(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 609 922**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 12/08 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.12.2008 PCT/CN2008/002162**

(87) Fecha y número de publicación internacional: **08.07.2010 WO10075644**

(96) Fecha de presentación y número de la solicitud europea: **31.12.2008 E 08879260 (1)**

(97) Fecha y número de publicación de la concesión europea: **12.10.2016 EP 2384038**

(54) Título: **Método y sistema para realizar bloqueo y desbloqueo en una red mediante un dispositivo terminal**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.04.2017

(73) Titular/es:

ZTE CORPORATION (100.0%)
ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District
Shenzhen, Guangdong 518057, CN

(72) Inventor/es:

LIU, XIAOPENG

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Método y sistema para realizar bloqueo y desbloqueo en una red mediante un dispositivo terminal

Sector técnico

La presente invención se refiere al mecanismo de protección de seguridad de la red de los productos de dispositivo terminal en la comunicación de red inalámbrica, y en particular, al mecanismo de protección de seguridad de la red, para productos de dispositivo terminal en la red de Interoperabilidad mundial para acceso por microondas (WiMAX, World Interoperability for Microwave Access), y a un método, un sistema y un dispositivo terminal para la implementación de bloqueo en la red.

Antecedentes de la técnica relacionada

Después de acceder a la red proporcionada por el operador, un dispositivo terminal lleva a cabo operaciones de bloqueo en la red para impedir que este dispositivo terminal acceda a otras redes, lo que tiene los objetivos de: 1) evitar el acceso del dispositivo terminal a estaciones base falsas; algunos piratas informáticos pueden establecer por sí mismos una estación base falsa que imponga al dispositivo terminal que acceda a la estación base falsa, robando así información personal, e incluso dañando el dispositivo terminal; y 2) evitar el acceso del dispositivo terminal a las redes proporcionadas por los otros operadores. En la actualidad, hay una fuerte competencia en el mercado de la comunicación, y cada gran operador adopta diversos esquemas para atraer a nuevos clientes y conservar a los clientes antiguos. Donde el modo de venta que vincula los dispositivos terminales, tales como teléfonos móviles/tarjetas de red y similares, con los servicios es uno de los esquemas para captar nuevos clientes. En este esquema, el precio de venta real de dispositivos terminales tales como teléfonos móviles/tarjetas de red y similares es inferior al precio de mercado, de modo que los operadores no desean que los abonados utilicen dispositivos terminales en las redes de otros operadores una vez que finalizan los servicios, sino que desean que los abonados sigan utilizando los servicios que ellos mismos proporcionan. Con el fin de conseguir el objetivo de conservar a los clientes antiguos, surge la necesidad de añadir una función de bloqueo en la red. Esta función puede vincular los dispositivos terminales con los operadores, y por lo tanto se impide a los abonados de los dispositivos terminales el uso de los servicios proporcionados por otros operadores.

Al mismo tiempo, los operadores también pueden desbloquear los dispositivos terminales para cumplir varios requisitos, tales como el mantenimiento y la reparación postventa, y en situaciones particulares, pueden permitir el desbloqueo de los usuarios mediante el pago de una determinada tarifa y similares.

Los documentos WO2008079490A1 y US20088209206A1 dan a conocer diferentes métodos para la implementación del bloqueo de un dispositivo terminal en una red.

Con el fin de resolver el problema técnico anterior, la presente invención propone los siguientes esquemas técnicos.

Contenido de la invención

El problema a resolver en la presente invención es dar a conocer un método, un sistema y un dispositivo terminal para la implementación del bloqueo de un dispositivo terminal en una red con el fin de implementar la función de bloqueo en la red.

Las características del método y el sistema según la presente invención se definen en las reivindicaciones independientes 1 a 4 y las características preferentes según la presente invención se definen en las reivindicaciones dependientes.

Para resolver el problema anterior, se da a conocer un método para implementar el bloqueo de un dispositivo terminal en una red, y este método comprende un procedimiento de bloqueo en la red durante el acceso a la red, realizando particularmente una verificación de la configuración de bloqueo en la red en el proceso de autenticación de acceso a la red, y si la verificación de la configuración de bloqueo en la red es satisfactoria, permite la verificación de un certificado de autenticación, o de lo contrario rechaza el acceso del dispositivo terminal a la red.

Asimismo, el proceso de autenticación de acceso a la red se refiere a un proceso en el que el dispositivo terminal autentica un servidor de Autenticación, Autorización y Contabilidad (AAA, Authentication Authorization Accounting), la verificación de la configuración de bloqueo en la red se refiere a la comparación de una cadena de caracteres de bloqueo en la red en un certificado de autenticación del servidor de AAA con una cadena de caracteres de bloqueo en la red memorizada en el dispositivo terminal, si la cadena de caracteres de bloqueo en la red en el certificado de autenticación del servidor de AAA es igual que la memorizada en el dispositivo terminal, se considera que la verificación de la configuración de bloqueo en la red es satisfactoria.

Asimismo, la cadena de caracteres de bloqueo en la red se refiere a un ID del nombre de red de un operador dispuesto en un campo CN en el Asunto en el certificado de autenticación.

Asimismo, en la verificación de la configuración de bloqueo en la red, antes de realizar la comparación de las cadenas de caracteres de bloqueo en la red, se determina si la función de bloqueo en la red está activada según un bit indicador de bloqueo en la red memorizado en el dispositivo terminal, y en caso afirmativo, se realiza la comparación de las cadenas de caracteres de bloqueo en la red, o de lo contrario se realiza directamente la verificación del certificado de autenticación.

Asimismo, el método comprende además un procedimiento de desbloqueo, y este procedimiento comprende: un servidor inalámbrico (OTA, "Over The Air") que obtiene las claves de desbloqueo memorizadas por un servidor del operador y el dispositivo terminal respectivamente y compara la clave de desbloqueo memorizada por un operador con la memorizada por el dispositivo terminal; y si las claves de desbloqueo son iguales, el servidor OTA notifica al dispositivo terminal que establezca el bit indicador de bloqueo en la red como función de bloqueo en la red desactivada y borre la cadena de caracteres de bloqueo en la red.

