo de red 2 y cifrar la contraseña de activación original. Específicamente, el terminal de cliente 1 envía una clave pública generada a través de un primer algoritmo al aparato de monitoreo de red 2. El aparato de monitoreo de red 2 cifra una cadena aleatoria original generada por el aparato de monitoreo de red a través de la clave pública para generar una cadena aleatoria cifrada. El terminal de cliente 2 descifra la cadena aleatoria cifrada devuelta por el aparato de monitoreo de red 2 mediante el uso de una clave privada generada a través del primer algoritmo para obtener la cadena aleatoria original. El terminal de cliente 1 establece la cadena aleatoria original obtenida como clave de un segundo algoritmo, cifra la contraseña de activación original a través del segundo algoritmo para obtener una contraseña de activación cifrada y envía la contraseña de activación cifrada al aparato de monitoreo de red 2.

Específicamente, la contraseña de activación original se cifra en un modo en base a una dirección IP y un modo en base a una dirección MAC.

El aparato de monitoreo de red 2 se configura para recibir la contraseña de activación cifrada del terminal de cliente 1, descifrar la contraseña de activación cifrada para obtener la contraseña de activación original ingresada por el usuario, determinar si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado, activar, cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red establece la contraseña de activación original como una contraseña de administrador y devuelve información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente 1. Después de recibir la información que indica que el aparato de monitoreo de red se activó con éxito, el terminal de cliente 1 envía un mensaje al usuario para indicar que el aparato de monitoreo de red se activó con éxito.

Es importante notar que el sistema de activación remota en base al aparato de monitoreo de red de la presente invención incluye: un modo de activación en base a una dirección IP y un modo de activación en base a una dirección MAC de acuerdo con diferentes modos de interacción con la red. La diferencia entre dos modos de activación radica en la interacción de la red y los modos de cifrado de los dos modos de activación son consistentes.

(1) Modo de activación en base a la dirección IP

El terminal de cliente 1 adopta un primer algoritmo para generar una clave pública, envía la clave pública al aparato de monitoreo de red 2, descifra una cadena aleatoria que se devuelve por el aparato de monitoreo de red 2 y cifrada a través de la clave pública, establece una cadena aleatoria original obtenida como clave de un segundo algoritmo, cifra una contraseña de activación original a través del segundo algoritmo para obtener una contraseña de activación cifrada, y envía la contraseña de activación cifrada al aparato de monitoreo de red 2.

(2) Modo de activación en base a la dirección MAC

El terminal de cliente recibe direcciones MAC notificadas por múltiples aparatos de monitoreo de red, adopta un primer algoritmo para generar una clave pública y una clave privada y envía la clave pública y la dirección MAC a cada uno de los aparatos de monitoreo de red. Luego, se descifra una cadena aleatoria que se devuelve por cada uno de los aparatos de monitoreo de red y cifrada a través de la clave pública, y una cadena aleatoria original

obtenida se establece como clave de un segundo algoritmo. Una contraseña de activación original se cifra a través del segundo algoritmo, y la contraseña de activación cifrada se envía a cada uno de los aparatos de monitoreo de red.

En una realización de la presente invención, en el modo de activación en base a la dirección IP y el modo de activación en base a la dirección MAC. El primer algoritmo es un algoritmo de cifrado asimétrico RSA y el segundo algoritmo es un algoritmo de cifrado simétrico AES.

La Figura 8 es un diagrama de flujo de activación de un sistema de activación remota en base a un aparato de monitoreo de red de acuerdo con una realización ejemplar de la presente invención.

En el paso S81, un usuario envía una instrucción de arranque a un aparato de monitoreo de red 2 no activado a través de un terminal de cliente 1, y después de recibir la instrucción de arranque, el aparato de monitoreo de red 2 no activado completa una acción de arranque.

En el paso S82, el usuario envía además una solicitud de acceso a la red al aparato de monitoreo de red no activado 2 a través del terminal de cliente 1. Dado que el aparato de monitoreo de red no se encuentra activado, el acceso falla y, a continuación, el usuario ejecuta en primer lugar una operación de activación.

En el paso S83, el terminal de cliente 1 cifra una contraseña de activación original del aparato de monitoreo de red 2 para obtener una contraseña de activación y envía la contraseña de activación cifrada al aparato de monitoreo de red 2.

En el paso S84, el aparato de monitoreo de red 2 recibe la contraseña de activación cifrada del terminal de cliente 1, descifra la contraseña de activación cifrada, obtiene la contraseña de activación original y determina si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado. Cuando la contraseña de activación original cumple con el requisito de intensidad de contraseña predeterminado, se ejecuta el paso S85.

En el paso S85, el aparato de monitoreo de red 2 activa el aparato de monitoreo de red y establece la contraseña de activación original como contraseña de administrador.

En el paso S86, el aparato de monitoreo de red 2 devuelve información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente 1.

En el paso S87, el terminal de cliente 1 envía una solicitud de operación de red específica al aparato de monitoreo de red 2 ya activado.

En el paso S88, el aparato de monitoreo de red 2 devuelve, en respuesta a la solicitud de operación de red, una respuesta de operación de red al terminal de cliente 1.

