(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 401 027**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.04.2007 E 07720902 (1)**

(97) Fecha y número de publicación de la concesión europea: **26.12.2012 EP 2015507**

(54) Título: **Gestión segura de una red doméstica**

(30) Prioridad:

28.04.2006 CN 200610060542

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.04.2013

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
HUAWEI ADMINISTRATION BUILDING BANTIAN LONGGANG DISTRICT
SHENZHEN GUANGDONG PROVINCE 518129, CN

(72) Inventor/es:

DING, ZHIMING

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Gestión segura de una red doméstica

Antecedentes de la invención

Campo de la invención

La presente invención está relacionada con la tecnología de gestión de la seguridad de dispositivos de una red doméstica y, más en particular, con un sistema y un método de gestión de la seguridad de una red doméstica.

Descripción de la técnica asociada

En la actualidad, están a punto de reemplazarse los modem ADSL que convencionalmente únicamente realizan funciones de acceso por un dispositivo denominado “pasarela doméstica (HGW)” con funciones más amplias. Como se muestra en la FIG. 1, la HGW no realiza únicamente las funciones de acceso y encaminamiento del modem ADSL, sino que también integra la función de conmutación LAN, proporciona el cortafuegos, NAT, QoS, servicio de tiempo, etc., e incluso proporciona directamente el servicio de VoIP. Además, la HGW proporciona, en general, una función de acceso inalámbrico de modo que un ordenador con una tarjeta de red inalámbrica se pueda conectar con la HGW sin ningún cable.

El foro de tecnología de UPnP es una organización que investiga la tecnología de plug and play (conexión y uso inmediato) de los dispositivos de red domésticos y fue promovida por Microsoft Corporation. La organización investiga el protocolo de comunicación de Plug and Play Universal (UPnP) con el objetivo de permitir que cualquier dispositivo inteligente de aplicación doméstica, incluyendo dispositivos de información domésticos, se puedan utilizar con acceso a la red con este protocolo de forma tan sencilla como las aplicaciones domésticas de hoy en día sin necesitar usuarios expertos. Dicha red se denomina red UPnP.

El protocolo UPnP clasifica de forma lógica las entidades de red en puntos de control (CP) y dispositivos. Los CP descubren y controlan los dispositivos. Después del inicio, el CP busca de forma activa los dispositivos existentes en la red. El dispositivo lleva a cabo una función de aplicación específica. Después del inicio, el dispositivo informa de su existencia al exterior de modo que los CP le puedan descubrir y en la declaración hace públicos eventos que puede llevar a cabo. Después del descubrimiento del dispositivo, el CP puede suscribirse a un evento del dispositivo CP que le interese. Después de producirse el evento, el dispositivo envía este evento al CP que se ha suscrito a este evento. Igualmente, el CP puede controlar el evento del dispositivo. El CP puede controlar el dispositivo automáticamente o mediante una interfaz hombre-máquina. Debe observarse que los dispositivos mencionados en el UPnP son entidades lógicas en lugar de dispositivos físicos. Un dispositivo físico puede consistir en uno o más dispositivos UPnP, o incluir, además, una entidad CP. Un dispositivo físico también puede consistir en solo un CP. En casos especiales, un dispositivo físico puede incluir múltiples CP, por ejemplo, múltiples fragmentos de software en el ordenador que llevan a cabo funciones de múltiples entidades CP.

El protocolo UPnP también tiene un mecanismo de seguridad y, por lo tanto, se añade una entidad de consola de seguridad (SC). La SC no es solo un CP, sino que también es un dispositivo. Como CP, la SC puede descubrir y controlar otros dispositivos/SC. Como dispositivo, la SC puede anunciarse a sí misma a otros CP/SC y ser controlada.

El mecanismo de seguridad del UPnP se adopta teniendo en cuenta el acceso a y el control sobre los dispositivos de seguridad del CP/SC. El UPnP clasifica los dispositivos en dispositivos de seguridad y dispositivos que no son de seguridad. El acceso a y el control sobre un dispositivo de seguridad está limitado y el dispositivo de seguridad tiene que autorizarlo. Más aún, cuando se accede a un dispositivo de seguridad, es necesario certificar el dispositivo de acceso.

El dispositivo UPnP proporciona uno o más servicios. La diferencia entre el dispositivo de seguridad y el dispositivo que no es de seguridad reside en que el dispositivo de seguridad tiene un servicio especial de seguridad. Mediante el servicio de seguridad del dispositivo, la SC puede obtener la clave, el certificado, la lista de control de acceso, la lista de propietarios y otra información para utilizar el dispositivo. El dispositivo de seguridad UPnP utiliza la lista de propietarios, la lista de control de acceso y el certificado como tres elementos para componer un marco de seguridad de gestión de la autoridad de acceso.

El dispositivo almacena una lista de propietarios que registra a qué CP/SC pertenece este dispositivo. Los CP/SC (i.e. propietarios) a los que pertenece este dispositivo tienen el 100% de derechos de control sobre este dispositivo. El primer propietario (necesariamente la SC) del dispositivo obtiene la propiedad de este dispositivo mediante el Protocolo Simple de Descubrimiento de Servicios (SSDP) en combinación con una operación manual. Cada dispositivo de seguridad tiene un sistema de claves inicial. Para llevar a cabo la operación de primera propiedad, el dispositivo de seguridad tiene un ID de seguridad y una contraseña inicial (debe observarse que la SC es también un dispositivo de seguridad) pudiéndose obtener ambos directamente desde el cuerpo de la máquina, la pantalla, o una

tarjeta de claves del dispositivo. Cuando el dispositivo tiene una lista de propietarios vacía y accede a la red UPnP, la SC puede descubrir este dispositivo mediante el protocolo de descubrimiento automático, determinar que es un dispositivo de seguridad mediante la característica de que dispone de un servicio de seguridad, leer el ID de seguridad del dispositivo y, después, mostrárselo al usuario. El usuario identifica el dispositivo mediante el ID de seguridad, selecciona el dispositivo y, a continuación, le asigna un nombre al dispositivo. El dispositivo que al que se ha asignado el nombre se muestra con su nombre en lugar de utilizar el ID de seguridad (el nombre se almacena en la SC). El usuario puede continuar introduciendo la contraseña inicial del dispositivo. Después de una confirmación, la SC envía su propio ID de seguridad al dispositivo. El dispositivo añade esta SC a la lista de propietarios y la SC es propietaria de este dispositivo. A partir de ese momento, otros SC/CP pueden ser propietarios de este dispositivo mediante la operación de autorización en esta SC.

El dispositivo también almacena una lista de control de acceso para autorizar parcialmente a los CP/SC. Los CP/SC autorizados parcialmente no son propietarios del dispositivo y únicamente pueden tener un acceso limitado a este dispositivo. El usuario puede editar la lista de control de acceso en la SC que es propietaria de este dispositivo. Las afirmaciones de que el dispositivo autoriza a los CP/SC y que la SC propietaria del dispositivo autoriza a otros CP/SC tienen el mismo significado porque si un propietario posee completamente el dispositivo, el propietario se convierte en un representante apropiado del dispositivo.

Cada CP/SC que pueda utilizar el dispositivo de seguridad mantiene un certificado que indica la autoridad legítima de este dispositivo. Este certificado lo genera la SC propietaria del dispositivo.

El mecanismo de seguridad del UPnP también utiliza un modo de firma y cifrado para garantizar la seguridad de los mensajes. El dispositivo tiene una clave pública inicial que la SC puede obtener directamente. El ID de seguridad del dispositivo de seguridad es en realidad un valor hash visual basado en su clave pública con, generalmente, pocos bits, el cual se utiliza únicamente para identificación y es equivalente al nombre. Este ID de seguridad lo obtienen tanto la SC como el dispositivo mediante exactamente el mismo algoritmo hash.

El mecanismo de seguridad del UPnP es igualmente aplicable a un acceso con cable o inalámbrico y, por supuesto, se propone primero para el acceso inalámbrico. El acceso con cable está restringido físicamente al interior de una casa que se considera segura. Como se muestra en la FIG. 2, con respecto al acceso inalámbrico, un CP/SC ilegal no puede utilizar el dispositivo ya que no puede ser autorizado por el dispositivo de seguridad, garantizando, por lo tanto, la seguridad. De forma parecida, este mecanismo funciona igualmente en el acceso con cable extendido en el exterior.

Como se puede observar a partir de la descripción anterior, el mecanismo de seguridad del UPnP tiene los siguientes defectos.

(1) El mecanismo de seguridad del UPnP necesita la intervención manual. Los procesos de propiedad y autorización descritos por el mecanismo de seguridad del UPnP no son simples, y el usuario sigue necesitando poseer cierta experiencia, por ejemplo, conocimiento sobre la lista de propietarios, la lista de control de acceso, etcétera.

(2) El mecanismo de seguridad del UPnP evita que dispositivos (físicos) no autorizados accedan a dispositivos de seguridad protegidos por la autoridad, pero no puede evitar que usuarios ilegales accedan a aquellos dispositivos de seguridad ni evitar que dispositivos de seguridad no-UPnP accedan a la red y accedan, además, a Internet a través de la HGW, i.e., apropiándose de cuentas de acceso a Internet. La última situación ocurre fácilmente cuando se utiliza el acceso inalámbrico.

(3) Antes de transferir (por ejemplo, por reventa) un dispositivo UPnP, el dispositivo se debe devolver a su estado inicial, i.e., las configuraciones de fábrica y la eliminación de propietarios artificialmente. En el caso de una transferencia antes de devolverlo al estado inicial (por ejemplo, un robo), la falsificación de cuentas ocurre fácilmente. Por ejemplo, un dispositivo de usuarios de VoIP en general asocia un número llamante con el propio dispositivo. Después de que el dispositivo se ha transferido a algún sitio, el número original puede seguirse utilizando para realizar una llamada IP.

Una publicación de patente europea (número de publicación: EP 1372301A) divulga un sistema de red. En el sistema, el MTID de un equipo terminal se registra de forma preliminar en una base de datos de un ISP. En alguna ocasión, el router recibe una señal de transmisión y se transmite el dato (HGWID = A, MTID = B) desde el router al ISP. Si en la base de datos se ha registrado el dato (HGWID = A, MTID = B), el ISP transmite un mensaje de autorización y si el dato (HGWID = A, MTID = B) no se ha registrado, se envía al router un mensaje de rechazo.

Una publicación de patente europea (número de publicación: EP 1416684A1) divulga un dispositivo doméstico instalado en un hogar, el dispositivo está conectado a una red sin conexión de tipo abierto desde el exterior. El dispositivo doméstico establece una conexión mediante la red y la mantiene transmitiendo continuamente paquetes de datos a un servidor de red dentro de cierto período de tiempo. Un terminal de usuario fuera de la casa obtiene el acceso al dispositivo doméstico mediante el servidor de red.

Una publicación de solicitud de patente de los Estados Unidos (número de publicación: US 2005/0210532 A1) divulga dispositivos electrónicos en una LAN, por ejemplo, un grabador de vídeo DVD, una pantalla de plasma y un controlador de audio en una red doméstica. Los dispositivos están protegidos por un sistema de seguridad que está conectado en red con los dispositivos. En un aspecto, el sistema de seguridad sondea periódicamente a los dispositivos para confirmar que se encuentran presentes en la LAN. Si un dispositivo no responde, se activa una alarma. Se detecta la instalación del dispositivo electrónico en una red no autorizada verificando la dirección IP del dispositivo como, por ejemplo, cuando el dispositivo intenta contactar con un servidor que proporciona servicios como, por ejemplo, descargar software nuevo o actualizado al dispositivo, realizar programación remota y enviar al servidor datos de diagnóstico. Los dispositivos pueden cifrar sus mensajes utilizando códigos de cifrado que son únicos individualmente o para un grupo específico de dispositivos electrónicos.

Resumen de la invención

A la vista de los defectos descritos más arriba de la técnica anterior, algunos modos de realización de la presente invención se orientan a resolver el problema de que la autorización de un acceso de un dispositivo deba ser realizada mediante una operación manual de un usuario, y en el mecanismo actual se puede producir fácilmente la apropiación indebida de una cuenta de usuario y del dispositivo.

Un modo de realización de la presente invención proporciona un método de gestión de la seguridad de una red doméstica. El método incluye los siguientes pasos:

enviar a un servidor de gestión de la seguridad, SMS, por parte de un módulo de gestión de la seguridad, SMM, un mensaje de registro de la red doméstica; en donde, el mensaje de registro de la red doméstica comprende, al menos, una identificación del terminal de red, NTID, de un dispositivo que tiene el SMM, la NTID es capaz de identificar unívocamente a un dispositivo, el SMM se encuentra dentro de la red doméstica y el SMM se comunica con el SMS mediante una pasarela doméstica, HGW, dentro de la red doméstica;

obtener desde el dispositivo de usuario, por parte del SMM, una NTID del dispositivo de usuario dentro de la red doméstica; y

enviar al SMS, por parte del SMM, un mensaje de registro del dispositivo de usuario; en donde el mensaje de registro del dispositivo de usuario comprende, al menos, la NTID del dispositivo de usuario y una identificación de red, NID, de la red doméstica, y la NID es capaz de identificar la red doméstica de forma unívoca;

en donde, el SMS está adaptado para determinar si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario.