Asimismo, el método además comprende un procedimiento de bloqueo de nuevo tras el acceso a la red, y este procedimiento comprende: un servidor inalámbrico (OTA) calcula una clave de desbloqueo del dispositivo terminal, e notifica al servidor del operador y al dispositivo terminal que almacenen esta clave de desbloqueo; el servidor OTA transmite el bit indicador de bloqueo en la red y la cadena de caracteres de bloqueo en la red al dispositivo terminal; y el dispositivo terminal almacena esta cadena de caracteres de bloqueo en la red y establece el bit indicador de bloqueo en la red como función de bloqueo en la red activada.

Para resolver el problema técnico anterior, se da a conocer un sistema para implementar el bloqueo de un dispositivo terminal en una red, y este sistema se utiliza para realizar una verificación de la configuración de bloqueo en la red en un proceso de autenticación de acceso a la red, y permitir la verificación de un certificado de autenticación si la verificación de la configuración de bloqueo en la red es satisfactoria, o de lo contrario rechazar el acceso del dispositivo terminal a la red.

Asimismo, el sistema incluye un servidor de Autenticación, Autorización y Contabilidad (AAA) y un dispositivo terminal, en que

el servidor de AAA se utiliza para transmitir un certificado de autenticación al dispositivo terminal, incluyendo el certificado de autenticación una cadena de caracteres de bloqueo en la red;

el dispositivo terminal incluye un módulo transceptor, un módulo de bloqueo en la red y un módulo de autenticación, en que,

el módulo transceptor se utiliza para recibir el certificado de autenticación;

el módulo de bloqueo en la red se utiliza para realizar la verificación del bloqueo en la red para una cadena de caracteres de bloqueo en la red en el certificado de autenticación transmitido por el servidor de AAA y una cadena de caracteres de bloqueo en la red memorizada en el dispositivo terminal, y permite que el módulo de autenticación realice la autenticación si la cadena de caracteres de bloqueo en la red en el certificado de autenticación transmitido por el servidor de AAA es igual que la memorizada en el dispositivo terminal;

el módulo de autenticación se utiliza para verificar el certificado de autenticación transmitido por el servidor de AAA según un certificado memorizado por sí mismo.

Asimismo, el módulo de bloqueo en la red también se utiliza para almacenar un bit indicador de bloqueo en la red; y si el bit indicador de bloqueo en la red indica que la función de bloqueo en la red está desactivada, el módulo de red de bloqueo también se utiliza para activar directamente el módulo de autenticación para que realice la autenticación, o de lo contrario para iniciar la verificación de la cadena de caracteres de bloqueo en la red.

Asimismo, el sistema además incluye un servidor inalámbrico (OTA) y un servidor del operador; el servidor OTA se utiliza para verificar las claves de desbloqueo memorizadas por un servidor del operador y el dispositivo terminal respectivamente, e notifica al dispositivo terminal que borre la cadena de caracteres de bloqueo en la red y restablezca el bit indicador de bloqueo en la red para implementar una función de desbloqueo; el servidor OTA también se utiliza para calcular una clave de desbloqueo e notificar al servidor del operador y al dispositivo terminal que almacenen esta clave de desbloqueo, y notifica al dispositivo terminal que almacene la cadena de caracteres de bloqueo en la red y que establezca el bit indicador de bloqueo en la red para implementar una función de bloqueo de nuevo tras el acceso a la red; el módulo de bloqueo en la red del dispositivo terminal se utiliza para realizar el almacenamiento y la actualización según las notificaciones del servidor OTA.

Para resolver el problema anterior, se da a conocer un dispositivo terminal, el dispositivo terminal tiene una función de bloqueo en la red, incluyendo el dispositivo terminal un módulo transceptor, un módulo de bloqueo en la red y un módulo de autenticación, en que,

el módulo transceptor se utiliza para recibir un certificado de autenticación transmitido por un servidor de Autenticación, Autorización y Contabilidad (AAA), y el certificado de autenticación incluye una cadena de caracteres de bloqueo en la red;

el módulo de bloqueo en la red se utiliza para realizar la verificación del bloqueo en la red para la cadena de caracteres de bloqueo en la red en el certificado de autenticación transmitido por el servidor de AAA y para una cadena de caracteres de bloqueo en la red memorizada en el dispositivo terminal, y para activar el módulo de autenticación para que realice la autenticación si la cadena de caracteres de bloqueo en la red en el certificado de autenticación transmitido por el servidor de AAA es igual que la memorizada en el dispositivo terminal;

el módulo de autenticación se utiliza para verificar el certificado de autenticación transmitido por el servidor de AAA según un certificado memorizado por sí mismo.

Asimismo, el módulo de bloqueo en la red también se utiliza para almacenar un bit indicador de bloqueo en la red; y si el bit indicador de bloqueo en la red indica que la función de bloqueo en la red está desactivada, el módulo de bloqueo en la red también se utiliza para activar directamente el módulo de autenticación para que realice la autenticación, o de lo contrario para iniciar la verificación de la cadena de caracteres de bloqueo en la red.

En comparación con la técnica anterior, el método, el sistema y el dispositivo terminal de la presente invención adoptan el proceso de autenticación y requieren que el dispositivo terminal y el servidor configuren uniformemente una cadena de caracteres de bloqueo en la red con el fin de tener una alta seguridad. Además, el método, el sistema y el dispositivo terminal de la presente invención pueden implementar el desbloqueo y el bloqueo de nuevo tras el acceso a la red por medio de una gestión de la interfaz aérea de manera OTA, lo que tiene una flexibilidad y una aplicabilidad elevadas, y puede cumplir perfectamente los requisitos de las redes 4G tales como la red WiMAX, la red LTE y similares.

Breve descripción de los dibujos

La figura 1 es una ilustración de un croquis del contenido del certificado X.509;

La figura 2 es una ilustración de un croquis de la cadena de certificados X.509;

La figura 3 es un diagrama de flujo de la autenticación bidireccional de EAP-TLS y EAP-TTLS;

La figura 4 es un diagrama de flujo del bloqueo en la red durante un acceso del dispositivo terminal a la red, según la presente invención;

La figura 5 es un diagrama de flujo del desbloqueo, según la presente invención;

La figura 6 es un diagrama de flujo del bloqueo en la red de nuevo tras el acceso a la red, según la presente invención.