En el sistema de activación remota en base al aparato de monitoreo de red provisto en, al menos, algunas realizaciones de la presente invención, no se establece una contraseña predeterminada para el aparato de monitoreo de red, y el aparato de monitoreo de red no puede usarse antes de activarse, es decir, el aparato de monitoreo de red puede usarse después de activarse por un usuario, de modo que se cambia el antiguo mal hábito de usar siempre la contraseña predeterminada por parte del usuario. Además, una contraseña de activación original ingresada por el usuario se encuentra sujeta a verificación de seguridad, y no se permite usar una contraseña demasiado simple para activar el dispositivo, de modo que un usuario ilegal no puede controlar de forma remota el aparato de monitoreo mediante el uso de la contraseña predeterminada o al adivinar una contraseña actual que es demasiado simple, lo que mejora la seguridad de la contraseña. Además, la presente invención combina un algoritmo de cifrado asimétrico RSA y un algoritmo de cifrado simétrico AES en un procedimiento de cifrado de una contraseña de activación original ingresada por un usuario, y es difícil descifrar la contraseña de activación ingresada por el usuario desde una red, por lo que se mejora la seguridad de un procedimiento de activación.

Se apreciará que las realizaciones ejemplares mencionadas anteriormente de la presente invención se usan para ilustrar o explicar ejemplarmente el principio de la presente invención, y no constituyen una limitación a la presente invención. Por lo tanto, cualquier modificación, sustitución equivalente y mejora realizada sin apartarse del espíritu y ámbito de la presente invención debería estar dentro del ámbito de protección de la presente invención. Además, las reivindicaciones adjuntas de la presente invención pretenden cubrir todos los ejemplos de cambio y modificación que caen dentro del ámbito y límite de las reivindicaciones adjuntas o una forma equivalente de este ámbito y límite.

En una realización de la presente invención, se proporciona un terminal de computadora. La terminal de computadora es cualquier dispositivo de terminal de computadora en un grupo de terminales de computadora. Alternativamente, en la presente realización, el terminal informático también se sustituye por un dispositivo terminal tal como un terminal móvil.

Alternativamente, en la presente realización, el terminal informático se ubica en, al menos, un dispositivo de red en múltiples dispositivos de red de una red informática.

En la presente realización, el terminal informático ejecuta códigos de programa para los siguientes pasos en el procedimiento de activación remota de un aparato de monitoreo de red: recibir una contraseña de activación cifrada enviada por un terminal de cliente; descifrar la contraseña de activación cifrada para obtener una contraseña de activación original; determinar si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado; cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, activar el aparato de monitoreo de red y establecer la contraseña de activación original como una contraseña de administrador; y devolver información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente.

Alternativamente, el terminal de computadora incluye: uno o más procesadores, una memoria y un aparato de transmisión.

La memoria se dispone para almacenar un programa de software y un componente, tal como una instrucción/componente de programa correspondiente a un procedimiento de activación remota de un aparato de monitoreo de red en, al menos, una realización de la presente invención. El procesador ejecuta diversas aplicaciones de funciones y procesamiento de datos al ejecutar el programa de software y el componente almacenado en la memoria, concretamente al implementar el procedimiento de activación remota mencionado anteriormente de un aparato de monitoreo de red. La memoria puede incluir una memoria de acceso aleatorio de alta velocidad (RAM) y también puede incluir una memoria no volátil, tal como uno o más aparatos de almacenamiento en disco, memorias flash u otras memorias de estado sólido no volátiles. En algunos ejemplos, la memoria incluye además memorias dispuestas remotamente con respecto al procesador. Estas memorias remotas se conectan a un terminal a través de una red. Los ejemplos de red incluyen, entre otros, Internet, intranet, red de área local, red de comunicación móvil y una combinación de Internet, intranet, red de área local y red de comunicación móvil.

El aparato de transmisión se dispone para recibir o enviar datos a través de una red. Un ejemplo específico para la red incluye, al menos, uno de una red de cable y una red de radio. En un ejemplo, el aparato de transmisión incluye un controlador de interfaz de red (NIC), que se conecta a un enrutador a través de un cable de red y otros dispositivos de red, para comunicarse con Internet o la red de área local. En un ejemplo, el aparato de transmisión es un componente de radiofrecuencia (RF), dispuesto para comunicarse con Internet por radio.

Específicamente, la memoria se dispone para almacenar condiciones de acción predeterminadas, información de usuario de permisos predeterminados y programas de aplicación.

El procesador llama a programas de aplicación e información almacenados en la memoria a través del aparato de transmisión, para ejecutar códigos de programa para los pasos del procedimiento de cada realización alternativa o ejemplar en las realizaciones del procedimiento mencionadas anteriormente.

Un experto en la técnica puede comprender que el terminal informático también es un dispositivo terminal como un teléfono inteligente (como un teléfono Android y un teléfono iOS), una tableta, una computadora de mano, un MID y un PAD.

Un experto en la técnica puede comprender que todos o algunos pasos en cada procedimiento de las realizaciones mencionadas anteriormente se completan al instruir un hardware relevante del dispositivo terminal a través de un programa. Y el programa se almacena en un medio de almacenamiento legible por computadora, y el medio de almacenamiento incluye: un disco flash, una memoria de solo lectura (ROM), una RAM, un disco magnético o un disco óptico.

En una realización de la presente invención se proporciona un medio de almacenamiento. Alternativamente, en la presente realización, el medio de almacenamiento se dispone para almacenar códigos de programa ejecutados para un procedimiento de activación remota de un aparato de monitoreo de red proporcionado en las realizaciones del procedimiento y realizaciones del aparato antes mencionadas.

Alternativamente, en la presente realización, el medio de almacenamiento se ubica en cualquier terminal de computadora en un grupo de terminales de computadora en una red de computadoras, o ubicado en cualquier terminal móvil en un grupo de terminales móviles.

Alternativamente, en la presente realización, el medio de almacenamiento se dispone para almacenar códigos de programa para ejecutar los siguientes pasos: recibir una contraseña de activación cifrada enviada por un terminal de cliente; descifrar la contraseña de activación cifrada para obtener una contraseña de activación original; determinar si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado; cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, activar el aparato de monitoreo de red y establecer la contraseña de activación original como una contraseña de administrador; y devolver información que indica que el aparato de monitoreo de red se activó con éxito al terminal de cliente.