Un modo de realización de la presente invención proporciona otro método de gestión de la seguridad de una red doméstica. El método incluye los siguientes pasos:

obtener, por parte de un servidor de gestión de la seguridad, SMS, un mensaje de registro de la red doméstica desde un módulo de gestión de la seguridad, SMM; en donde el mensaje de registro de la red doméstica comprende, al menos, una identificación de terminal de red, NTID, de un dispositivo que tiene el SMM, la NTID es capaz de identificar un dispositivo de forma unívoca, el SMM se encuentra dentro de la red doméstica y el SMS se comunica con el SMM mediante una pasarela doméstica, HGW, dentro de la red doméstica;

obtener del SMM, por parte del SMS, un mensaje de registro de un dispositivo de usuario dentro de la red doméstica; en donde el mensaje de registro del dispositivo de usuario comprende, al menos, la NTID del dispositivo de usuario y una identificación de red, NID, de la red doméstica, la NID es capaz de identificar la red doméstica de forma unívoca y el SMM obtiene desde el dispositivo de usuario la NTID del dispositivo de usuario; y

determinar, por parte del SMS, si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario.

Un modo de realización de la presente invención proporciona un módulo de gestión de la seguridad (SMM). El SMM está adaptado para:

enviar un mensaje de registro de la red doméstica a un servidor de gestión de la seguridad, SMS; en donde el mensaje de registro de la red doméstica comprende, al menos, una identificación de terminal de red, NTID, de un dispositivo que tiene el SMM, la NTID es capaz de identificar un dispositivo de forma unívoca, el SMM se encuentra dentro de la red doméstica, y el SMM se comunica con el SMS mediante una pasarela doméstica, HGW, dentro de la red doméstica;

obtener del dispositivo de usuario una NTID de un dispositivo de usuario dentro de la red doméstica; y

enviar al SMS un mensaje de registro del dispositivo de usuario; en donde el mensaje de registro del dispositivo de usuario comprende, al menos, la NTID del dispositivo de usuario y una identificación de red, NID, de la red

doméstica, y la NID es capaz de identificar la red doméstica de forma unívoca;

en donde el SMS está adaptado para determinar si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario.

Un modo de realización de la presente invención proporciona un módulo de gestión de la seguridad (SMS). El SMS está adaptado para:

obtener desde un módulo de gestión de la seguridad, SMM, un mensaje de registro de la red doméstica; en donde el mensaje de registro de la red doméstica comprende, al menos, una identificación de terminal de red, NTID, de un dispositivo que tiene el SMM, la NTID es capaz de identificar un dispositivo de forma unívoca, el SMM se encuentra dentro de la red doméstica, y el SMS se comunica con el SMM a través de una pasarela doméstica, HGW, dentro de la red doméstica;

obtener desde el SMM un mensaje de registro de un dispositivo de usuario dentro de la red doméstica; en donde el mensaje de registro del dispositivo de usuario comprende, al menos, la NTID del dispositivo de usuario y una identificación de red, NID, de la red doméstica, la NID es capaz de identificar la red doméstica de forma unívoca, y el SMM obtiene desde el dispositivo de usuario la NTID del dispositivo de usuario; y

determinar si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario.

Con los esquemas técnicos descritos más arriba, los modos de realización de la presente invención tienen, al menos, los siguientes efectos beneficiosos.

(1) Siempre que el usuario solicite previamente al SMS un servicio de seguridad para su dispositivo, el dispositivo puede realizar automáticamente un proceso de registro al servicio de seguridad similar al proceso de confirmación manual del usuario en el mecanismo de seguridad UPnP al acceder a la red, y este proceso de solicitud previa únicamente requiere que el usuario proporcione información relevante en lugar de entender problemas técnicos.

(2) La seguridad del acceso es más robusta que la del mecanismo de seguridad UPnP. Todos los dispositivos a los que se accede pueden verificar la validez de los dispositivos que acceden mediante registros.

(3) Debido a que el dispositivo se registra con el SMS, el SMS descubrirá un dispositivo después de haber sido transferido de forma ilegal a otra red. Se puede resolver el problema de que la cuenta de usuario y el dispositivo sean fácilmente utilizadas de forma fraudulenta debido al SMM dispuesto.

Breve descripción de los dibujos

La presente invención será comprendida de forma más completa a partir de la descripción detallada ofrecida en la presente solicitud más abajo únicamente a modo de ilustración y así no resulta limitante de la presente invención, y en donde:

la FIG. 1 es un diagrama de ejemplo que ilustra las conexiones de una red doméstica;

la FIG. 2 es un diagrama esquemático de un mecanismo actual;

la FIG. 3 es un diagrama de la estructura de un modo de realización de un sistema de la presente invención;

la FIG. 4 es un diagrama de flujo que ilustra un proceso cuando un módulo de gestión de la seguridad (SMS) recibe un mensaje de registro de servicio de seguridad de red de un módulo de gestión de la seguridad (SMM) en un modo de realización de un método de la presente invención;

la FIG. 5 es un diagrama de flujo que ilustra un proceso para que un equipo en las instalaciones del cliente (CPE) que no es de seguridad con solicitud previa para un servicio de seguridad registre en primer lugar el servicio de seguridad en el modo de realización del método de la presente invención;

la FIG. 6 es un diagrama de flujo que ilustra procesos para que un CPE de seguridad con solicitud previa para un servicio de seguridad registre en primer lugar el servicio de seguridad en el modo de realización del método de la presente invención;

la FIG. 7 es un diagrama de flujo que ilustra procesos para que un CPE que no es de seguridad sin solicitud previa para un servicio de seguridad registre en primer lugar el servicio de seguridad en el modo de realización del método de la presente invención;

la FIG. 8 es un diagrama de flujo que ilustra procesos para que un CPE de seguridad sin solicitud previa para un servicio de seguridad registre en primer lugar el servicio de seguridad en el modo de realización del método de la

presente invención;

la FIG. 9 es un diagrama de flujo que ilustra procesos para que un dispositivo legítimo vuelva a registrar un servicio de seguridad en el modo de realización del método de la presente invención;

la FIG. 10 es un diagrama de flujo que ilustra un procesamiento cuando el SMS descubre un dispositivo ilegal en el modo de realización del método de la presente invención;

la FIG. 11 es un diagrama de flujo que ilustra un primer paso para que un CPE1 acceda a un CPE2: incluyendo una identificación de dispositivo (NTID) cuando se establece una conexión en el modo de realización del método de la presente invención;

la FIG. 12 es un diagrama que ilustra un primer paso para que un CPE1 acceda a un CPE2: sin incluir una NTID cuando se establece una conexión en el modo de realización del método de la presente invención;

la FIG. 13 es un diagrama de flujo que ilustra procesos para que el CPE2 autentifique al CPE1 en el modo de realización del método de la presente invención;

la FIG. 14 es un diagrama de flujo que ilustra procesos para que un usuario cancele el servicio de seguridad del CPE con el SMS en el modo de realización del método de la presente invención; y

la FIG. 15 es un diagrama de flujo que ilustra una confirmación en línea para transferir un dispositivo en el modo de realización del método de la presente invención.

Descripción detallada de los modos de realización

En los modos de realización de la presente invención se proporciona un mecanismo de gestión de la seguridad de dispositivos de red utilizando un concepto de identificación de red (NID) junto con identificaciones de terminal de red (NTID) únicas. La NID es una cadena de caracteres asignada automáticamente por un servidor en una red pública, i.e. una red de área amplia (WAN), o designada por un usuario, e identifica de forma unívoca a una red de área local (LAN). La NTID es una cadena de información reconocible por todos los dispositivos en una red doméstica del usuario que tiene un formato unificado y que puede identificar un dispositivo de forma unívoca. El formato de la NTID puede ser el formato “OUI-device serial number” (número de serie del dispositivo OUI) definido en el documento técnico TR069 del foro de DSL. También existen otras formas para la información de NTID única como, por ejemplo, una identificación de dispositivo de una pasarela doméstica (HGW) o una identificación de dispositivo de un dispositivo que tiene un módulo de gestión de la seguridad (SMM), una cuenta de acceso WAN, un nombre de dominio de Internet o una dirección IP fija y un número de teléfono doméstico del usuario.

Como se muestra en la FIG. 3, el sistema en un modo de realización de la presente invención incluye un servidor de gestión de la seguridad (SMS) en la red pública, un SMM dentro de la red doméstica, todos los equipos en las instalaciones del cliente (CPE, i.e., dispositivos de usuario) en la red doméstica, y un servidor de configuración automática (ACS) en la red pública. En un sentido amplio, el CPE puede incluir el SMM y la HGW. A continuación se introducirán las funciones de cada una de las entidades funcionales de la FIG. 3. El SMM puede ser un dispositivo físico independiente o un módulo funcional de otro dispositivo, por ejemplo, un módulo funcional de la HGW.

1. SMS

En un modo de realización de la presente invención, se dispone en la WAN un servidor de gestión de la seguridad (SMS). Se puede denominar proveedor de servicios de seguridad de redes domésticas (SSP) a una entidad empresarial que es propietaria y gestiona este servidor. El SMS proporciona servicio para una gestión de la seguridad de los dispositivos de la red doméstica y tiene las siguientes funciones principales.

1) El SMS acepta la solicitud del usuario para un servicio de seguridad de red.

1.1) Cuando solicita el servicio de seguridad de red, el usuario proporciona una NTID del dispositivo del SMM.

1.2) El SMS genera automáticamente una identificación de red (NID) doméstica única y una contraseña, o acepta una NID y una contraseña especificada por el usuario con el fin de asegurar la unicidad de la NID.

1.3) En una lista de NID (NID-L) se generan nuevos registros. En la Tabla 1 se muestra una estructura de la NID-L.

Tabla 1 Formato de la NID-L

NID	$PSW_{(NID)}$	$NTID_{(SMM)}$	$SKey_{(SMM)}$	Nombre de usuario	Dirección de usuario	Otro método de contacto	Estado	Observaciones	Última vez que se ha registrado

NID: una identificación de red única asignada automáticamente por el SMS o especificada por el usuario.

$PSW_{(NID)}$: una contraseña correspondiente de la NID, generada automáticamente por el SMS o especificada por el usuario.

$NTID_{(SMM)}$: una identificación única del SMM del dispositivo de usuario (ver descripción posterior) proporcionada por el usuario cuando solicita el servicio de seguridad de red.

$SKEY_{(SMM)}$: una clave pública de cifrado del SMM.

Nombre de usuario: el nombre del usuario, al cual se puede añadir información de la tarjeta de identidad.

Dirección de usuario: información de la dirección del usuario.

Otro método de contacto: número de teléfono o correo electrónico y similares para contactar con el usuario en casos especiales.

Estado: sus valores se describen a continuación.

"1"-solicitado: el SMM del usuario no se ha registrado con el SMS; un valor inicial de un nuevo registro.

"2"-bajo solicitud: el SMM del usuario se ha registrado con el SMS, no indica si el dispositivo se encuentra en línea.

"3"-baja: el usuario ha cancelado el servicio de seguridad de red. Dicho registro se puede transferir a otra lista y almacenarse para una referencia futura.

Última vez que se ha registrado: la última vez que el SMM se registra en el servicio de seguridad, la cual se anota cuando el SMS acepta el registro.

Observaciones: otra información útil.

2) El SMS acepta el registro del servicio de seguridad de la red doméstica del usuario.

Después de que el usuario solicite el servicio de seguridad de red, el SMM de la red del usuario puede registrar el servicio de seguridad de la red con el SMS para obtener su propia NID. El proceso se describirá en el método de registro del servicio de seguridad de la red.

3) El SMS acepta la solicitud previa del usuario del servicio de seguridad para su CPE.

3.1) Cuando solicita previamente el servicio de seguridad para su CPE, el usuario debería proporcionar la NID, la $PSW_{(NID)}$, la NTID del CPE y una contraseña inicial del CPE (cuando el CPE es un dispositivo de seguridad).

3.2) El SMS genera nuevos registros en una lista NTID (NTID-L). En la Tabla 2 se muestra el formato de la NTID-L

Tabla 2 Formato de la NTID-L

$NTID_{(CPE)}$	NID	$PSW_{(CPE)}$	Estado	Última vez que se ha registrado

$NTID_{(CPE)}$: la NTID del CPE.

NID: la NID de la red doméstica del CPE.