Realizaciones preferentes de la presente invención

El método para implementar el bloqueo de un dispositivo terminal en una red según la presente invención incluye tres procedimientos, particularmente, un procedimiento de bloqueo en una red durante el acceso a la red, un procedimiento de desbloqueo y un procedimiento de bloqueo de nuevo tras el acceso a la red. El procedimiento de bloqueo en la red durante el acceso a la red lleva a cabo la verificación de la configuración de bloqueo en la red en un proceso de autenticación de acceso a la red, si la verificación de la configuración de bloqueo en la red es satisfactoria, permite la verificación de un certificado de autenticación, o de lo contrario rechaza el acceso a la red del terminal móvil.

A continuación se describen los tres procedimientos, respectivamente.

1. El procedimiento de bloqueo en una red durante el acceso a la red

Las autenticaciones EAP-TLS y EAP-TTLS utilizan un certificado X.509 como identificación de un servidor de AAA y un dispositivo terminal. Además de la versión, el número de serie, el ID del algoritmo de firma, el nombre del firmante, el período de validez y la clave pública, el certificado X.509 también incluye un Asunto personalizado. Los operadores ponen su propio ID del nombre de red en el campo CN del Asunto para utilizarlo en la verificación del bloqueo en la red en el proceso de autenticación. El formato del certificado X.509 se muestra en la figura 1.

La arquitectura del certificado X.509 se muestra en la figura 2, en la que se puede omitir el certificado raíz de nivel secundario duplicado. Debido a que la firma se lleva a cabo capa a capa, solamente el certificado raíz que firma su certificado de nivel inferior puede verificar este certificado de nivel inferior, y los certificados con esta arquitectura de capas se denominan en conjunto una cadena de certificados, tal como se muestra en la figura 2.

Según el protocolo 806.16e, el proceso de acceso a la red por un dispositivo terminal WiMAX se divide en una serie de partes, que incluyen: la búsqueda de la red, la autenticación, el registro y el establecimiento de una conexión IP. En el que la parte de autenticación se utiliza para controlar el acceso a la red, y la función de bloqueo en la red propuesta en la presente invención se implementa en esta etapa.

Dos métodos recomendados por el protocolo WiMAX son el Protocolo de autenticación extensible - Seguridad de la capa de transporte (EAP-TLS, Extensible Authentication Protocol - Transport Layer Security) y el EAP - Seguridad de la capa de transporte tunelizada (EAP-TTLS, EAP Tunneled Transport Layer Security) basados en el certificado X.509, y los flujos de autenticación son similares para EAP-TLS y EAP-TTLS, excepto en que TTLS puede seleccionar una autenticación del dispositivo unidireccional (autenticando únicamente el servidor de AAA), y también puede seleccionar una autenticación del dispositivo bidireccional (el servidor de AAA autentica el dispositivo terminal y el dispositivo terminal autentica el servidor de AAA, tal como se muestra en la figura 3), y también puede seleccionar la autenticación del usuario (autenticando el usuario según el nombre y la contraseña del usuario).

En el método de autenticación de acceso a la red basado en EAP-TLS y EAP-TTLS, según la presente invención, se comprueba el bit indicador de bloqueo en la red y se comparan las cadenas de caracteres de bloqueo en la red, y si el bit indicador de bloqueo en la red está activado, entonces no se permite pasar la autenticación salvo que la cadena de caracteres de bloqueo en la red del certificado del servidor de AAA sea igual que la cadena de caracteres de bloqueo en la red memorizada en el dispositivo terminal, de lo contrario se devuelve un fallo de autenticación y se rechaza el acceso a la red, consiguiendo así el objetivo de bloqueo en la red. El método de bloqueo en la red se implementa adoptando el certificado del servidor para determinar si la red actual es o no una red legal en el proceso de autenticación, y si la red no es una red legal, la autenticación falla, lo que da lugar a un fallo de acceso a la red, consiguiendo así el objetivo de bloqueo en la red.

La autenticación bidireccional del dispositivo se tomará como ejemplo para la siguiente descripción.

Tal como se muestra en la figura 4, el flujo incluye específicamente:

Etapa -401-: un dispositivo terminal recibe una cadena de certificados transmitida por un servidor, esta cadena de certificados incluye el certificado del servidor de AAA y un certificado de nivel intermedio del mismo, en donde una cadena de caracteres en el campo CN del certificado del servidor es una cadena de caracteres de bloqueo en la red, que se utiliza para verificar el bloqueo en la red, y esta cadena de caracteres es el nombre del operador;

Etapa -402-: el dispositivo terminal comprueba un bit indicador de bloqueo en la red, y si este bit indicador de bloqueo en la red indica que la función de bloqueo en la red está activada, avanza a la etapa -403-, de lo contrario avanza a la etapa -404-;

Etapa -403-: el dispositivo terminal comprueba si la cadena de caracteres de bloqueo en la red en el certificado del servidor es igual que la memorizada en el dispositivo terminal, en caso afirmativo, avanza a la etapa -404-, de lo contrario determina que la red actual no es una red legal, y devuelve automáticamente el fallo de autenticación al servidor de AAA, rechaza el acceso a la red y finaliza el flujo;

Etapa -404-: el dispositivo terminal verifica la cadena de certificados del servidor recibida utilizando el certificado raíz de nivel superior de los certificados del servidor de AAA memorizados en el propio dispositivo terminal, y si se pasa la verificación, se avanza a la etapa -405-, de lo contrario se devuelve el fallo de autenticación para rechazar el acceso a la red y finalizar el flujo;

Etapa -405-: el dispositivo terminal transmite una cadena de certificados de dispositivo del dispositivo terminal (que incluye el certificado del dispositivo y los certificados de nivel intermedio) al servidor;

Etapa -406-: el servidor de AAA verifica la cadena de certificados del dispositivo recibida utilizando el certificado raíz memorizado del certificado del dispositivo, y si se pasa la verificación, la autenticación es satisfactoria, permitiendo el acceso a la red, de lo contrario la autenticación falla, rechazando el acceso a la red.