Alternativamente, en la presente realización, el medio de almacenamiento también se dispone para almacenar códigos de programa para ejecutar cada paso de procedimiento ejemplar o alternativo provisto en un procedimiento de activación remota de un aparato de monitoreo de red.

Los números de serie de las realizaciones de la presente invención se usan para descripciones y no representan la preferencia de las realizaciones.

En las realizaciones mencionadas anteriormente de la presente invención, las descripciones de cada realización se enfatizan respectivamente, y las partes que no se elaboran en una determinada realización pueden hacer referencia a descripciones relevantes de otras realizaciones.

En algunas realizaciones proporcionadas por la presente solicitud, se apreciará que los contenidos técnicos divulgados se implementan en otros modos. En la presente memoria, la realización del aparato descrita anteriormente es esquemática. Por ejemplo, la división de los elementos es la división de funciones lógicas y hay modos de división adicionales durante la implementación real. Por ejemplo, una pluralidad de elementos o componentes se combinan o integran a otro sistema, o se omiten o no se ejecutan algunas características. Además, el acoplamiento mutuo mostrado o discutido o el acoplamiento directo o la conexión de comunicación se realizan a través de algunas interfaces, y el acoplamiento indirecto o la conexión de comunicación entre elementos o componentes están en forma eléctrica o de otras formas.

Los elementos ilustrados como partes separadas se encuentran o no físicamente separados. Las partes para la visualización de elementos son o no elementos físicos. Es decir, las partes se ubican en un lugar o se distribuyen en una pluralidad de elementos. Los objetivos de las soluciones de las realizaciones se logran al seleccionar algunos o todos los elementos de acuerdo con los requisitos reales.

Además, todos los elementos funcionales en todas las realizaciones de la presente invención se integran en un elemento de procesamiento, o cada elemento existe por separado y físicamente, o dos o más elementos se integran en un elemento. El elemento integrado se implementa en forma de hardware o se implementa en forma de elemento de función de software.

Cuando se implementa en forma de elemento de función de software y se vende o usa como un producto independiente, el elemento integrado se almacena en un medio de almacenamiento legible por computadora. En base a este entendimiento, las soluciones técnicas de la presente invención se incorporan sustancialmente en forma de producto de software o partes que contribuyen a la técnica relacionada o todas o algunas de las soluciones técnicas se incorporan en forma de producto de software, y el producto de software informático se almacena en un medio de almacenamiento que incluye una pluralidad de instrucciones que permiten a un dispositivo informático (que es una computadora personal, un servidor, un dispositivo de red o similar) ejecutar todos o algunos de los pasos del procedimiento de acuerdo con cada realización de la presente invención. El medio de almacenamiento mencionado anteriormente incluye: varios medios capaces de almacenar códigos de programa, como un disco U, una ROM, una RAM, un disco duro móvil, un disco magnético o un disco óptico.

Los anteriores son modos de implementación ejemplares de la presente invención. Cabe señalar que un experto en la técnica también puede realizar algunas mejoras y modificaciones sin apartarse del principio de la presente invención. Estas mejoras y modificaciones deben estar dentro del ámbito de protección de la presente invención

REIVINDICACIONES

1. Un procedimiento de activación remota de un aparato de monitoreo de red no activado, que comprende:

el aparato de monitoreo de red no activado que recibe una contraseña de activación cifrada enviada por un terminal de cliente, en el que el aparato de monitoreo de red no activado no tiene contraseña de administrador predeterminada y no puede usarse antes de la activación (S11);
el aparato de monitoreo de red no activado descifra la contraseña de activación cifrada para obtener una contraseña de activación original (S12);
solo en caso de que la contraseña de activación original cumpla con un requisito de seguridad de contraseña predeterminado, se activa el aparato de monitoreo de red no activado y se establece la contraseña de activación original como una contraseña de administrador (S13); y
el aparato de monitoreo de red activado devuelve información que indica que el aparato de monitoreo de red no activado se activó con éxito al terminal de cliente (S14).

2. El procedimiento de activación remota del aparato de monitoreo de red no activado como se reivindicó en la reivindicación 1, en el que recibir la contraseña de activación cifrada enviada por el terminal de cliente comprende: recibir una clave pública enviada por el terminal de cliente y generada a través de un primer algoritmo, cifrar una cadena aleatoria original generada por el aparato de monitoreo de red no activado a través de la clave pública para generar una cadena aleatoria cifrada, devolver la cadena aleatoria cifrada al terminal de cliente; y recibir una contraseña de activación enviada por el terminal de cliente y cifrada a través de un segundo algoritmo, en el que la contraseña de activación se genera al cifrar una contraseña de activación original a través del segundo algoritmo, en el que una contraseña del segundo algoritmo es la cadena aleatoria original;
o en el que descifrar la contraseña de activación cifrada para obtener la contraseña de activación original comprende:
descifrar la contraseña de activación a través de un segundo algoritmo para obtener la contraseña de activación original.

3. El procedimiento de activación remota del aparato de monitoreo de red no activado como se reivindicó en la reivindicación 2, antes de recibir la clave pública enviada por el terminal de cliente y generada a través del primer algoritmo, que comprende, además:

informar de una dirección MAC de control de acceso a medios al terminal de cliente, en el que la dirección MAC se usa para identificar de forma única una identidad del aparato de monitoreo de red no activado;
o en el que, al devolver la cadena aleatoria cifrada al terminal de cliente, el procedimiento de activación remota comprende, además: informar una dirección MAC al terminal de cliente, en el que la dirección MAC se usa para identificar de forma única una identidad del aparato de monitoreo de red no activado;
o en el que el primer algoritmo es un algoritmo de cifrado asimétrico RSA y el segundo algoritmo es un algoritmo de cifrado simétrico AES estándar de cifrado avanzado.