$PSW_{(CPE)}$: la contraseña del CPE marcada en una etiqueta, tarjeta de claves, especificación u otros datos del CPE, la cual es nula si el CPE no es un dispositivo de seguridad.

Estado: sus valores se describen a continuación.

"1"-solicitado: el usuario ha solicitado previamente el servicio de seguridad pero no lo ha registrado en línea; un valor inicial de un nuevo registro;

"2"-bajo solicitud: el usuario ha registrado en línea el servicio de seguridad, no indica si el dispositivo se encuentra

en línea en este momento;

"3"-baja: el usuario ha cancelado el servicio de seguridad del dispositivo. Dicho registro se puede transferir a otra lista y almacenarse para una referencia futura.

Última vez que se ha registrado: la última vez que el SMM registra el servicio de seguridad para el CPE, la cual se anota cuando el SMS acepta el registro.

4) El SMS acepta el registro del CPE del servicio de seguridad.

La NID se obtiene siempre y cuando el usuario haya solicitado el servicio de seguridad de red. Independientemente de si el usuario ha solicitado o no previamente el servicio de seguridad para el CPE, se puede aceptar el registro del servicio de seguridad del CPE. Más tarde se describirá el proceso detallado para que el CPE registre el servicio de seguridad.

5) El SMS genera registros de todos los eventos de registro del SMM incluyendo el registro del SMM del servicio de seguridad de red y el registro de un servicio de seguridad del dispositivo para el CPE, y almacena los registros.

2. SMM dentro de la red doméstica

Dentro de la red doméstica del usuario existe un SMM, el cual puede ser parte de la HGW o ser un dispositivo independiente. El SMM tiene las siguientes funciones principales.

1) El SMM registra y gestiona las NTID de todos los CPE en la red doméstica y otra información auxiliar. Para gestionar los CPE el SMM utiliza una lista de CPE (CPE-L), tal y como se muestra en la Tabla 3.

Tabla 3 CPE-L utilizada por el SMM

$NTID_{(CPE)}$	Dirección IP	Estado	Otra información

$NTID_{(CPE)}$: la NTID del CPE.

Dirección IP: información de la dirección IP cuando el CPE se encuentra en línea, la cual no está definida si el CPE se encuentra desconectado.

Estado: indica el estado del CPE y tiene los siguientes valores posibles:

"0"-desconectado;

"1"-en línea.

2) El SMM registra el servicio de seguridad para el CPE con el SMS en la red doméstica. Los procesos de registro se describirán en el método de registro del servicio de seguridad del CPE.

3) Cuando el SMM no se puede conectar al SMS, el SMM puede proporcionar el servicio de seguridad para el CPE en la red y almacena temporalmente los registros en línea del CPE en una lista CPE-L-UR (UR significa sin registrar con el SMS). Más tarde se describe el método del SMM para proporcionar el servicio de seguridad. La CPE-L-UR puede tener el formato de la Tabla 4

Tabla 4 Formato de la lista de registros en línea de CPE no certificados por el SMS (CPE-L-UR)

$NTID_{(CPE)}$	Tiempo en línea	Contraseña

$NTID_{(CPE)}$: la NTID del CPE.

Tiempo en línea: el instante en el que el CPE se anuncia al encenderse, incluyendo año, mes, día, hora, minuto y segundo.

Contraseña: la contraseña del CPE (cuando el CPE es un dispositivo de seguridad), la cual es nula si el CPE no es un dispositivo de seguridad y puede ser nula si el CPE es un dispositivo de seguridad registrado. La contraseña es útil únicamente cuando el dispositivo de seguridad accede por primera vez a la red del usuario mediante la confirmación manual, y se adapta para notificar esta información al SMS. Después, la información es almacenada por el SMS.

4) Cuando el SMM se puede conectar al SMS, si existe un registro sin registrar en el SMS de un CPE en línea, el SMM lo envía al SMS para una verificación de seguridad de histéresis.

5) El SMM proporciona un servicio de certificación de seguridad para el acceso a un dispositivo en la red.

6) El SMM almacena eventos de acceso al dispositivo en la red.

3. CPE

Para implementar el servicio de seguridad descrito en los modos de realización de la presente invención, el CPE debe tener las funciones siguientes.

1) El CPE debería ser capaz de anunciarse a sí mismo cuando acceda a la red e incluir su propia NTID en el mensaje de anuncio, o devolver la NTID cuando el SMM consulta la NTID después de recibir el mensaje de anuncio. El menaje de anuncio puede ser un mensaje de multidifusión o un mensaje enviado punto a punto. De este modo, el SMM de la red puede obtener la NTID del CPE cuando sepa que el CPE se encuentra en línea, y registrar el servicio de seguridad con el SMS para el CPE. En un modo de realización, se toma como ejemplo que el CPE incluye la NTID en el mensaje de anuncio. El dispositivo de seguridad debería, además, identificarse en el anuncio como un dispositivo de seguridad, y el SMM también incluirá en el mensaje de registro una identificación que indique que el CPE es un dispositivo de seguridad. El mensaje de anuncio del CPE es un mensaje de multidifusión, de modo que el CPE no necesita conocer desde el principio la dirección del SMM. En cada inicio, el SMM indica al CPE su información de dirección sin almacenar la información en un almacenamiento permanente.

2) Mediante el SMM, el CPE puede verificar si, cuando recibe un acceso a sí mismo, lo hace un dispositivo legítimo. Se describirán los procesos detallados en un método de control de acceso de seguridad. Cuando el CPE no puede obtener la dirección del SMM, el propio CPE determinará si otro dispositivo puede acceder al CPE, lo cual no está limitado en la presente invención.

3) El CPE puede enviarse a sí mismo un evento de acceso para que el SMM lo almacene.

4. ACS

El servidor de configuración automática (ACS) es también un servidor en la WAN adaptado para implementar una configuración automática del CPE. En un modo de realización de la presente invención, es necesario que un archivo de configuración enviado desde el ACS al SSM contenga la información de dirección del SMS y un certificado. De este modo, el SSM obtiene la dirección del SMS y una clave que permite una comunicación secreta con el SMS cuando obtiene la configuración automática.

A continuación se describen uno a uno los métodos de proceso relevantes en el modo de realización de la presente invención.

I. Método de registro del servicio de seguridad de red

1) Al iniciarse, si el SMM no conoce una dirección del SMS, el SMM envía al ACS una petición para solicitar una configuración del ACS; si el SMM ya conoce la dirección del SMS, el flujo continúa en el Paso 3.

2) El ACS envía, de cierto modo, al SMM la información de dirección del SMS y un certificado, por ejemplo, mediante un archivo de configuración o accediendo a un nodo de datos del SMM.

3) Después de obtener la dirección del SMS, el SMM envía al SMS un mensaje de registro del servicio de seguridad de red que incluye su propia NTID, una NID y una clave pública de cifrado. Cuando el SMM no ha obtenido la NID, la NID del mensaje de registro es nula. La comunicación entre el SMS y el SMM tiene que ser segura. Por lo tanto, el SMM tiene que obtener una clave pública desde el SMS, utilizar la clave pública del SMS para cifrar la información enviada por él mismo, e incluir en el mensaje de registro su propia clave pública de cifrado. Después, el SMS puede utilizar la clave pública del SMM para cifrar un mensaje cuando envíe el mensaje al SMM. El SMM debería obtener la clave pública del SMS antes de enviar el mensaje de registro. El SMM puede obtener directamente la clave pública del SMS o desde un CA del SMS, el cual no está definido en la presente invención.

4) Después de recibir el mensaje de registro del servicio de seguridad de red, el SMS busca la NTID del SMM en la lista NID-L como se muestra en la FIG. 4.

4.1) Si el SMS no encuentra la NTID o el SMS encuentra la NTID pero el valor de la identificación de aplicación en el registro es “3” (lo que indica que se ha eliminado la NTID), el SMS la ignora y no necesita enviar un mensaje de respuesta.

4.2) Si el SMS encuentra la NTID y la NID enviada por el SMM es nula (en este momento, la identificación de aplicación en el registro debería ser “1”), el SMS almacena la información de la clave pública del SMM enviada por el SMM, cambia a “2” la identificación de aplicación, responde con un mensaje de registro satisfactorio, y se incluye la NID del registro en el mensaje de registro satisfactorio. El mensaje de respuesta se cifra con la clave pública del SMM (lo cual es igual más abajo y no se repetirá).

4.3) Si el SMS encuentra la NTID pero la NID enviada por el SMM no es nula y no coincide con la NID del registro, el

SMS activa una alarma y responde con un error o no responde (dicho caso no debería ocurrir).

4.4) Si el SMS encuentra la NTID y la NID enviada por el SMM no es nula y coincide con la NID del registro (en este momento la identificación de aplicación en el registro debería ser “2”), el SMS responde con el mensaje de registro satisfactorio.

5) El SMM recibe el mensaje de respuesta del SMS.

5.1) Si el mensaje es de registro satisfactorio, indica que el servicio de seguridad de red se ha registrado con éxito. Si el registro es el primer registro del SMM, se extrae la NID del mensaje de respuesta y se almacena.

5.2) Si el mensaje de respuesta es una información de error, indica que el servicio de seguridad de red no se ha registrado satisfactoriamente.

II. Método de registro del servicio de seguridad del CPE

1) Después de acceder a la red, el CPE, por ejemplo, anuncia su existencia con un mensaje de multidifusión e incluye su propia NTID en el mensaje de anuncio. Si el CPE es un dispositivo de seguridad con acceso limitado a él mismo, también se debería incluir una identificación que indique que el CPE es un dispositivo de seguridad.

2) Después de recibir el mensaje de anuncio del CPE, el SMM envía al SMS un mensaje de registro del servicio de seguridad del dispositivo CPE que incluye una NID, una NTID del CPE, y una identificación que indica si el CPE es un dispositivo de seguridad. El mensaje se cifra con una clave pública del SMS (todos los mensajes interactivos siguientes también se cifran y no se volverá a repetir).

3) Después de enviar el mensaje de registro del CPE, el SMM busca la NTID del CPE en la CPE-L.

3.1) Si este CPE existe en la CPE-L, el SMM añade el CPE a la lista CPE-L-UR (ver la Tabla 4) y envía al CPE la dirección del SMM.

3.2) Si este CPE no existe en la CPE-L, el SMM añade el CPE a la lista CPE-L-UC (UC significa sin confirmar por el usuario) de CPE sin confirmar, indica si el CPE es un dispositivo de seguridad o no es un dispositivo de seguridad y, a continuación, espera una confirmación manual o un resultado del registro del SMS. En la Tabla 5 se muestra el formato de la CPE-L-UC.

Tabla 5 Formato de la lista de registros de CPE sin confirmar CPE-L-UC

$NTID_{(CPE)}$	Etiqueta de seguridad

$NTID_{(CPE)}$: la NTID del CPE.

Etiqueta de seguridad: a continuación se describen sus valores:

0- dispositivo que no es de seguridad;

1- dispositivo de seguridad.

4) El usuario confirma el dispositivo de seguridad de forma manual.

4.1) El SMM muestra al usuario la NITD o una identificación simple del terminal (STID) del CPE en la CPE-L-UC. La STID son los primeros 4 ó 5 caracteres de la información resumida de la NTID obtenida utilizando cierto algoritmo de resumen y se codifica con el BASE64. La STID no puede identificar un dispositivo de forma unívoca, pero es difícil que se repita en un hogar y se puede leer fácilmente debido a su brevedad.

4.2) Para obtener la NTID o la STID del dispositivo, el usuario consulta la etiqueta, la tarjeta de claves, la especificación y otros datos del CPE, consulta la información que se muestra en el SMM, selecciona el CPE deseado y confirma el CPE. Para un dispositivo de seguridad, es necesario introducir una contraseña del CPE en el momento de la confirmación. Igualmente, la contraseña se obtiene de la tarjeta, la etiqueta, la especificación y otros datos del dispositivo. Si el CPE no es un dispositivo de seguridad, el flujo continúa en el Paso 4.6 después de la confirmación.

4.3) Si el CPE es una confirmación del dispositivo de seguridad, el SMM cifra la contraseña de entrada con una clave pública del CPE y se la envía al CPE. El CPE de seguridad tiene un certificado de seguridad inicial y se puede leer directamente su clave pública de cifrado.

4.4) El CPE recibe desde el SMM la información de la contraseña, verifica que la información de la contraseña es correcta y devuelve al SMM un resultado de la verificación que puede ser Positiva o Negativa.

4.5) El SMM recibe el resultado de la verificación del CPE. Si la verificación ha fallado el flujo vuelve al paso 4.2; en caso contrario, el flujo continúa en el paso 4.6.