El flujo anterior se describe tomando como ejemplo el flujo de autenticación bidireccional del dispositivo terminal, sin embargo, se puede comprender que el método de la presente invención también es apropiado para implementar la función de bloqueo en la red en el flujo de autenticación unidireccional del dispositivo terminal, en el que la etapa -405- y la etapa -406- se omiten en comparación con el flujo anterior.

La presente invención adopta la cadena de caracteres de bloqueo en la red para verificar el bloqueo en la red, donde la cadena de caracteres de bloqueo en la red generalmente es el nombre del operador. El dispositivo terminal puede almacenar este valor en la memoria de sólo lectura programable y borrable eléctricamente (EEPROM, Electrically Erasable Programmable Read-Only Memory), y el bit indicador de activación para la función de bloqueo en la red también se puede almacenar en la EEPROM.

2. Procedimiento de desbloqueo

Dado que se permite que el propio usuario desbloquee el dispositivo, la función de desbloqueo se debería controlar para impedir la operación de desbloqueo no autorizada. En la presente memoria se adopta un modo de control que utiliza una clave. Se generará durante la fabricación del dispositivo una clave del dispositivo según información tal como el ID del dispositivo, la clave de control principal y similares, y a continuación se guardará en la EEPROM del dispositivo. Hay una correspondencia de uno a uno entre esta clave y el dispositivo. Cuando se entrega el dispositivo al operador, esta clave también se transfiere al operador de manera segura, y el operador almacena la clave en una base de datos segura. La clave se puede generar con algoritmos tales como SHA256 y similares.

Cuando un dispositivo terminal presenta una petición de desbloqueo y el operador la autoriza, o expira el límite de tiempo del bloqueo en la red, o se cumplen otras condiciones de desbloqueo para el dispositivo terminal cuya función de bloqueo en la red se ha activado, se puede utilizar el siguiente método para eliminar la restricción de acceso a la red impuesta por la función de bloqueo en la red.

Un servidor del operador hace uso del módulo inalámbrico (OTA) para implementar la función de gestión inalámbrica de los dispositivos terminales. El servidor del operador almacena parámetros de cada dispositivo terminal tales como el ID MAC, la clave de desbloqueo y similares. Un servidor OTA lee la clave de desbloqueo correspondiente a este dispositivo terminal, y la clave de desbloqueo de la EEPROM del dispositivo a través de la interfaz OTA, y las compara. Si son iguales, el servidor OTA establece el bit indicador de bloqueo en la red a FALSO y borra la cadena de caracteres de bloqueo en la red, de lo contrario el desbloqueo falla.

Tal como se muestra en la figura 5, ésta es un flujo de desbloqueo implementado por el servidor del operador o el dispositivo terminal, que incluye las siguientes etapas.

Etapa -501-: el servidor OTA obtiene la clave de desbloqueo del dispositivo terminal y el ID del dispositivo terminal, memorizados por el servidor del operador;

Etapa -502-: el servidor OTA de manera OTA obtiene la clave de desbloqueo memorizada por el dispositivo terminal con el ID correspondiente;

Etapa -503-: el servidor OTA compara las claves de desbloqueo obtenidas, y si son iguales, se lleva a cabo la etapa -504-, de lo contrario finaliza el flujo.

Etapa -504-: el servidor OTA transmite de manera OTA una notificación de desbloqueo al dispositivo terminal para que el dispositivo terminal restablezca el bit indicador de bloqueo en la red a FALSO y borre la cadena de caracteres de bloqueo en la red para implementar el desbloqueo.

La configuración de bloqueo en la red se puede también cambiar directamente por el servidor del operador o el dispositivo terminal sin realizar la verificación de la clave de desbloqueo. La verificación de la clave de desbloqueo es solamente para aumentar la seguridad.

3. Procedimiento de bloqueo de nuevo tras acceder a la red

Los dispositivos desbloqueados se pueden bloquear de nuevo tras volver a acceder a la red, lo que se implementa de manera OTA utilizando una interfaz aérea. El proceso de bloqueo de nuevo después de que el dispositivo accede a la red se muestra en la figura 6, que incluye las siguientes etapas.

Etapa -601-: un dispositivo terminal lee el bit indicador de bloqueo en la red memorizado en el dispositivo para determinar si se ha bloqueado, en caso afirmativo, finaliza el flujo, de lo contrario se lleva a cabo la etapa -602-;

Etapa -602-: el servidor OTA en el lado de red descubre de manera OTA que el dispositivo terminal no está bloqueado y, a continuación, calcula una clave de desbloqueo según los parámetros del dispositivo terminal tales como la dirección MAC, la hora actual, el ID de red y similares;

Etapa -603-: el servidor OTA en el lado de red transmite la clave de desbloqueo calculada al servidor del operador para su almacenamiento, y al mismo tiempo, transmite de manera OTA la clave de desbloqueo calculada al dispositivo terminal para que el dispositivo terminal actualice la clave de bloqueo en la red en la EEPROM;

Etapa -604-: el servidor OTA en el lado de red transmite de manera OTA una notificación de bloqueo al dispositivo terminal, donde la notificación de bloqueo lleva la cadena de caracteres de bloqueo en la red y el bit indicador de bloqueo en la red (VERDADERO o FALSO) para que el dispositivo terminal actualice el valor del campo correspondiente en la EEPROM.

Con el fin de implementar el método anterior, la presente invención también da a conocer un sistema para implementar el bloqueo del dispositivo terminal en la red. Este sistema incluye un servidor de AAA, un servidor del operador y un dispositivo terminal, donde,

El servidor del operador se utiliza para almacenar parámetros tales como el ID MAC del dispositivo terminal y la clave de bloqueo en la red y similares.

El servidor de AAA se refiere al servidor de red, que tiene funciones de Autenticación, Autorización y Contabilidad, e incluye particularmente un módulo transceptor y un módulo de autenticación, donde

El módulo transceptor se utiliza para recibir y transmitir diversos mensajes de señalización, incluyendo la transmisión de una cadena de certificados al dispositivo terminal, la recepción de la cadena de certificados transmitida por el dispositivo terminal y la transmisión de una respuesta de autenticación según el resultado de la autenticación, incluyendo dicha cadena de certificados transmitida al dispositivo terminal una cadena de caracteres de bloqueo en la red.