4. El procedimiento de activación remota del aparato de monitoreo de red no activado como se reivindicó en la reivindicación 3, en el que recibir la clave pública enviada por el terminal de cliente y generada a través del primer algoritmo comprende:

recibir una clave pública emparejada con una dirección MAC del aparato de monitoreo de red no activado, enviada por el terminal de cliente y generada a través del primer algoritmo;
o en el que recibir la contraseña de activación enviada por el terminal de cliente y cifrada mediante el segundo algoritmo comprende: recibir una contraseña de activación emparejada con una dirección MAC del aparato de monitoreo de red no activado, enviada por el terminal de cliente y cifrada mediante el segundo algoritmo.

5. Un aparato de monitoreo de red no activado, en el que el aparato de monitoreo de red no activado no tiene una contraseña de administrador predeterminada y no puede usarse antes de la activación; que comprende:

una interfaz (41), dispuesta para recibir una contraseña de activación cifrada enviada por un terminal de cliente;
un elemento de cifrado y descifrado (42), dispuesto para descifrar la contraseña de activación cifrada para obtener una contraseña de activación original;
un elemento de determinación (43), dispuesto para determinar que la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado;
un elemento de activación (44), dispuesto para activar, solo en caso de que la contraseña de activación original cumpla con el requisito de seguridad de contraseña predeterminado, el aparato de

monitoreo de red no activado y establecer la contraseña de activación original como contraseña de administrador; y
la interfaz, dispuesta además para devolver información que indica que el aparato de monitoreo de red no activado se activó con éxito al terminal de cliente.

6. El aparato de monitoreo de red no activado como se reivindicó en la reivindicación 5, en el que la interfaz se dispone para recibir una clave pública enviada por el terminal de cliente y generada a través de un primer algoritmo, y devolver una cadena aleatoria cifrada al terminal de cliente, en el que la cadena aleatoria cifrada se obtiene al cifrar, mediante el elemento de cifrado y descifrado, una cadena aleatoria original generada por el aparato de monitoreo de red no activado a través de la clave pública, y la cadena aleatoria cifrada se descifra por el terminal de cliente a través de una clave privada del primer algoritmo para obtener la cadena aleatoria original; y la interfaz se dispone además para recibir una contraseña de activación enviada por el terminal de cliente y cifrada a través de un segundo algoritmo, en el que la contraseña de activación se genera al cifrar, por parte del terminal de cliente, la contraseña de activación original a través del segundo algoritmo, y una contraseña del segundo algoritmo es la cadena aleatoria original;
o en el que el elemento de cifrado y descifrado se dispone para descifrar la contraseña de activación cifrada a través de un segundo algoritmo para obtener la contraseña de activación original.

7. El aparato de monitoreo de red no activado como se reivindicó en la reivindicación 6, en el que la interfaz se dispone además para, antes de recibir la clave pública enviada por el terminal de cliente y generada a través del primer algoritmo, informar una dirección MAC de control de acceso a medios al terminal de cliente, en el que la dirección MAC se usa para identificar de manera única una identidad del aparato de monitoreo de red no activado;

o en el que la interfaz se dispone además para, además de devolver la cadena aleatoria cifrada al terminal de cliente, informar una dirección MAC al terminal de cliente, en el que la dirección MAC se usa para identificar de manera única una identidad del aparato de monitoreo de red no activado;
o en el que la interfaz se dispone para recibir una contraseña de activación que coincida con una dirección MAC del aparato de monitoreo de red no activado, enviada por el terminal de cliente y cifrada mediante el segundo algoritmo;
o en el que el primer algoritmo es un algoritmo RSA de cifrado asimétrico y el segundo algoritmo es un algoritmo AES estándar de cifrado avanzado de cifrado simétrico.

8. El aparato de monitoreo de red no activado como se reivindicó en la reivindicación 7, en el que la interfaz se dispone para recibir una clave pública emparejada con una dirección MAC del aparato de monitoreo de red no activado, enviada por el terminal de cliente y generada a través del primer algoritmo.

9. Un sistema de activación remota en base a un aparato de monitoreo de red no activado, que comprende

un terminal de cliente (1), dispuesto para recibir una contraseña de activación original de un aparato de monitoreo de red no activado, y cifrar la contraseña de activación original; y
el aparato de monitoreo de red no activado (2), dispuesto para recibir una contraseña de activación cifrada desde el terminal de cliente, descifrar la contraseña de activación cifrada para obtener la contraseña de activación original, activar, solo en el caso de que la contraseña de activación original coincida con un requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red no activado, establece la contraseña de activación original como una contraseña de administrador, y el aparato de monitoreo de red activado devuelve información que indica que el aparato de monitoreo de red no activado se activó con éxito al terminal de cliente, en el que el aparato de monitoreo de red no activado no tiene una contraseña de administrador predeterminada y no puede usarse antes de la activación;
el terminal de cliente, dispuesto además para enviar, después de recibir la información que indica que el aparato de monitoreo de red no activado se activó con éxito, un aviso que indica que el aparato de monitoreo de red no activado se activó con éxito.