4.6) El SMM añade la información apropiada del CPE a las listas CPE-L-UR y CPE-L, elimina la información apropiada del CPE de la lista CPE-L-UC y, a continuación, envía al CPE la dirección del SMM. Después, el SMM espera un mensaje de respuesta del SMS y el flujo continúa en el Paso 6.

5) Después del Paso 2, después de recibir el mensaje de registro del servicio de seguridad del dispositivo, el SMS busca en la NID-L.

5.1) Si la NID especificada no existe en la NID-L, el SMS la ignora y no devuelve ninguna respuesta.

5.2) Si la NID especificada existe en la NID-L, el SMS busca en la NTID-L en función de la NTID y la NID.

5.2.1) Si en la NTID-L se encuentran registros que encajan perfectamente con las NTID y NID especificadas, ello indica que el dispositivo ha solicitado o ha registrado el servicio de seguridad, y el SMS responde con un mensaje de registro satisfactorio. Si el mensaje de registro indica que el CPE es un dispositivo de seguridad, el SMS adjunta al mensaje de respuesta la contraseña del dispositivo que se encuentra registrada en la NTID-L. Si en ese momento la identificación del estado en el registro es “1”, el estado se cambia a “2”.

5.2.2) Si el registro NTID especificada se encuentra en la NTID-L pero la NID del registro es distinta de la NID del mensaje de registro, el SMS activa una alarma y responde al SMM que el CPE se ha registrado en otra red.

5.2.3) Si en la NTID-L no existe ningún registro con la NTID especificada, ello indica que el usuario no ha solicitado previamente el servicio de seguridad para este dispositivo, y el SMS envía un mensaje que debería incluir la NTID para averiguar si el SMM lleva a cabo el registro.

6) El SMM recibe el mensaje de respuesta del SMS al mensaje de registro.

6.1) El mensaje de respuesta de registro es “registro satisfactorio”.

6.1.1) Si el SMM está esperando que el usuario confirme el CPE, si el CPE no es un dispositivo de seguridad, el flujo continúa directamente en el paso 6.1.1.4; en caso contrario, se llevan a cabo los siguientes pasos.

6.1.1.1) El SMM envía al CPE la contraseña transmitida desde el SMS.

6.1.1.2) El CPE verifica si la contraseña es correcta y devuelve al SMM un resultado de la verificación (positiva o negativa).

6.1.1.3) El SMM recibe el resultado de la verificación del CPE. Si falla la verificación, el SMM devuelve al SMS una información de error que indica que ha ocurrido un error cuando se ha solicitado previamente el servicio de seguridad y entretanto espera la confirmación manual del usuario, i.e., el flujo vuelve al Paso 4.

6.1.1.4) El SMM añade el CPE a la lista CPE-L, envía al CPE la dirección del SMM y deja de esperar la confirmación, i.e. elimina de la CPE-L-UC la información apropiada de este CPE.

6.1.2) Si el usuario ha realizado la confirmación manual, en este momento, el CPE se ha eliminado de la lista CPE-L-UC y se ha añadido simultáneamente a la lista CPE-L-UR y a la lista CPE-L, y el CPE ha sido informado de la dirección del SMM, la información apropiada del CPE se elimina de la CPE-L-UR, en cuyo momento se ignora la contraseña enviada desde el SMS.

6.1.3) O el CPE se ha registrado antes y ya existía en la lista CPE-L y también aparece en la CPE-L-UR mediante el Paso 3.1, y el CPE ha sido informado de la dirección del SMM. A continuación se elimina de la CPE-L-UR la información apropiada del CPE.

6.2) El mensaje de respuesta de registro es “el CPE se ha registrado en otra red”. El SMM avisa al usuario que no se puede utilizar el dispositivo, o no da ningún aviso y elimina la información apropiada del CPE en todas las listas.

6.3) El mensaje de respuesta de registro es “solicitar si realiza el registro”, lo cual indica que el CPE no tiene que solicitar previamente al SMS el servicio de seguridad.

6.3.1) Si el SMM está esperando la confirmación del usuario, el SMM espera a que el usuario complete la información (ver Paso 4), o la confirmación se puede haber completado.

6.3.2) Después de completarse la confirmación manual, el SMM envía al SMS un mensaje de registro positivo y añade el CPE a la lista CPE-L, pero no elimina la información relevante del CPE de la lista CPE-L-UR. Si el CPE es un dispositivo de seguridad, el mensaje de registro positivo incluye la contraseña del CPE.

7) Después del Paso 6, el SMM puede enviar al SMS un mensaje indicando que el registro es correcto o que la contraseña es errónea o que no se ha enviado ningún mensaje.

7.1) El SMS recibe el mensaje indicando que la contraseña del CPE es errónea, y el mensaje incluye la NID y la NTID del CPE. El SMS realiza una solicitud de intervención manual y de corrección de la información y, entretanto, cambia el estado de registro a “1”.

7.2) El SMS recibe el mensaje de “registro positivo” incluyendo la NID, la NTID del CPE, y la contraseña (la cual es nula si no es un dispositivo de seguridad). El SMS busca primero en la NID-L.

7.2.1) Si en la NID-L no existe la NID especificada, el SMS la ignora y no devuelve ninguna respuesta.

7.2.2) Si en la NID-L existe la NID especificada, el SMS busca en la NTID-L en función de la NTID y la NID.

7.2.2.1) Si en la NTID-L se encuentran registros que se corresponden totalmente con la NTID y la NID especificadas, el SMS responde con un mensaje de registro satisfactorio, registra en la NTID-L la contraseña del CPE (que es nula si no es un dispositivo de seguridad) recibida desde el SMM y, entretanto, cambia a “2” la identificación en el registro.

7.2.2.2) Si en la NTID-L se encuentra el registro NTID especificado pero la NID registrada es distinta de la NID especificada, el SMS envía una alarma y responde al SMM que el CPE se ha registrado en otra red.

7.2.2.3) Si en la NTID-L no existe registro de la NTID especificada, el SMS añade directamente el registro incluyendo la contraseña registrada, y responde con el mensaje de registro satisfactorio.

8) Para los Pasos 5 y 7 en los que el SMM recibe del SMS el mensaje de “registro satisfactorio”, el método incluye, además, los siguientes pasos.

8.1) Para el mensaje de “registro satisfactorio” del Paso 7.2.2.3, el SMM elimina de la lista CPE-L-UR la información apropiada del CPE.

8.2) El SMM puede necesitar devolver de nuevo al SMS un mensaje de confirmación y terminar la sesión después.

De acuerdo con la descripción anterior, se pueden describir más abajo varios casos para que el CPE solicite el servicio de seguridad mediante los diagramas interactivos correspondientes.

Si el usuario solicita previamente al SSP el servicio de seguridad para un dispositivo que no es de seguridad, los procesos para que el CPE registre por primera vez el servicio de seguridad con el SMS se muestran en la FIG. 5. El número de paso marcado antes de cada paso en la figura se corresponde con el paso descrito en el punto II “Método de registro del servicio de seguridad del CPE”, el cual es el mismo para las FIG. 6 a 15.

Si el usuario solicita previamente al SSP el servicio de seguridad para un dispositivo de seguridad, los procesos para que el CPE registre por primera vez el servicio de seguridad con el SMS se muestran en la FIG. 6.

Si el dispositivo que no es de seguridad no solicita previamente el servicio de seguridad, el dispositivo puede ser simplemente confirmado después del acceso siempre que el usuario haya solicitado el servicio de seguridad para su red doméstica, tal y como se muestra en la FIG. 7.

Si el dispositivo de seguridad no solicita previamente el servicio de seguridad, el dispositivo puede obtener el servicio de seguridad del SMS mediante una confirmación manual después del acceso siempre que el usuario haya solicitado el servicio de seguridad para su red doméstica, tal y como se muestra en la FIG. 8.

En la FIG. 9 se muestra un proceso para volver a registrar un CPE que ha registrado satisfactoriamente el servicio de seguridad.

Si un CPE que ha registrado satisfactoriamente un servicio de seguridad en otra red o para el que se solicita previamente el servicio de seguridad se transfiere a una red que no puede utilizar, el SMS puede averiguar este hecho y proporcionar una alarma, tal y como se muestra en la FIG. 10.

III. Servicio de seguridad sin SMS.

Este mecanismo asegura que la red doméstica del usuario puede seguir funcionando normalmente cuando el SMM no puede acceder al SMS. El mecanismo se materializa de modo que, cuando el dispositivo se registra por primera vez, no es necesario esperar una respuesta del SMS, y el CPE puede obtener el servicio de seguridad del SMM a través de la confirmación manual del usuario tal y como se muestra en el Paso 4 del punto II mencionado anteriormente.

En el punto II mencionado anteriormente, si el SMM no puede acceder al SMS, puede utilizarse el proceso de

confirmación manual. En ese momento, el SMM almacena toda la información relevante del CPE sin registrar con el SMS, la cual se almacena en la CPE-L-UR.

Cuando el SMM puede acceder al SMS, el SMM envía información como, por ejemplo, la NTID del CPE de la CPE-L-UR a la SMS para un registro de histéresis. El método es el mismo que el del punto II mencionado anteriormente, pero es de histéresis en el tiempo. El SMS puede descubrir dispositivos ilegítimos a partir de dicho comportamiento de registro del servicio de seguridad de histéresis, la cual es la función principal del SMS en dicho caso. Sin embargo, el usuario no puede modificar la información de la CPE-L-UR en el SMM.

IV. Método de control de acceso de seguridad.

1. Acceso entre dispositivos dentro de una red doméstica.

Cuando un dispositivo accede a otro dispositivo dentro de la red doméstica, el dispositivo que accede puede enviar en primer lugar una solicitud de acceso que incluya su propia NTID, o iniciar directamente el proceso para establecer una conexión del modo estándar.

Cuando recibe la solicitud para establecer la conexión, el dispositivo accedido consulta a la parte que accede la NTID de la parte que accede, si no ha recibido antes la NTID enviada de forma activa por la parte que accede. Cuando se recibe dicha consulta, la parte que accede debe enviar su propia NTID a la parte accedida.

Mediante el siguiente método la parte accedida consulta al SMM si la NTID de la parte que accede es legítima. El dispositivo accedido utiliza una interfaz del SMM. El SMM comprueba la CPE-L. Si la NTID del dispositivo que accede se encuentra en la CPE-L, el dispositivo se considera legítimo; en caso contrario, el dispositivo es ilegal.

En las FIG. 11 y 12 se muestra el proceso para establecer la conexión. La FIG. 11 muestra un flujo de proceso en el que se incluye la NTID cuando se solicita el establecimiento de la conexión. La FIG. 12 muestra un flujo de proceso en el que no se incluye la NTID cuando se solicita el establecimiento de la conexión.

Tal y como se muestra en la FIG. 13, el dispositivo accedido puede autentificar al dispositivo que accede. El dispositivo almacena, por sí mismo, una lista de autoridades de acceso que incluye las NTID y las claves de certificación de los dispositivos autorizados a acceder al dispositivo. Cuando el dispositivo accedido encuentra que la parte que accede no existe en la lista o falla la autentificación (i.e., falla la comprobación de la contraseña de la FIG. 13), el dispositivo accedido informa de este hecho al SMM. El usuario puede determinar mediante el SMM de forma manual si el dispositivo que accede está realmente autorizado a acceder al dispositivo accedido. Si el SMM confirma que el dispositivo que accede está realmente autorizado a acceder al dispositivo accedido, el SMM lee una contraseña de la parte accedida y reenvía la contraseña a la parte que accede. La comunicación entre el SMM y la parte accedida se transmite de forma secreta. La comunicación entre el SMM y la parte que accede también se transmite de forma secreta. Si la parte que accede no tiene certificado, el SMM le expide uno; en caso contrario, se utiliza el certificado original.

El CPE puede obtener un certificado del SMM mediante el proceso siguiente. El CPE genera de forma aleatoria una clave equivalente, cifra la clave equivalente con una clave pública del SMM y transmite al SMM la clave cifrada. El SMM utiliza la clave equivalente del CPE para cifrar un certificado y envía el certificado al CPE.

El certificado enviado por el SMM al CPE lo puede generar el propio SMM o se puede obtener del SMS. El SMS genera un certificado y lo envía al SMM a petición del SMM.

En la FIG. 13 se muestra el proceso para que un CPE autentifique a otro CPE.

2. Acceso al exterior de un dispositivo dentro de la red doméstica

Cuando intenta acceder al exterior, un dispositivo dentro de la red doméstica debe realizar el acceso mediante una HGW. La HGW puede verificar la validez del dispositivo mediante el mismo método de más arriba y limitar la autoridad del dispositivo con la misma lista de autoridades de acceso, de modo que se permite que el dispositivo legítimo confirmado pase a través de la pasarela y un dispositivo legítimo sin confirmar no puede pasar a través de la misma, lo que es equivalente a una lista de filtrado que no está editada previamente pero se establece de forma inmediata cuando el dispositivo accede a la red externa.