El módulo de autenticación sirve para verificar la cadena de certificados transmitida por el dispositivo terminal según el certificado memorizado por sí mismo.

El dispositivo terminal se refiere a un dispositivo terminal de un producto de red tal como una tarjeta de red, un teléfono móvil y similares, que incluye un módulo transceptor, un módulo de autenticación y un módulo de bloqueo en la red.

Donde, el módulo transceptor se utiliza para recibir o transmitir diversos mensajes de señalización, incluyendo la recepción de la cadena de certificados transmitida por el servidor de AAA y la transmisión de una cadena de certificados del dispositivo terminal al servidor de AAA, y la transmisión de respuestas de autenticación al servidor de AAA según los resultados de la verificación del módulo de autenticación y el módulo de bloqueo en la red.

Si no se pasa la verificación de módulo de bloqueo en la red, el módulo transceptor transmite directamente una respuesta de fallo de autenticación al servidor de AAA.

El módulo de autenticación se utiliza para verificar la cadena de certificados transmitida por el servidor de AAA según el certificado memorizado por sí mismo.

El módulo de bloqueo en la red se utiliza para almacenar el bit indicador de bloqueo en la red y la cadena de caracteres de bloqueo en la red, el bit indicador de bloqueo en la red se utiliza para indicar si la función de bloqueo en la red está activada, y si el bit indicador de bloqueo en la red indica que la función de bloqueo en la red está activada, el módulo de bloqueo en la red se utiliza también para verificar el bit indicador de bloqueo en la red en la cadena de certificados transmitida por el servidor de AAA y el bit indicador de bloqueo en la red memorizado por sí mismo, si son iguales, el módulo de bloqueo en la red también se utiliza para activar el módulo de autenticación para autenticar, si el bit indicador de bloqueo en la red indica que la función de bloqueo en la red no está activada, el módulo de bloqueo en la red también se utiliza para que el módulo de autenticación inicie directamente la autenticación.

Para implementar la función de desbloqueo, el sistema de la presente invención además incluye un servidor OTA, que se utiliza para obtener la clave de desbloqueo del dispositivo terminal en el servidor del operador y la clave de desbloqueo memorizada en el dispositivo terminal correspondiente, utilizándose también para comparar las claves de desbloqueo obtenidas y transmitir una notificación de desbloqueo si las claves de desbloqueo obtenidas son iguales.

Dicho módulo de bloqueo en la red del dispositivo terminal se utiliza para proporcionar la clave de desbloqueo memorizada al servidor OTA, restablecer el bit indicador de bloqueo en la red y borrar la cadena de caracteres de bloqueo en la red según la notificación de desbloqueo.

Para implementar de nuevo la función de bloqueo en la red tras acceder a la red, el servidor OTA también se utiliza para calcular la clave de desbloqueo del dispositivo terminal e notificar al servidor del operador y al dispositivo terminal que almacenen la clave de desbloqueo. El servidor OTA también se utiliza para enviar una notificación de bloqueo al dispositivo terminal, donde la notificación de bloqueo incluye el bit indicador de bloqueo en la red y la cadena de caracteres de bloqueo en la red.

Dicho módulo de bloqueo en la red del dispositivo terminal se utiliza para determinar si éste ha sido bloqueado según el bit indicador de bloqueo en la red, y también se utiliza para establecer el bit indicador de bloqueo en la red y actualizar la cadena de caracteres de bloqueo en la red según la notificación de bloqueo en la red transmitida por el servidor OTA para implementar de nuevo la función de bloqueo en la red tras acceder a la red.

Asimismo, la presente invención también da a conocer un dispositivo terminal, y este dispositivo terminal puede implementar la función de bloqueo en la red durante el acceso a la red. Y la arquitectura modular particular es la misma que en la descripción anterior.

En los anteriores método, sistema y dispositivo terminal, sólo se proporciona la posibilidad de activar la función de bloqueo en la red utilizando el bit indicador de bloqueo en la red, y el operador o el dispositivo terminal tienen derecho a seleccionar si desean activar la función de bloqueo en la red. Naturalmente, la presente invención también se puede implementar sin el bit indicador de bloqueo en la red. Para garantizar la compatibilidad con el dispositivo terminal existente, la presente invención se puede implementar determinando si este dispositivo terminal tiene la función de bloqueo en la red según una información que tenga un determinado significado descriptivo, como por ejemplo la fecha de fabricación del dispositivo terminal y, llevando a cabo a continuación una verificación de bloqueo en la red.

Para el modo EAP-TTLS según la presente invención, se puede utilizar cualquier método de autenticación, independientemente del modo de autenticación al que pertenezca, siempre que el método de autenticación incluya una autenticación para el servidor, debido a que la autenticación para el servidor significa que la cadena de caracteres de bloqueo en la red se puede leer a partir de la certificación del servidor, de tal modo que la cadena de caracteres de bloqueo en la red se puede comparar con la cadena de caracteres memorizada en el dispositivo terminal con el fin de conseguir el objetivo de bloqueo en la red.

Aplicabilidad industrial

En comparación con la técnica anterior, el método, el sistema y el dispositivo terminal de la presente invención adoptan el proceso de autenticación, y requieren que el dispositivo terminal y el servidor configuren uniformemente una cadena de caracteres de bloqueo en la red para tener una alta seguridad. Además, el método, el sistema y el dispositivo terminal de la presente invención pueden implementar el bloqueo y desbloqueo en la red tras acceder a la red a través de la gestión de la interfaz aérea de manera OTA, lo que tiene una gran flexibilidad y aplicabilidad, y puede cumplir perfectamente los requisitos de las redes 4G tales como la red WiMAX, la red LTE y similares.