10. El sistema de activación remota en base al aparato de monitoreo de red no activado como se reivindicó en la reivindicación 9, en el que el terminal de cliente se dispone para recibir la contraseña de activación original de un aparato de monitoreo de red no activado y cifrar la contraseña de activación original comprende el siguiente paso:

enviar una clave pública generada a través de un primer algoritmo al aparato de monitoreo de red no activado, en el que la clave pública se adopta por el aparato de monitoreo de red no activado para cifrar la cadena aleatoria original generada por el aparato de monitoreo de red no activado para generar una cadena aleatoria cifrada; y
descifrar la cadena aleatoria cifrada devuelta por el aparato de monitoreo de red no activado mediante el uso de una clave privada generada a través del primer algoritmo para obtener la cadena aleatoria original, establecer la cadena aleatoria original como clave de un segundo algoritmo, cifrar la

contraseña de activación original a través del segundo algoritmo para obtener una contraseña de activación cifrada, y enviar la contraseña de activación cifrada al aparato de monitoreo de red no activado.

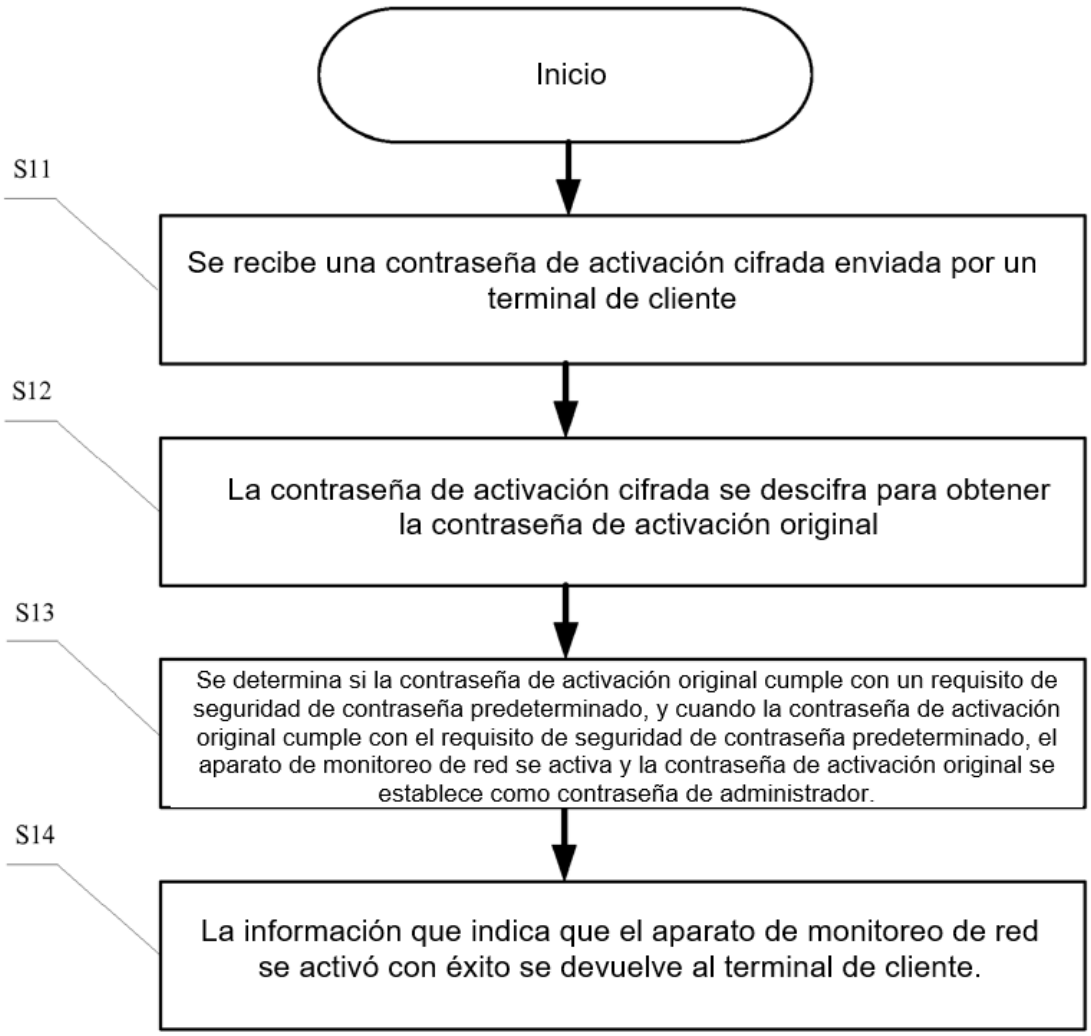
Inicio
S11
Se recibe una contraseña de activación cifrada enviada por un terminal de cliente
S12
La contraseña de activación cifrada se descifra para obtener la contraseña de activación original
S13
Se determina si la contraseña de activación original cumple con un requisito de seguridad de contraseña predeterminado, y cuando la contraseña de activación original cumple con el requisito de seguridad de contraseña predeterminado, el aparato de monitoreo de red se activa y la contraseña de activación original se establece como contraseña de administrador.
S14
La información que indica que el aparato de monitoreo de red se activó con éxito se devuelve al terminal de cliente.