3. Acceso de un dispositivo externo a un dispositivo dentro de la red doméstica

El mecanismo de control de acceso mencionado anteriormente para dispositivos dentro de la red doméstica se puede aplicar igualmente para el acceso de un dispositivo de fuera de la red a un dispositivo dentro de la red doméstica.

El propio dispositivo nómada del usuario puede solicitar previamente al SMS un servicio de seguridad o llevar a cabo un registro de servicio de seguridad confirmado de forma manual dentro de la red doméstica y estar realmente

registrado en el SMS. Cuando el dispositivo nómada accede a la red desde un punto de acceso público, un mensaje de anuncio suyo no funciona, porque no existe un SMM en el entorno del dispositivo nómada. Sin embargo, esto no afecta al acceso del dispositivo nómada a Internet, debido a que el dispositivo del usuario no se comunica directamente con el SMM.

Cuando el dispositivo nómada accede a cierto CPE dentro de la red doméstica del usuario, el CPE solicita la NTID del dispositivo nómada y, después, consulta al SMM. El proceso posterior es el mismo que el del acceso dentro de la red doméstica.

V. Cancelación de registro del dispositivo

Cuando se transfiere el dispositivo propio a otras personas, el usuario debería cancelar el registro del servicio de seguridad de este dispositivo en el SMS. De modo que el cesionario puede solicitar un servicio de seguridad para el dispositivo para evitar la alarma del SMS cuando el dispositivo acceda a otra red. El proceso de cancelación de registro se muestra en la FIG. 14. El usuario envía al SMS una solicitud para cancelar el servicio de seguridad con una NTID de un dispositivo cuyo registro se va a cancelar. El SMS encuentra un registro correspondiente en una NTID-L y cambia su estado a “3” y, después, devuelve al usuario un mensaje de cancelación satisfactoria de registro. Entretanto, el SMS envía al SMM un mensaje para cancelar el registro del servicio de seguridad con la NTID del dispositivo cuyo registro se va a cancelar. El SMM encuentra el registro correspondiente en una CPE-L y lo elimina.

El usuario también puede utilizar el SMM dentro de la red doméstica para eliminar un dispositivo. Después, el SMM envía al SMS una solicitud para cancelar el registro del servicio de seguridad con la NTID del dispositivo cuyo registro se va a cancelar. El SMS encuentra el registro correspondiente en la lista de registro NTID-L y cambia su estado a “3” y, después devuelve al usuario un mensaje de cancelación satisfactoria de registro.

VI. Transferencia de dispositivo en línea

Tal y como se muestra en la FIG. 15, el usuario no puede utilizar el método de cancelación de registro mencionado anteriormente cuando transfiere su dispositivo. Después de que un usuario que recibe el dispositivo hace que el dispositivo acceda a su red, el SMS puede enviar al SMM un mensaje que incluye información sobre un nombre de usuario y/o dirección, etc. del nuevo usuario y una NTID del dispositivo transferido en la red doméstica del usuario original del dispositivo en el paso de alarma. El SMM del usuario original del dispositivo muestra “Su dispositivo xxxx aparece en la casa de xxx cuya dirección es xxxxx, ¿lo confirma?” y el usuario original únicamente tiene que seleccionar “Sí”. Después de recibir el mensaje de confirmación del usuario original, el SMS cambia a “3” el estado del registro original en la lista NTID-L y genera automáticamente nuevos registros.

Como se puede observar a partir de los modos de realización preferidos mencionados anteriormente, los modos de realización de la presente invención tienen los siguientes efectos beneficiosos.

(1) El proceso de solicitud previa únicamente requiere que el usuario proporcione información apropiada en lugar de entender problemas técnicos.

(2) Los modos de realización de la presente invención son compatibles con el mecanismo UPnP o una confirmación de seguridad manual parecida. El usuario selecciona el uso de la solicitud previa o la confirmación manual por él mismo de acuerdo con su propia condición.

(3) La seguridad de acceso es más robusta que la del mecanismo de seguridad del UPnP. Todos los dispositivos accedidos pueden verificar la validez de los dispositivos que acceden a ellos.

(4) Debido a que el dispositivo está registrado con el SMS, un dispositivo será descubierto por el SMS si se transfiere ilegalmente a otra red. Siempre que el proveedor de la red de acceso fuerce a que la red doméstica del usuario disponga de dicho SMM que se pueda verificar (por ejemplo, el SMM es un módulo obligatorio de la HGW), se puede conseguir el efecto de este ítem.

REIVINDICACIONES

1. Un método de gestión de la seguridad de una red doméstica, que comprende:

enviar, por parte de un módulo de gestión de la seguridad, SMM, un mensaje de registro de la red doméstica a un servidor de gestión de la seguridad, SMS; en donde el mensaje de registro de la red doméstica comprende, al menos, una identificación de terminal de red, NTID, de un dispositivo que tiene el SMM, la NTID es capaz de identificar un dispositivo de forma unívoca, el SMM está dentro de la red doméstica, y el SMM se comunica con el SMS mediante una pasarela doméstica, HGW, dentro de la red doméstica;

obtener del dispositivo de usuario, por parte del SMM, una NTID de un dispositivo de usuario dentro de la red doméstica; y

enviar al SMS, por parte del SMM, un mensaje de registro del dispositivo de usuario; en donde, el mensaje de registro del dispositivo de usuario comprende, al menos, la NTID del dispositivo de usuario y una identificación de red, NID, de la red doméstica, y la NID es capaz de identificar la red doméstica de forma unívoca;

en donde, el SMS está adaptado para determinar si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario.

2. El método de acuerdo con la reivindicación 1, en donde el SMS está adaptado, además, para

aceptar el registro de la red doméstica si la NTID del SMM se registra de forma válida.

3. El método de acuerdo con la reivindicación 1, en donde el SMS asigna de forma automática la NID, o es designada por un usuario, o utiliza cualquiera de la información que comprende una NTID de un dispositivo de la HGW o del dispositivo que tiene el SMM, una cuenta de acceso a una red de área amplia, WAN, un nombre de dominio de Internet o una dirección de IP fija, y un número de teléfono del domicilio del usuario.

4. El método de acuerdo con la reivindicación 1, en donde el SMS se adapta, además, para

aceptar el registro del dispositivo de usuario y enviar al SMM un mensaje de registro satisfactorio si la NID de la red doméstica y la NTID del dispositivo de usuario se registran correspondientemente en un registro; y el método comprende, además

añadir la NTID del dispositivo de usuario a una lista de registros del SMM de acuerdo con el mensaje de registro satisfactorio.

5. El método de acuerdo con la reivindicación 4, en donde el mensaje de registro satisfactorio comprende una contraseña del dispositivo de usuario si el dispositivo de usuario es un dispositivo de seguridad; y el método comprende, además:

enviar al dispositivo de usuario, por parte del SMM, la contraseña del dispositivo de usuario, en donde el dispositivo de usuario está adaptado para verificar si la contraseña del dispositivo de usuario es correcta y enviar al SMM un resultado de la verificación;

en donde la incorporación de la NTID del dispositivo de usuario en una lista de registros del SMM de acuerdo con el mensaje de registro satisfactorio consiste en

incorporar la NTID del dispositivo de usuario a la lista de registros del SMM, y registrar la contraseña del dispositivo de usuario si el resultado de la verificación es positivo.

6. El método de acuerdo con la reivindicación 1 ó 4, en donde el SMS está adaptado, además, para enviar al SMM un mensaje de consulta si la NID de la red doméstica está registrada y la NTID del dispositivo de usuario no está registrada de forma correspondiente en el SMS, y el método comprende, además

mostrar a un usuario, por parte del SMM, información de la NTID del dispositivo de usuario de acuerdo con el mensaje de consulta;

recibir, por parte del SMM, un mensaje de confirmación enviado por el usuario de acuerdo con la información de la NTID;

incorporar la NTID del dispositivo de usuario a una lista de registros del SMM de acuerdo con el mensaje de confirmación; y

enviar al SMS, por parte del SMM, un mensaje de registro válido de acuerdo con el mensaje de confirmación;

en donde el SMS está adaptado, además, para registrar la NTID del dispositivo de usuario correspondientemente

con la NID de la red doméstica, y responder al SMM con un mensaje de registro satisfactorio como respuesta a la recepción del mensaje de registro válido.

7. El método de acuerdo con la reivindicación 1 ó 4 ó 6, en donde el SMS está adaptado, además, para enviar al SMM un mensaje de consulta si la NID de la red doméstica está registrada y la NTID del dispositivo de usuario no está registrada correspondientemente en el SMS, y el método comprende, además

solicitar a un usuario, por parte del SMM, que confirme la información de la NTID del dispositivo de usuario como respuesta a la recepción del mensaje de consulta;

recibir, por parte del SMM, un mensaje de confirmación que comprende una contraseña del dispositivo de usuario enviado por el usuario de acuerdo con la información de la NTID;

enviar al dispositivo de usuario, por parte del SMM, la contraseña a verificar;

recibir del dispositivo de usuario un resultado de la verificación;

incorporar la NTID del dispositivo de usuario a una lista de registros del SMM si el resultado de la verificación es positivo; y

enviar al SMS, por parte del SMM, un mensaje de registro válido de acuerdo con el mensaje de confirmación;

en donde el SMS está adaptado, además, para registrar la NTID del dispositivo de usuario correspondientemente con la NID de la red doméstica, y responder al SMM con un mensaje de registro satisfactorio como respuesta a la recepción del mensaje de registro válido.

8. El método de acuerdo con cualquiera de las reivindicaciones 1, 3, 4, 6 y 7, en donde cuando el SMM no puede acceder al SMS, después de que el SMM obtenga la NTID del dispositivo de usuario, el método comprende, además:

solicitar a un usuario, por parte del SMM, que introduzca una contraseña requerida por el dispositivo de usuario para confirmar información de la NTID del dispositivo de usuario;

recibir la contraseña introducida por el usuario, y enviar al dispositivo de usuario la contraseña a verificar y recibir un resultado de la verificación; e

incorporar la NTID del dispositivo de usuario a una lista de registros del SMM si el resultado de la verificación es positivo.

9. El método de acuerdo con cualquiera de las reivindicaciones 1-8, que comprende, además:

recibir, por parte de un dispositivo accedido, una solicitud de acceso desde un dispositivo que accede; en donde el dispositivo accedido está en la red doméstica;

obtener desde el dispositivo que accede, por parte del dispositivo accedido, una NTID del dispositivo que accede después de recibir la solicitud de acceso;

enviar al SMM de la red doméstica, por parte del dispositivo accedido, la NTID del dispositivo que accede y solicitar al SMM que verifique si el dispositivo que accede es válido; en donde el SMM está adaptado para comprobar si la NTID del dispositivo que accede existe en una lista de registros del SMM, y enviar al dispositivo accedido un resultado de la comprobación; y

permitir que el dispositivo que accede establezca una conexión con el dispositivo accedido si el mensaje de comprobación indica que la NTID del dispositivo que accede existe en la lista de registros del SMM.

10. El método de acuerdo con cualquiera de las reivindicaciones 1-9, en donde cuando un dispositivo de usuario dentro de la red doméstica accede a un dispositivo fuera de la red doméstica, el método comprende:

enviar, por parte del dispositivo que accede, un mensaje de acceso al exterior de la red doméstica a través de una pasarela doméstica, HGW, de la red doméstica; en donde la HGW está adaptada para solicitar del dispositivo que accede una NTID del dispositivo que accede si el dispositivo que accede envía primero el mensaje al exterior de la red doméstica; y

enviar a la HGW, por parte del dispositivo que accede, la NTID del dispositivo que accede; en donde la HGW está adaptada, además, para enviar al SMM la NTID del dispositivo que accede y solicitar al SMM que verifique si el dispositivo que accede es válido; y el SMM está adaptado para comprobar si la NTID del dispositivo que accede existe en una lista de registros del SMM, y para enviar a la HGW una información de respuesta correspondiente; y la HGW está adaptada, además, para enviar el mensaje de acceso al exterior de la red doméstica si la información de

respuesta correspondiente indica que la NTID del dispositivo que accede existe en la lista de registros del SMM.

11. Un método de gestión de la seguridad de una red doméstica, que comprende:

obtener desde un módulo de gestión de la seguridad, SMM, por parte de un servidor de gestión de la seguridad, SMS, un mensaje de registro de la red doméstica; en donde el mensaje de registro de la red doméstica comprende, al menos, una identificación de terminal de red, NTID, de un dispositivo que tiene el SMM, la NTID es capaz de identificar un dispositivo de forma unívoca, el SMM está dentro de la red doméstica, y el SMS se comunica con el SMM mediante una pasarela doméstica, HGW, dentro de la red;

obtener desde el SMM, por parte del SMS, un mensaje de registro de un dispositivo de usuario dentro de la red doméstica; en donde el mensaje de registro del dispositivo de usuario comprende, al menos, la NTID del dispositivo de usuario y un identificación de red, NID, de la red doméstica, la NID es capaz de identificar la red doméstica de forma unívoca, y el SMM obtiene del dispositivo de usuario la NTID del dispositivo de usuario; y

determinar, por parte del SMS, si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario.