REIVINDICACIONES

1. Método para implementar el bloqueo de un dispositivo terminal en una red, comprendiendo este método un procedimiento de bloqueo en la red durante el acceso a la red, en el que el procedimiento de bloqueo en la red comprende: realizar una verificación de la configuración de bloqueo en la red en un proceso de autenticación de acceso a la red, y si dicha verificación de la configuración de bloqueo en la red es satisfactoria, permitir la verificación de un certificado de autenticación, o de lo contrario rechazar el acceso del dispositivo terminal a la red;

en el que dicha verificación de la configuración de bloqueo en la red se refiere a la comparación de una cadena de caracteres de bloqueo en la red en un certificado de autenticación de un servidor de Autenticación, Autorización y Contabilidad, AAA, con una cadena de caracteres de bloqueo en la red memorizada en el dispositivo terminal, si la cadena de caracteres de bloqueo en la red en un certificado de autenticación del servidor de AAA es igual que la memorizada en el dispositivo terminal, se considera que la verificación de la configuración de bloqueo en la red es satisfactoria (403);

en dicha verificación de la configuración de bloqueo en la red, antes de realizar la comparación de las cadenas de caracteres de bloqueo en la red, determinar si una función de bloqueo en la red está activada según un bit indicador de bloqueo en la red memorizado en el dispositivo terminal, y en caso afirmativo, realizar la comparación de las cadenas de caracteres de bloqueo en la red, o de lo contrario realizar directamente la verificación del certificado de autenticación (402);

el método además comprende un procedimiento de desbloqueo, y este procedimiento comprende:

un servidor inalámbrico, OTA, que obtiene una clave de desbloqueo de dicho dispositivo terminal y un ID de dicho dispositivo terminal memorizados por un servidor del operador;

dicho servidor OTA obtiene de manera OTA una clave de desbloqueo memorizada por dicho dispositivo terminal con el ID;

dicho servidor OTA compara las claves de desbloqueo obtenidas;

si las claves de desbloqueo son iguales, dicho servidor OTA notifica de manera OTA a dicho dispositivo terminal que establezca el bit indicador de bloqueo en la red como función de bloqueo en la red desactivada y borre dicha cadena de caracteres de bloqueo en la red.

2. Método, según la reivindicación 1, en el que dicho proceso de autenticación de acceso a la red se refiere a un proceso en el que el dispositivo terminal autentica el servidor de Autenticación, Autorización y Contabilidad, AAA.

3. Método, según la reivindicación 1, que comprende además: un procedimiento de bloqueo de nuevo tras acceder a la red, comprendiendo este procedimiento: el servidor inalámbrico, OTA, calcula una clave de desbloqueo de dicho dispositivo terminal, y notifica al servidor del operador y a dicho dispositivo terminal que almacenen esta clave de desbloqueo; dicho servidor OTA transmite el bit indicador de bloqueo en la red y la cadena de caracteres de bloqueo en la red a dicho dispositivo terminal; y dicho dispositivo terminal almacena esta cadena de caracteres de bloqueo en la red y establece dicho bit indicador de bloqueo en la red como función de bloqueo en la red activada (601-604).

4. Sistema para implementar el bloqueo de un dispositivo terminal en una red, en el que este sistema está adaptado para realizar la verificación de la configuración de bloqueo en la red en un proceso de autenticación de acceso a la red, y permitir la verificación de un certificado de autenticación si dicha verificación de la configuración de bloqueo en la red es satisfactoria, o de lo contrario rechazar el acceso del dispositivo terminal a la red;

en el que este sistema incluye un servidor de Autenticación, Autorización y Contabilidad, AAA, y un dispositivo terminal, en el que,

dicho servidor de AAA está adaptado para transmitir un certificado de autenticación al dispositivo terminal, incluyendo dicho certificado de autenticación una cadena de caracteres de bloqueo en la red;

dicho dispositivo terminal incluye un módulo transceptor y un módulo de bloqueo en la red, en el que,

dicho módulo transceptor está adaptado para recibir dicho certificado de autenticación;

dicho módulo de bloqueo en la red está adaptado para realizar una verificación de bloqueo en la red para una cadena de caracteres de bloqueo en la red en el certificado de autenticación transmitido por el servidor de AAA y una cadena de caracteres de bloqueo en la red memorizada en el dispositivo terminal;

dicho módulo de bloqueo en la red además está adaptado para almacenar un bit indicador de bloqueo en la red; y si el bit indicador de bloqueo en la red indica que la función de bloqueo en la red está desactivada, dicho módulo de

red de bloqueo también está adaptado para activar directamente dicho módulo de autenticación para que realice la autenticación, o de lo contrario para iniciar la verificación de la cadena de caracteres de bloqueo en la red

en el que dicho sistema además incluye un servidor inalámbrico, OTA, y un servidor del operador; dicho servidor OTA está adaptado para: obtener una clave de desbloqueo de dicho dispositivo terminal y un ID de dicho dispositivo terminal memorizado por dicho servidor del operador, obtener de manera OTA una clave de desbloqueo memorizada por dicho dispositivo terminal con el ID, comparar las claves de desbloqueo obtenidas, y si las claves de desbloqueo son iguales, notificar de manera OTA a dicho dispositivo terminal que establezca el bit indicador de bloqueo en la red como función de bloqueo en la red desactivada y borre dicha cadena de caracteres de bloqueo en la red para implementar una función de desbloqueo.

5. Sistema, según la reivindicación 4, en el que dicho dispositivo terminal además incluye un módulo de autenticación, en el que,

dicho módulo de bloqueo en la red además está adaptado para activar dicho módulo de autenticación para que realice la autenticación si la cadena de caracteres de bloqueo en la red del certificado de autenticación transmitido por el servidor de AAA es igual que la memorizada en el dispositivo terminal;

dicho módulo de autenticación está adaptado para verificar el certificado de autenticación transmitido por el servidor de AAA según un certificado memorizado por sí mismo.

6. Sistema, según la reivindicación 4, en el que dicho servidor OTA también está adaptado para calcular una clave de desbloqueo y notificar a dicho servidor del operador y a dicho dispositivo terminal que almacenen esta clave de desbloqueo, y para notificar a dicho dispositivo terminal que almacene la cadena de caracteres de bloqueo en la red y establezca el bit indicador de bloqueo en la red para implementar la función de bloqueo de nuevo tras acceder a la red; estando adaptado dicho módulo de bloqueo en la red del dispositivo terminal para realizar el almacenamiento y la actualización según las notificaciones del servidor OTA.