Figura 1

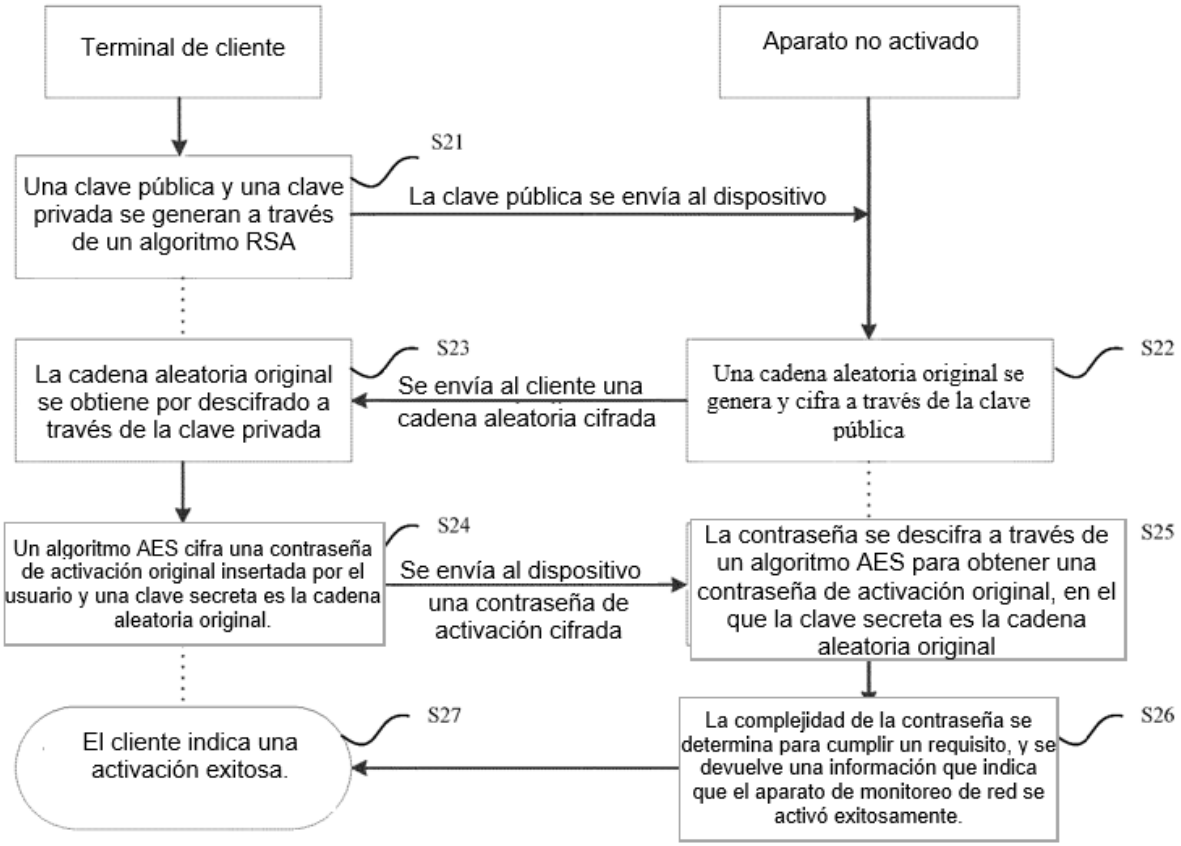
Terminal de cliente
Aparato no activado
S21
Una clave pública y una clave privada se generan a través de un algoritmo RSA
La clave pública se envía al dispositivo
S23
La cadena aleatoria original se obtiene por descifrado a través de la clave privada
Se envía al cliente una cadena aleatoria cifrada
Una cadena aleatoria original se genera y cifra a través de la clave pública
S22
S24
Un algoritmo AES cifra una contraseña de activación original insertada por el usuario y una clave secreta es la cadena aleatoria original.
Se envía al dispositivo una contraseña de activación cifrada
La contraseña se descifra a través de un algoritmo AES para obtener una contraseña de activación original, en el que la clave secreta es la cadena aleatoria original
S25
S27
El cliente indica una activación exitosa.
La complejidad de la contraseña se determina para cumplir un requisito, y se devuelve una información que indica que el aparato de monitoreo de red se activó exitosamente.
S26