12. El método de acuerdo con la reivindicación 11, en donde la determinación, por parte del SMS, de si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario comprende:

aceptar el registro de la red doméstica si la NTID del SMM está grabada de forma válida.

13. El método de acuerdo con la reivindicación 11 ó 12, en donde la determinación, por parte del SMS, de si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario comprende:

aceptar, por parte del SMS, el registro del dispositivo de usuario y enviar al SMM un mensaje de registro satisfactorio si la NID de la red doméstica y la NTID del dispositivo de usuario están registradas correspondientemente en un registro; en donde el SMM está adaptado para incorporar la NTID del dispositivo de usuario a una lista de registros del SMM de acuerdo con el mensaje de registro satisfactorio.

14. El método de acuerdo con la reivindicación 13, en donde el mensaje de registro satisfactorio comprende una contraseña del dispositivo de usuario si el dispositivo de usuario es un dispositivo de seguridad; y el SMM está adaptado, además, para

enviar al dispositivo de usuario la contraseña del dispositivo de usuario, en donde el dispositivo de usuario está adaptado para verificar si la contraseña del dispositivo de usuario es correcta y enviar al SMM un resultado de la verificación; y

incorporar a la lista de registros del SMM la NTID del dispositivo de usuario, y registrar la contraseña del dispositivo de usuario si el resultado de la verificación es Positivo.

15. El método de acuerdo con cualquiera de las reivindicaciones 11-13, en donde la determinación, por parte del SMS de si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario comprende:

enviar un mensaje de consulta al SMM si la NID de la red doméstica está registrada y la NTID del dispositivo de usuario no está registrada correspondientemente en el SMS, en donde el SMM está adaptado, además, para mostrar a un usuario información de la NTID del dispositivo de usuario de acuerdo con el mensaje de consulta, recibir un mensaje de confirmación enviado por el usuario de acuerdo con la información de la NTID, e incorporar a una lista de registros de la SMM la NTID del dispositivo de usuario de acuerdo con el mensaje de confirmación;

recibir desde el SMM, por parte del SMS, un mensaje de registro válido de acuerdo con el mensaje de confirmación; y

registrar, por parte del SMS, la NTID del dispositivo de usuario correspondientemente con la NID de la red doméstica, y responder al SMM con un mensaje de registro satisfactorio como respuesta a la recepción del mensaje de registro válido.

16. El método de acuerdo con cualquiera de las reivindicaciones 11-13, y 15, en donde la determinación, por parte del SMS, de si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario y la NTID del SMM comprende:

enviar al SMM un mensaje de solicitud si en el SMS está registrada la NID de la red doméstica y no está registrada correspondientemente la NTID del dispositivo de usuario, en donde el SMM está adaptado para pedir a un usuario

que confirme la información de la NTID del dispositivo de usuario como respuesta a la recepción del mensaje de consulta, recibir un mensaje de confirmación que comprende una contraseña del dispositivo de usuario enviado por el usuario de acuerdo con la información de la NTID, enviar al dispositivo de usuario la contraseña a verificar, recibir un resultado de la verificación por parte del dispositivo de usuario y, si el resultado de la verificación es Positivo, incorporar la NTID del dispositivo de usuario a una lista de registros del SMM;

recibir desde el SMM, por parte del SMS, un mensaje de registro válido de acuerdo con el mensaje de confirmación; y

registrar, por parte del SMS, la NITD del dispositivo de usuario correspondientemente con la NID de la red doméstica, y responder al SMM con un mensaje de registro satisfactorio como respuesta a la recepción del mensaje de registro válido.

17. Un módulo de gestión de la seguridad, SMM, para gestión de la seguridad de una red doméstica estando dicho SMM adaptado para

enviar un mensaje de registro de la red doméstica a un servidor de gestión de la seguridad, SMS; en donde el mensaje de registro de la red doméstica comprende, al menos, una identificación de terminal de red, NTID, de un dispositivo que tiene el SMM, la NTID es capaz de identificar un dispositivo de forma unívoca, el SMM está dentro de la red doméstica, y el SMM se comunica con el SMS mediante una pasarela doméstica, HGW, dentro de la red doméstica;

obtener desde el dispositivo de usuario una NTID de un dispositivo de usuario dentro de la red doméstica; y

enviar al SMS un mensaje de registro del dispositivo de usuario; en donde el mensaje de registro del dispositivo de usuario comprende, al menos, la NTID del dispositivo de usuario y una identificación de red, NID, de la red doméstica, y la NID es capaz de identificar una red doméstica de forma unívoca;

en donde, el SMS está adaptado para determinar si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario.

18. Un servidor de gestión de la seguridad, SMS, que comprende uno o más componentes para gestión de la seguridad de una red doméstica, estando adaptado dicho SMS para

obtener de un módulo de gestión de la seguridad, SMM, un mensaje de registro de la red doméstica; en donde, el mensaje de registro de la red doméstica comprende, al menos, una identificación de terminal de red, NTID, de un dispositivo que tiene el SMM, la NTID es capaz de identificar un dispositivo de forma unívoca, el SMM está dentro de la red doméstica, y el SMS se comunica con el SMM mediante una pasarela doméstica, HGW, dentro de la red doméstica;

obtener desde el SMM un mensaje de registro de un dispositivo de usuario dentro de la red doméstica; en donde, el mensaje de registro del dispositivo de usuario comprende, al menos, la NTID del dispositivo de usuario y una identificación de red, NID, de la red doméstica, la NID es capaz de identificar una red doméstica de forma unívoca, y el SMM obtiene del dispositivo de usuario la NTID del dispositivo de usuario; y

determinar si acepta el registro del SMM de acuerdo con la NTID del SMM y el registro del dispositivo de usuario de acuerdo con la NID de la red doméstica y la NTID del dispositivo de usuario.

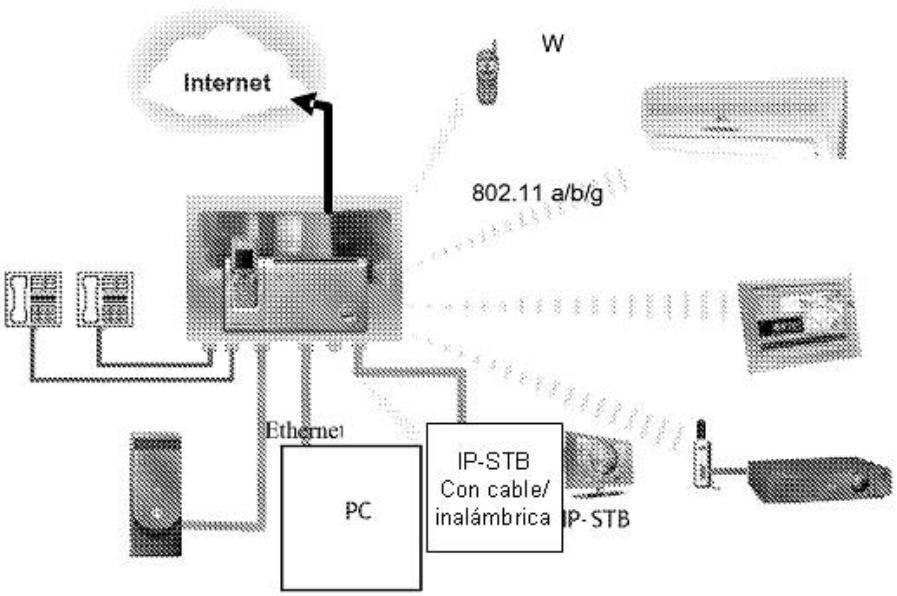
Internet
W
802.11 a/b/g
Ethernet
PC
IP-STB
Con cable/
inalámbrica
IP-STB

FIG. 1

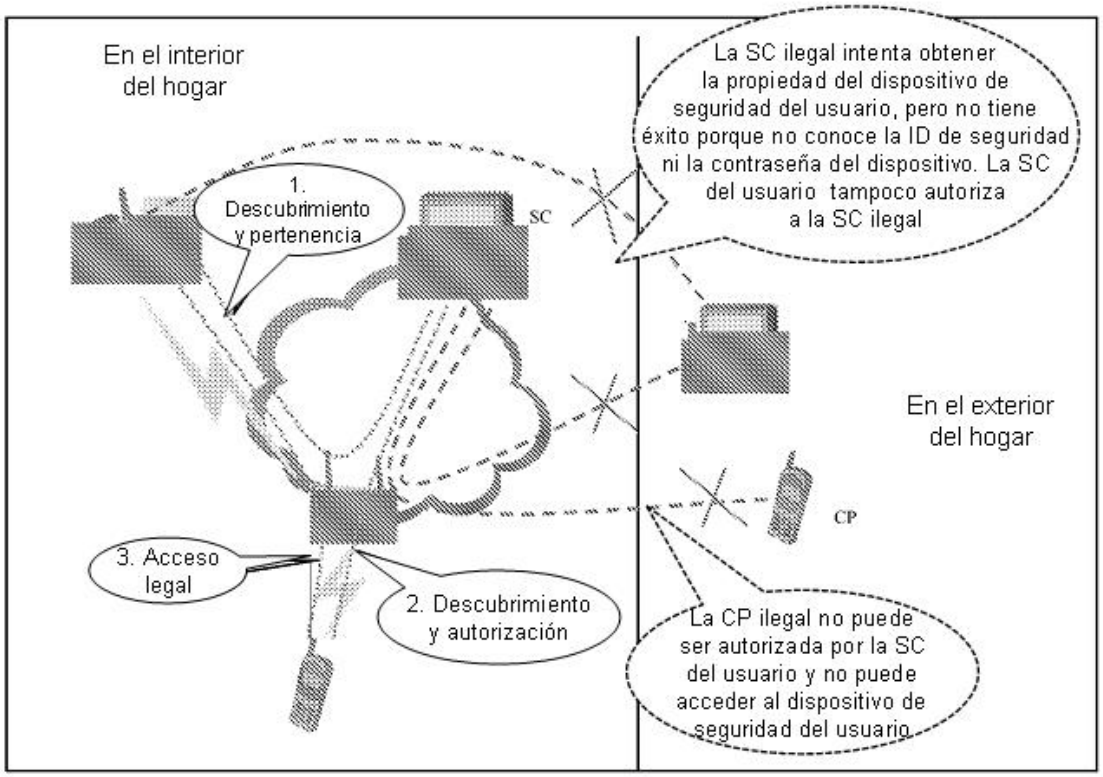
En el interior del hogar
La SC ilegal intenta obtener la propiedad del dispositivo de seguridad del usuario, pero no tiene éxito porque no conoce la ID de seguridad ni la contraseña del dispositivo. La SC del usuario tampoco autoriza a la SC ilegal
1. Descubrimiento y pertenencia
SC
En el exterior del hogar
CP
3. Acceso legal
2. Descubrimiento y autorización
La CP ilegal no puede ser autorizada por la SC del usuario y no puede acceder al dispositivo de seguridad del usuario

FIG. 2

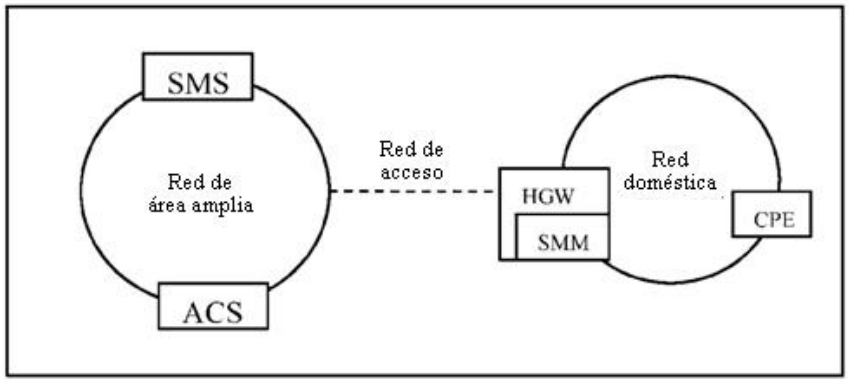
SMS
Red de área amplia
ACS
Red de acceso
HGW
SMM
Red doméstica
CPE