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 7829 (0x1e95)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST= Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
        Validity
            Not Before: Jul 9 16:04:02 1998 GMT
            Not After : Jul 9 16:04:02 1999 GMT
        Subject: c=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                 OU=FreeSoft, CN=ZTE Corporation
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit)
                    00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                    33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                    66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                    70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                    16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                    c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                    8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                    d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                    e8:35:1c:9e:27:52:7e:41:8f
                Exponent: 65537 (ox10001)
    Signature Algorithm: md5WithRSAEncryption
        93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
        92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
        ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
        d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
        0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
        5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
        8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
        68:9f
```

FIG. 1

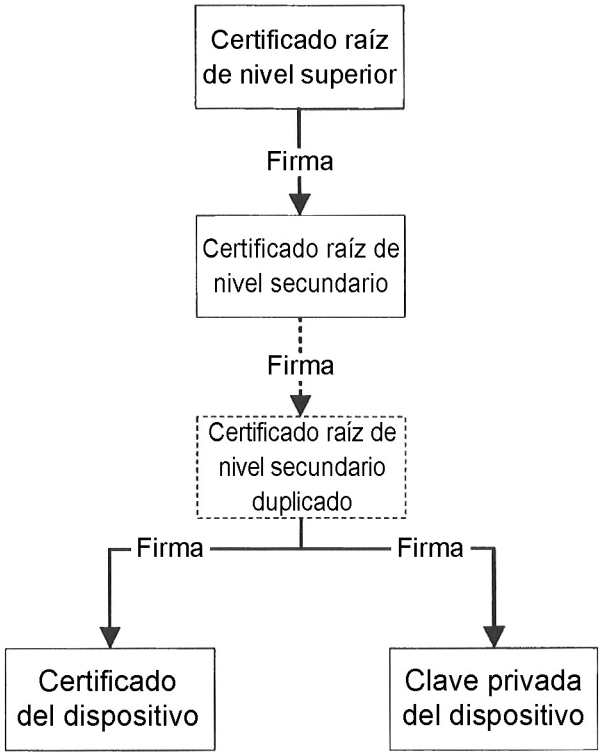
Certificado raíz de nivel superior
Firma
Certificado raíz de nivel secundario
Firma
Certificado raíz de nivel secundario duplicado
Firma
Firma
Certificado del dispositivo