Figura 2

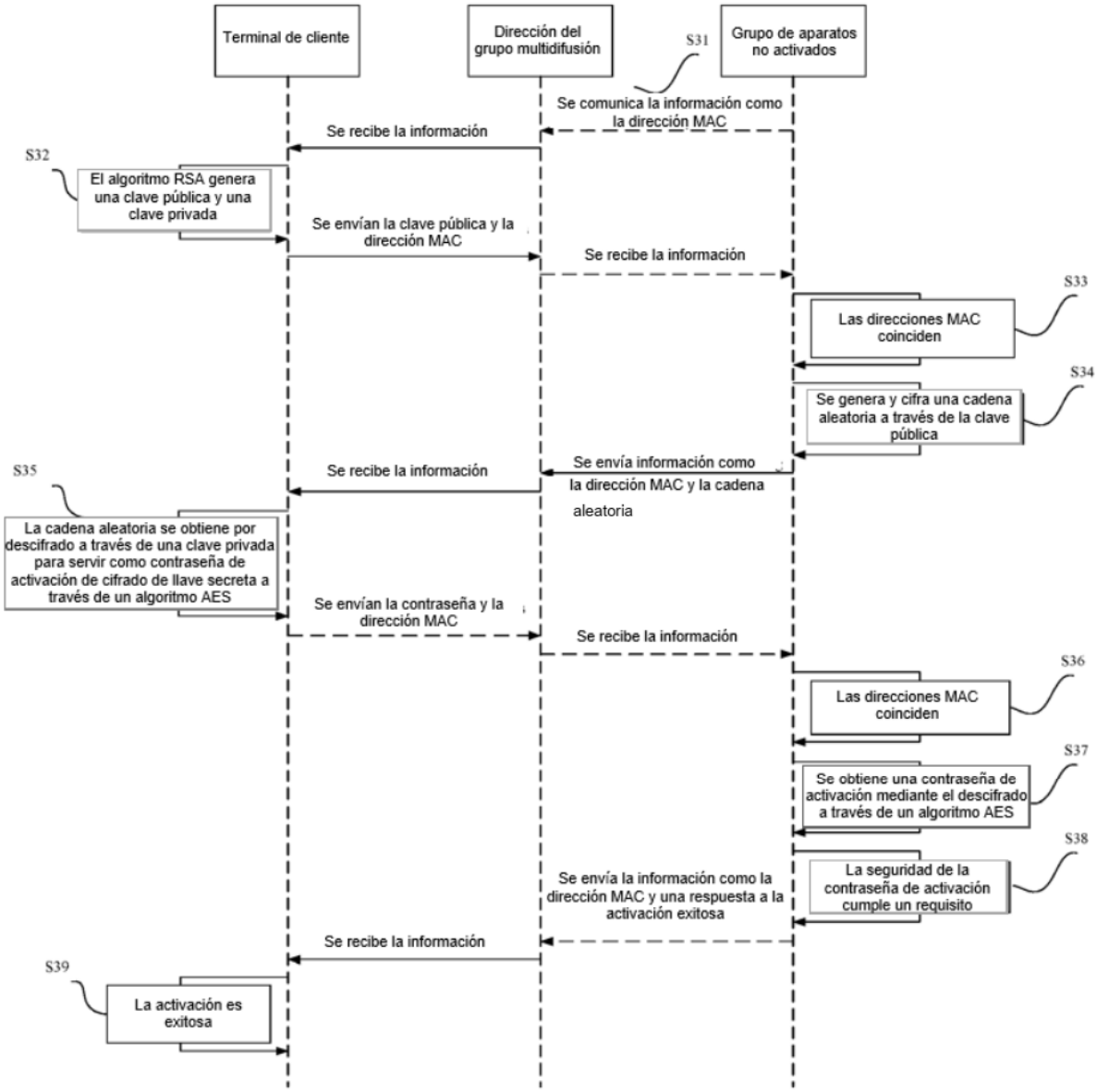

Figura 3

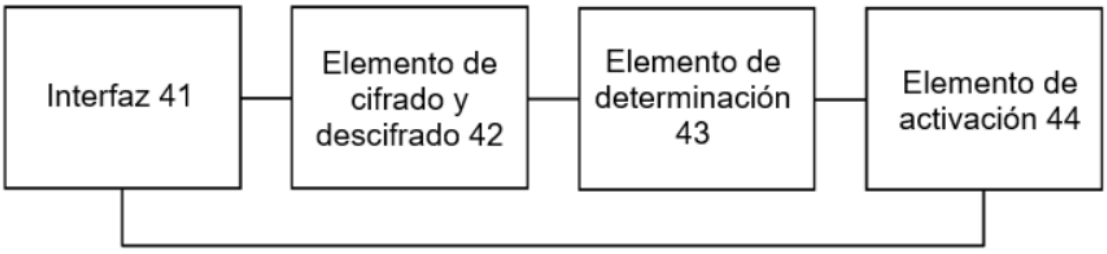

Figura 4

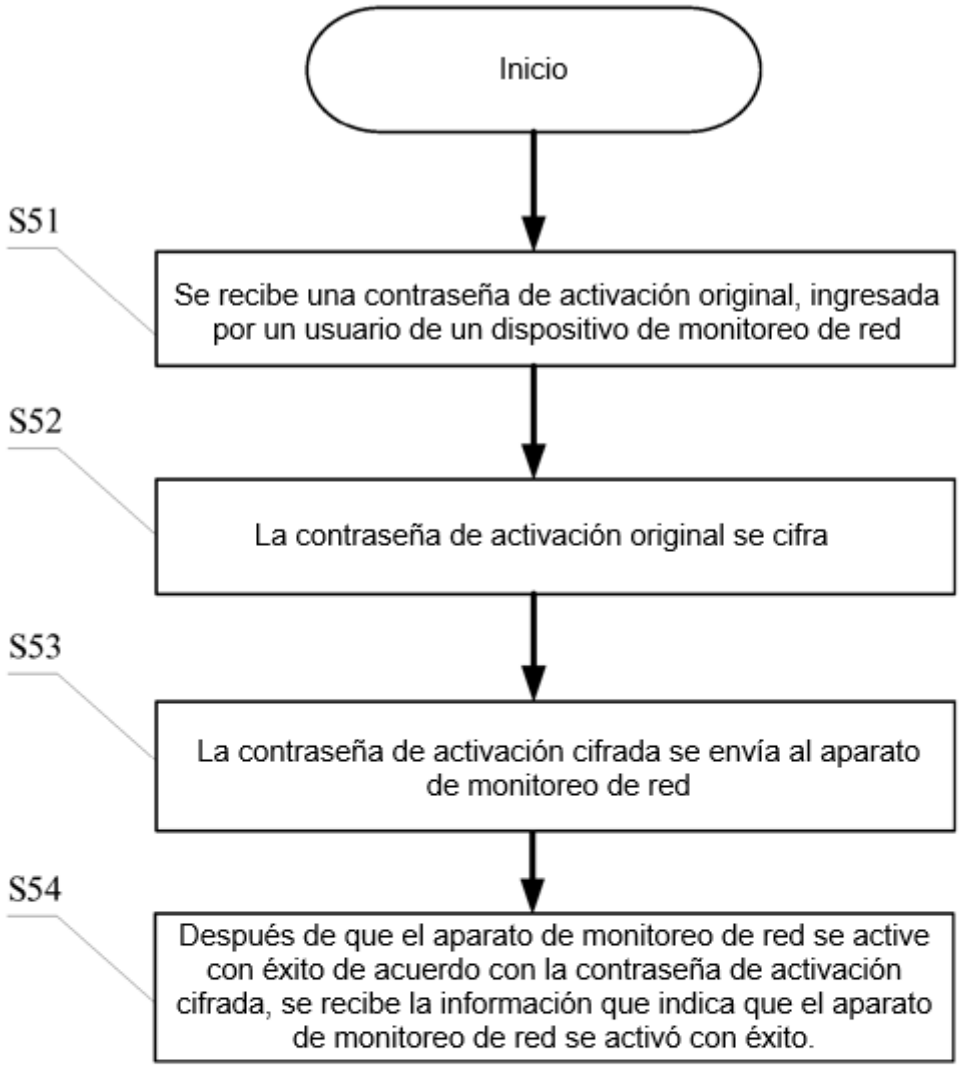