FIG. 3

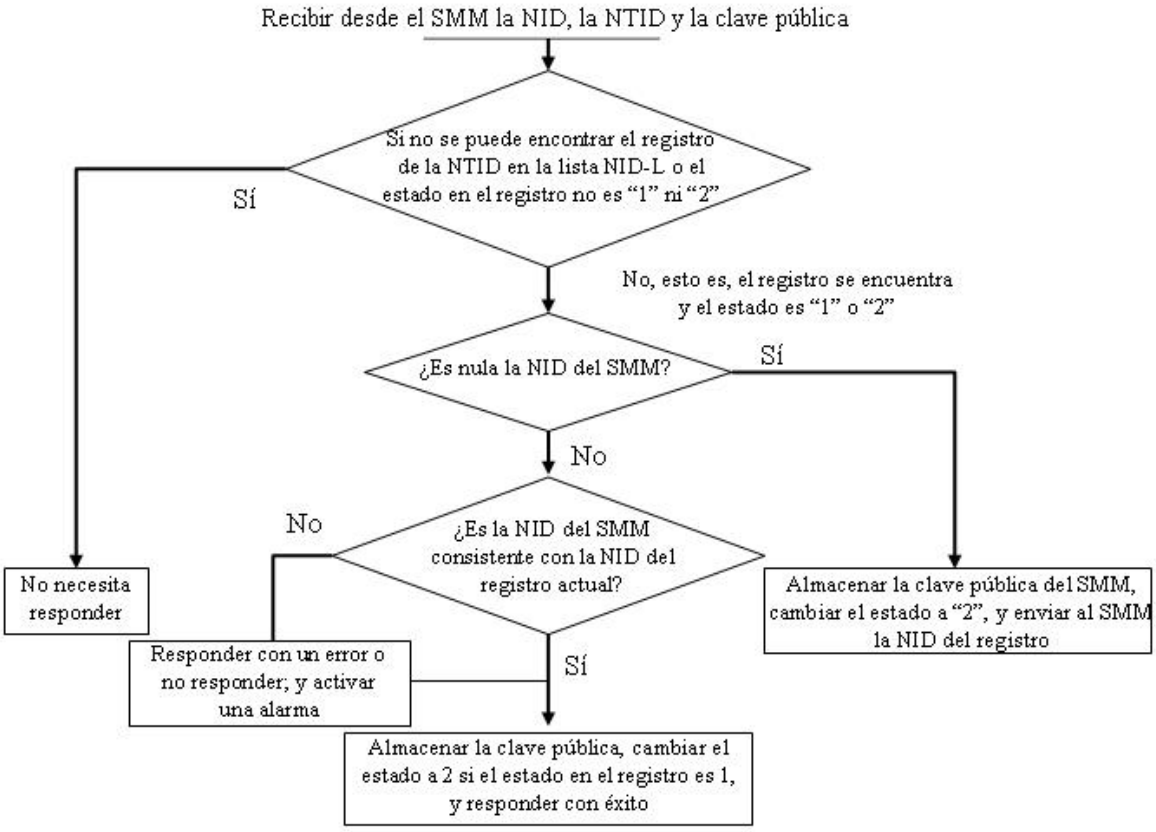
Recibir desde el SMM la NID, la NTID y la clave pública
Si no se puede encontrar el registro de la NTID en la lista NID-L o el estado en el registro no es "1" ni "2"
Sí
No, esto es, el registro se encuentra y el estado es "1" o "2"
¿Es nula la NID del SMM?
Sí
No
¿Es la NID del SMM consistente con la NID del registro actual?
No
No necesita responder
Responder con un error o no responder; y activar una alarma
Sí
Almacenar la clave pública del SMM, cambiar el estado a "2", y enviar al SMM la NID del registro
Almacenar la clave pública, cambiar el estado a 2 si el estado en el registro es 1, y responder con éxito

FIG. 4

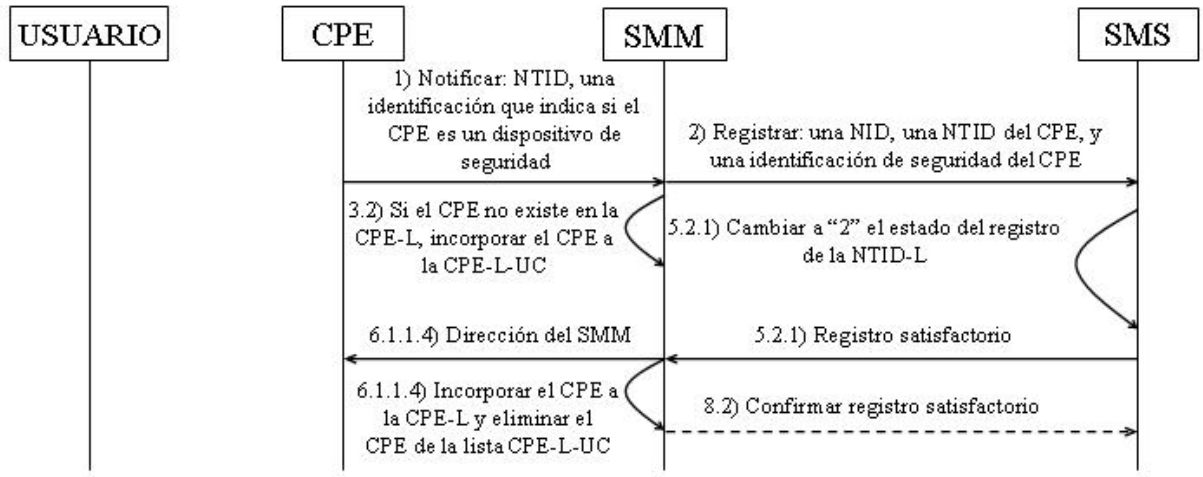
USUARIO
CPE
SMM
SMS
1) Notificar: NTID, una identificación que indica si el CPE es un dispositivo de seguridad
2) Registrar: una NID, una NTID del CPE, y una identificación de seguridad del CPE
3.2) Si el CPE no existe en la CPE-L, incorporar el CPE a la CPE-L-UC
5.2.1) Cambiar a "2" el estado del registro de la NTID-L
6.1.1.4) Dirección del SMM
5.2.1) Registro satisfactorio
6.1.1.4) Incorporar el CPE a la CPE-L y eliminar el CPE de la lista CPE-L-UC
8.2) Confirmar registro satisfactorio

FIG. 5

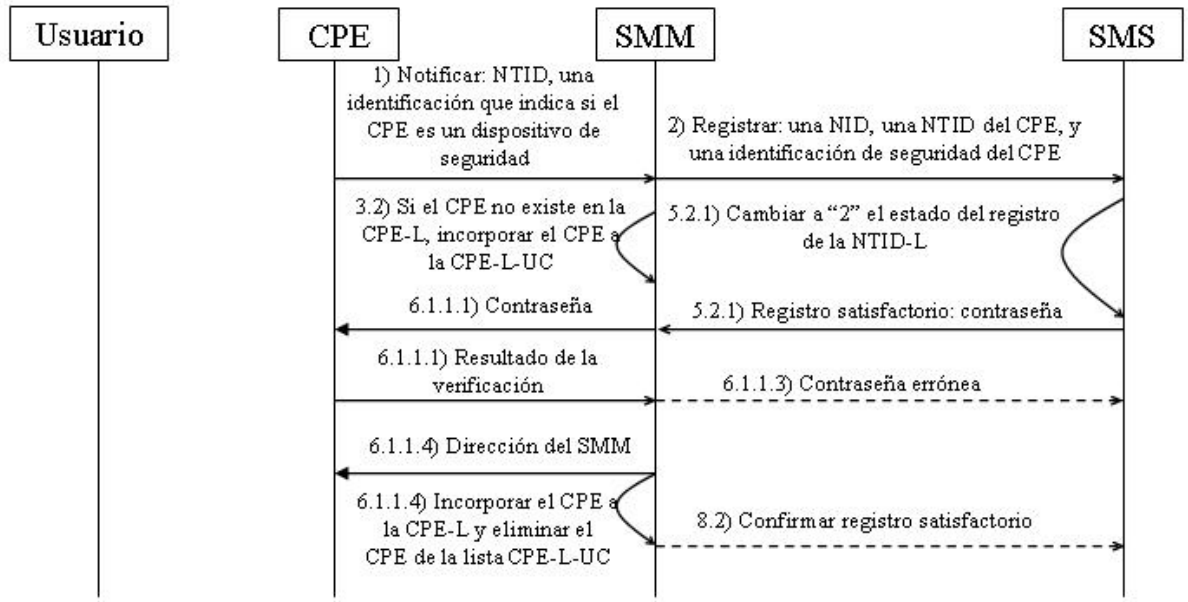
Usuario
CPE
SMM
SMS
1) Notificar: NTID, una identificación que indica si el CPE es un dispositivo de seguridad
2) Registrar: una NID, una NTID del CPE, y una identificación de seguridad del CPE
3.2) Si el CPE no existe en la CPE-L, incorporar el CPE a la CPE-L-UC
5.2.1) Cambiar a "2" el estado del registro de la NTID-L
6.1.1.1) Contraseña
5.2.1) Registro satisfactorio: contraseña
6.1.1.1) Resultado de la verificación
6.1.1.3) Contraseña errónea
6.1.1.4) Dirección del SMM
6.1.1.4) Incorporar el CPE a la CPE-L y eliminar el CPE de la lista CPE-L-UC
8.2) Confirmar registro satisfactorio

FIG. 6

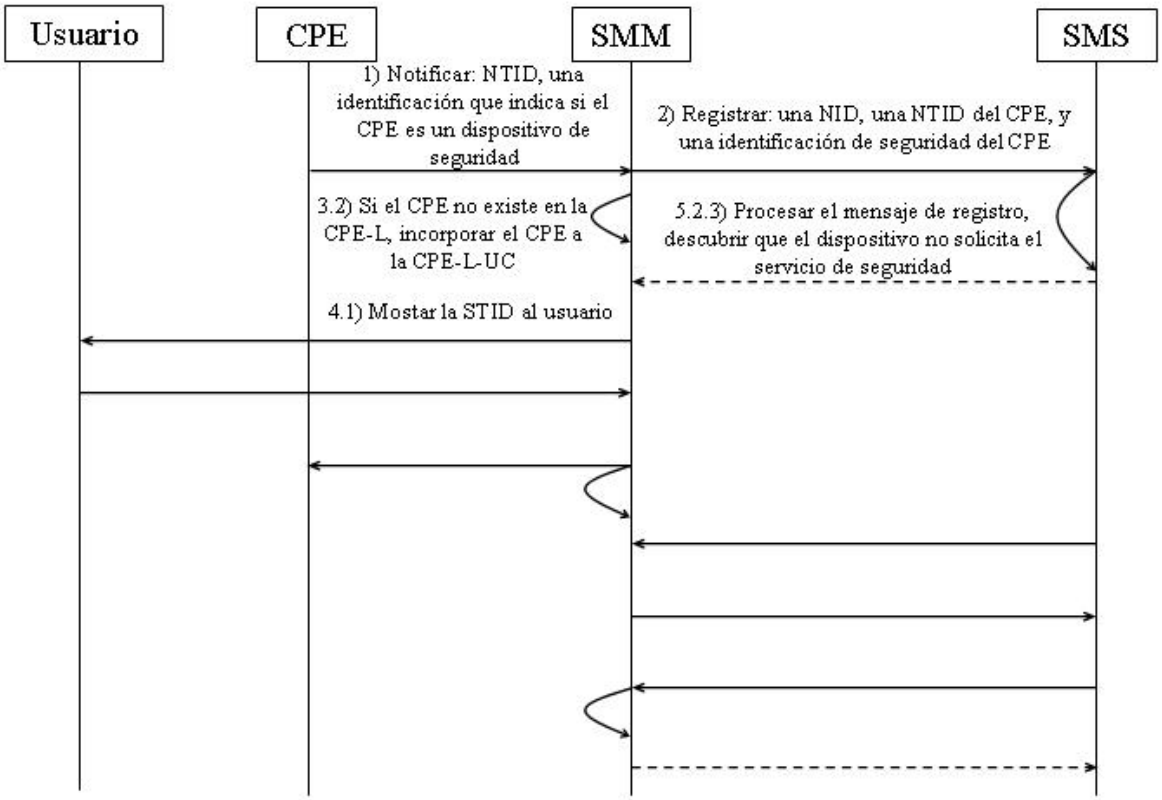
Usuario
CPE
SMM
SMS
1) Notificar: NTID, una identificación que indica si el CPE es un dispositivo de seguridad
2) Registrar: una NID, una NTID del CPE, y una identificación de seguridad del CPE
3.2) Si el CPE no existe en la CPE-L, incorporar el CPE a la CPE-L-UC
5.2.3) Procesar el mensaje de registro, descubrir que el dispositivo no solicita el servicio de seguridad
4.1) Mostar la STID al usuario