Clave privada del dispositivo

FIG. 2

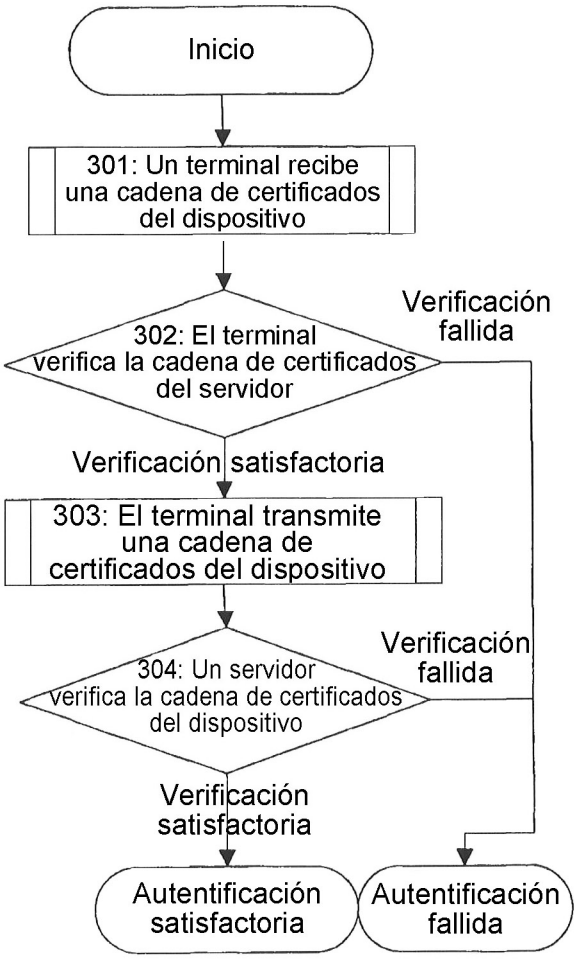
Inicio
301: Un terminal recibe una cadena de certificados del dispositivo
302: El terminal verifica la cadena de certificados del servidor
Verificación fallida
Verificación satisfactoria
303: El terminal transmite una cadena de certificados del dispositivo
304: Un servidor verifica la cadena de certificados del dispositivo
Verificación fallida
Verificación satisfactoria
Autentificación satisfactoria
Autentificación fallida

FIG. 3

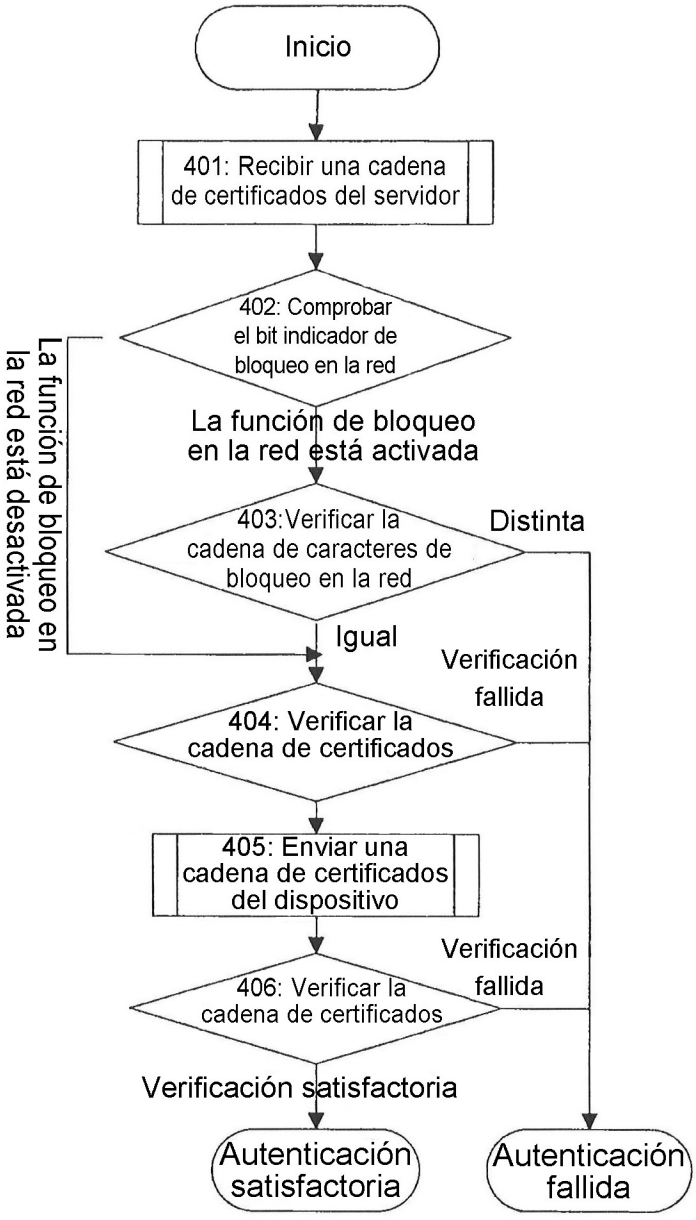
Inicio
401: Recibir una cadena de certificados del servidor
402: Comprobar el bit indicador de bloqueo en la red
La función de bloqueo en la red está activada
La función de bloqueo en la red está desactivada
403:Verificar la cadena de caracteres de bloqueo en la red
Distinta
Igual
Verificación fallida
404: Verificar la cadena de certificados
405: Enviar una cadena de certificados del dispositivo
Verificación fallida
406: Verificar la cadena de certificados
Verificación satisfactoria
Autenticación satisfactoria
Autenticación fallida

FIG. 4

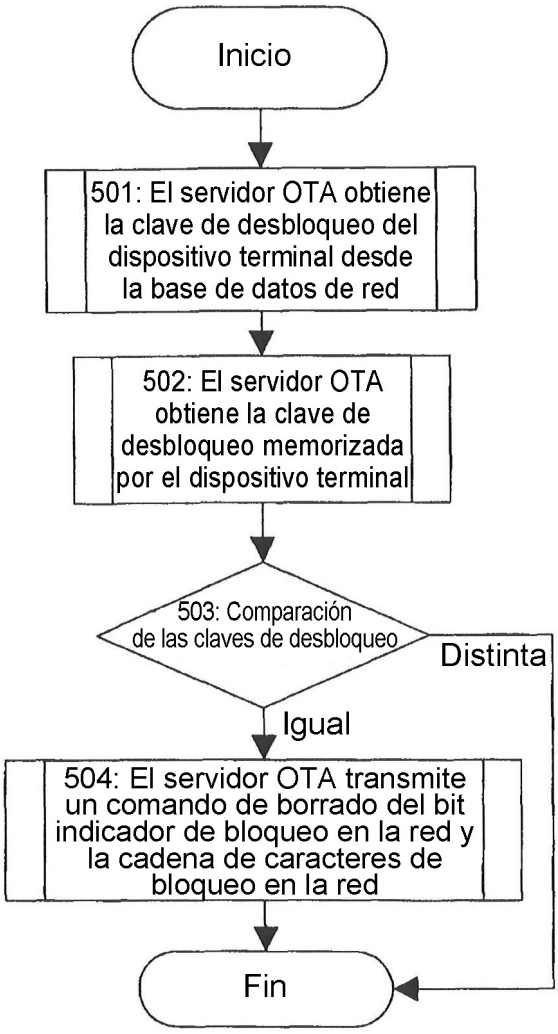
Inicio
501: El servidor OTA obtiene la clave de desbloqueo del dispositivo terminal desde la base de datos de red
502: El servidor OTA obtiene la clave de desbloqueo memorizada por el dispositivo terminal
503: Comparación de las claves de desbloqueo
Distinta
Igual
504: El servidor OTA transmite un comando de borrado del bit indicador de bloqueo en la red y la cadena de caracteres de bloqueo en la red
Fin

FIG. 5

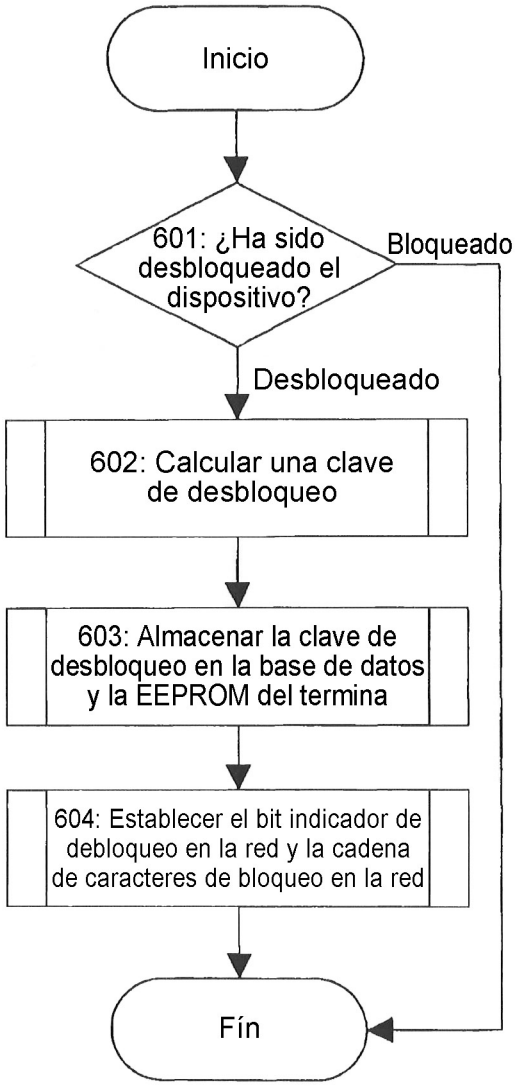
Inicio
601: ¿Ha sido desbloqueado el dispositivo?
Bloqueado
Desbloqueado
602: Calcular una clave de desbloqueo
603: Almacenar la clave de desbloqueo en la base de datos y la EEPROM del termina
604: Establecer el bit indicador de debloqueo en la red y la cadena de caracteres de bloqueo en la red
Fín

FIG. 6