Figura 5

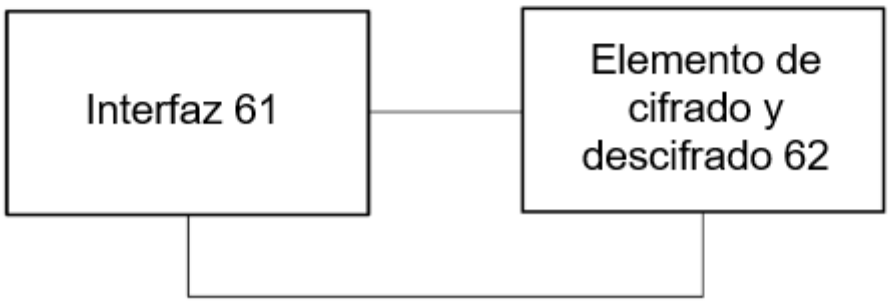

Figura 6

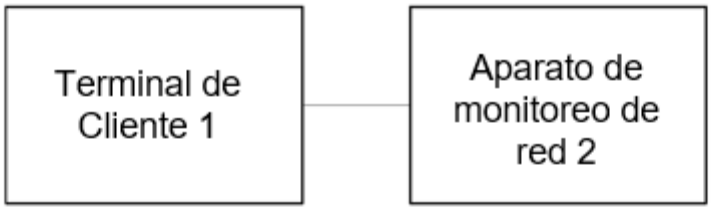

Figura 7

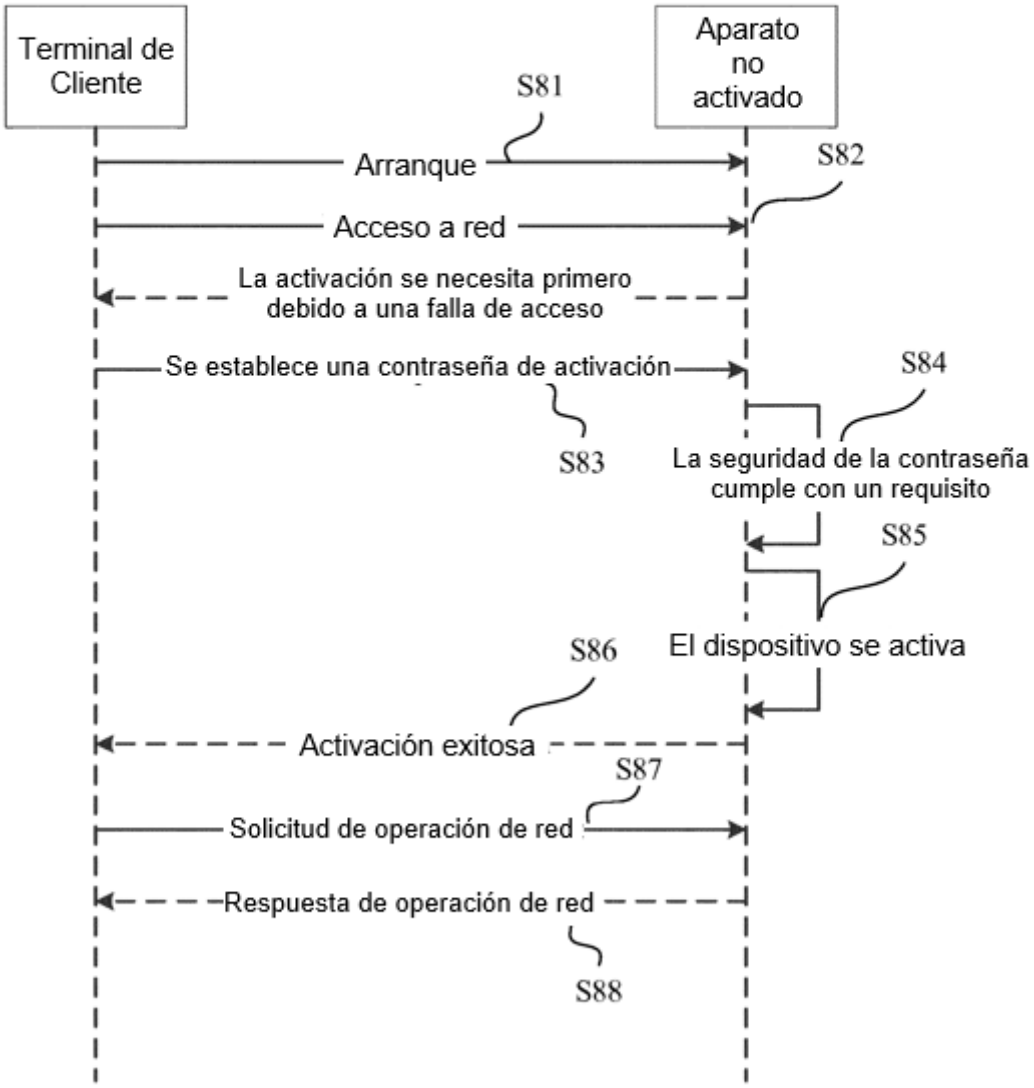

Figura 8