FIG. 7

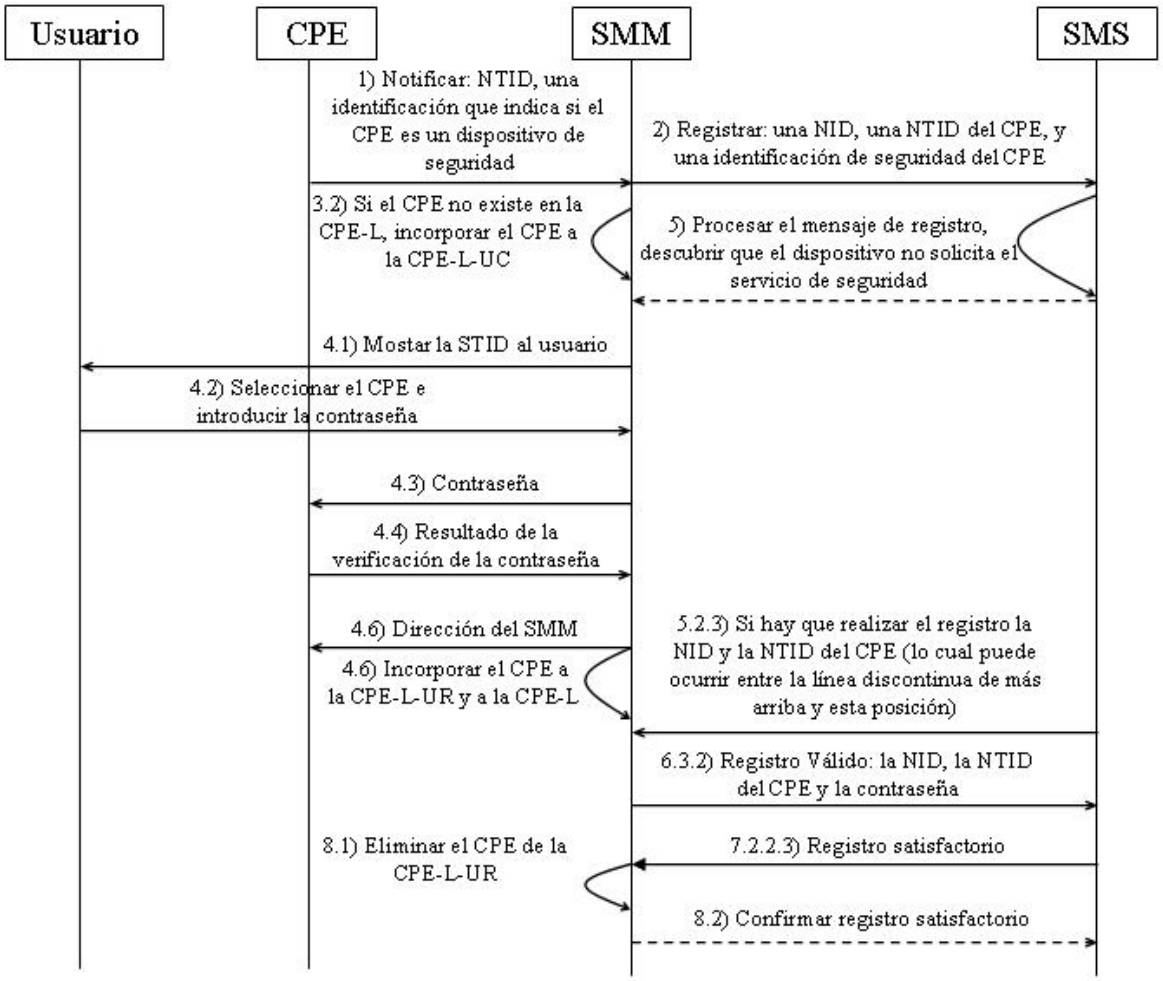
Usuario
CPE
SMM
SMS
1) Notificar: NTID, una identificación que indica si el CPE es un dispositivo de seguridad
2) Registrar: una NID, una NTID del CPE, y una identificación de seguridad del CPE
3.2) Si el CPE no existe en la CPE-L, incorporar el CPE a la CPE-L-UC
5) Procesar el mensaje de registro, descubrir que el dispositivo no solicita el servicio de seguridad
4.1) Mostar la STID al usuario
4.2) Seleccionar el CPE e introducir la contraseña
4.3) Contraseña
4.4) Resultado de la verificación de la contraseña
4.6) Dirección del SMM
4.6) Incorporar el CPE a la CPE-L-UR y a la CPE-L
5.2.3) Si hay que realizar el registro la NID y la NTID del CPE (lo cual puede ocurrir entre la línea discontinua de más arriba y esta posición)
6.3.2) Registro Válido: la NID, la NTID del CPE y la contraseña
8.1) Eliminar el CPE de la CPE-L-UR
7.2.2.3) Registro satisfactorio
8.2) Confirmar registro satisfactorio

FIG. 8

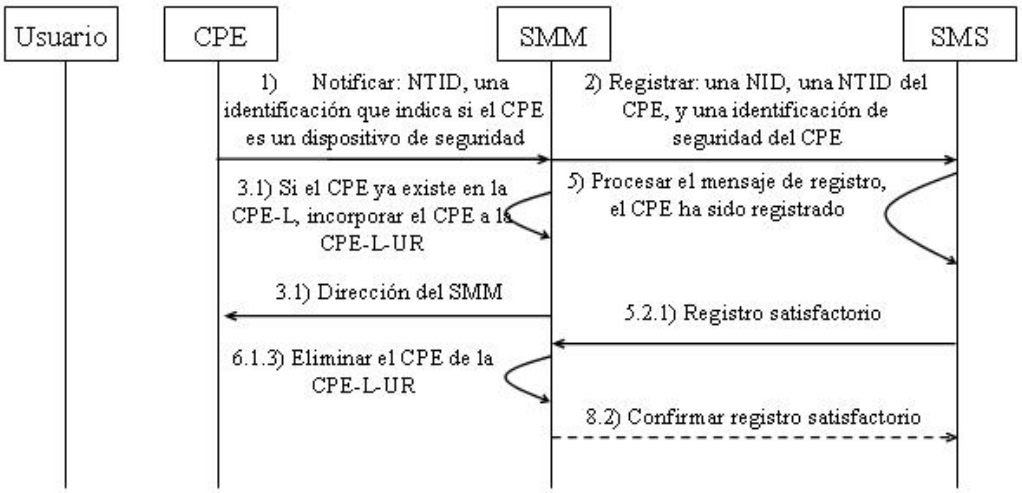
Usuario
CPE
SMM
SMS
1) Notificar: NTID, una identificación que indica si el CPE es un dispositivo de seguridad
2) Registrar: una NID, una NTID del CPE, y una identificación de seguridad del CPE
3.1) Si el CPE ya existe en la CPE-L, incorporar el CPE a la CPE-L-UR
5) Procesar el mensaje de registro, el CPE ha sido registrado
3.1) Dirección del SMM
5.2.1) Registro satisfactorio
6.1.3) Eliminar el CPE de la CPE-L-UR
8.2) Confirmar registro satisfactorio

FIG. 9


Usuario
CPE
SMM
SMS
1) Notificar: NTID, una identificación que indica si el CPE es un dispositivo de seguridad
2) Registrar: una NID, una NTID del CPE, y una identificación de seguridad del CPE
3.2) Si el CPE no existe en la CPE-L, incorporar el CPE a la CPE-L-UC
5) Procesar el mensaje de registro, descubrir que el dispositivo ha pertenecido a otra NID
6.2) Dispositivo no disponible
5.2.2) Se ha registrado en otra red
6.2) Eliminar el CPE de todas las listas

FIG. 10

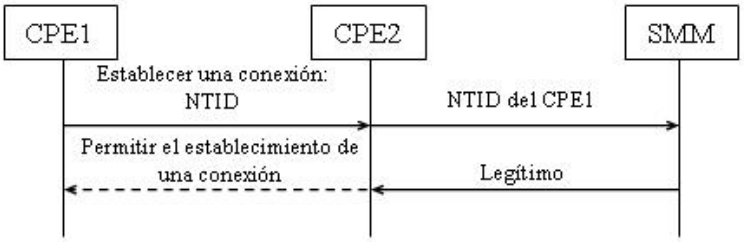
CPE1
CPE2
SMM
Establecer una conexión: NTID
NTID del CPE1
Permitir el establecimiento de una conexión
Legítimo

FIG. 11

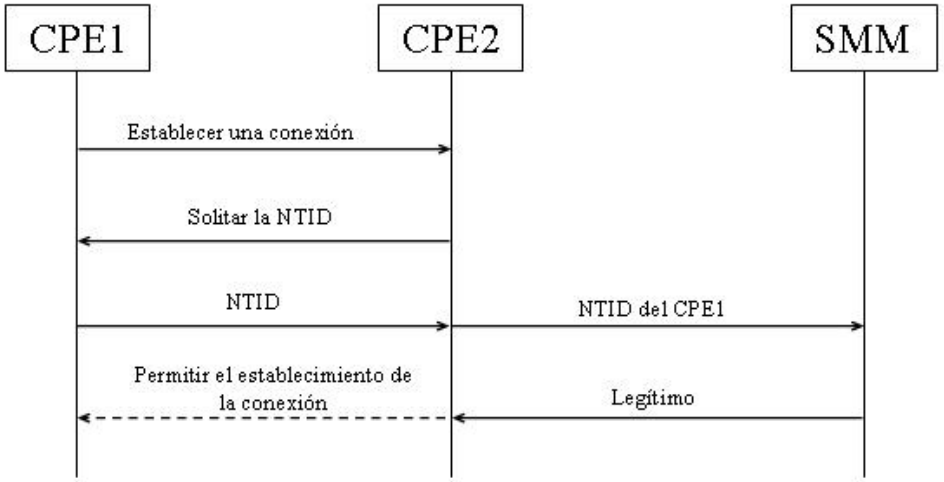
CPE1
CPE2
SMM
Establecer una conexión
Solitar la NTID
NTID
NTID del CPE1
Permitir el establecimiento de la conexión
Legítimo

FIG. 12

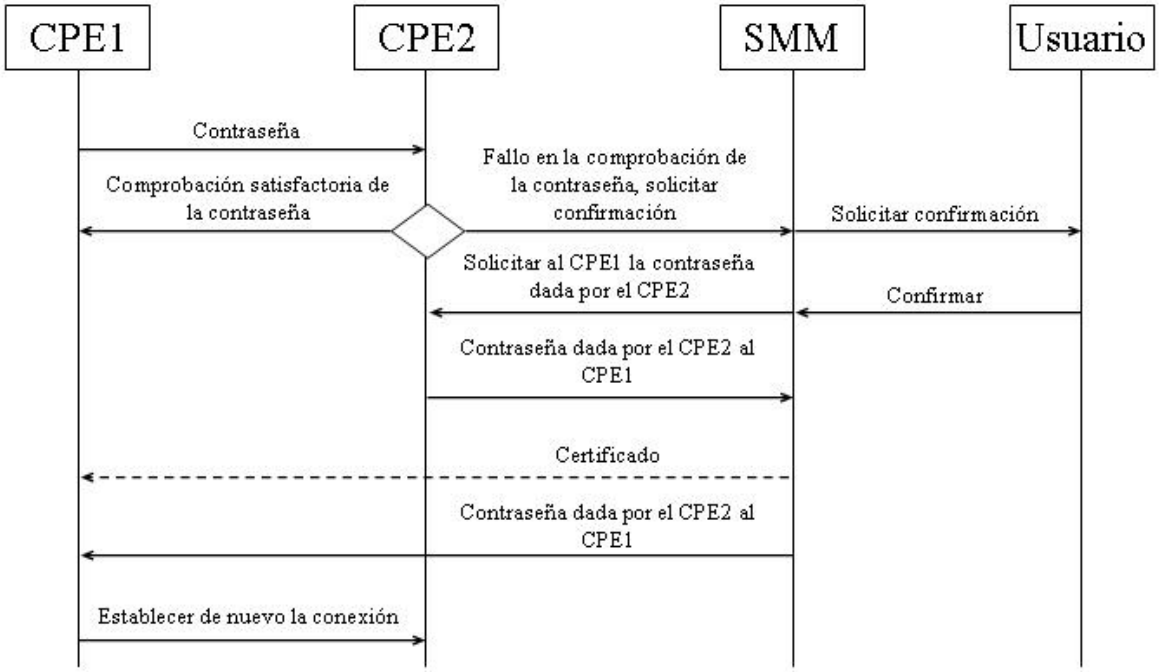
CPE1
CPE2
SMM
Usuario
Contraseña
Comprobación satisfactoria de la contraseña
Fallo en la comprobación de la contraseña, solicitar confirmación
Solicitar confirmación
Solicitar al CPE1 la contraseña dada por el CPE2
Confirmar
Contraseña dada por el CPE2 al CPE1
Certificado
Contraseña dada por el CPE2 al CPE1
Establecer de nuevo la conexión

FIG. 13

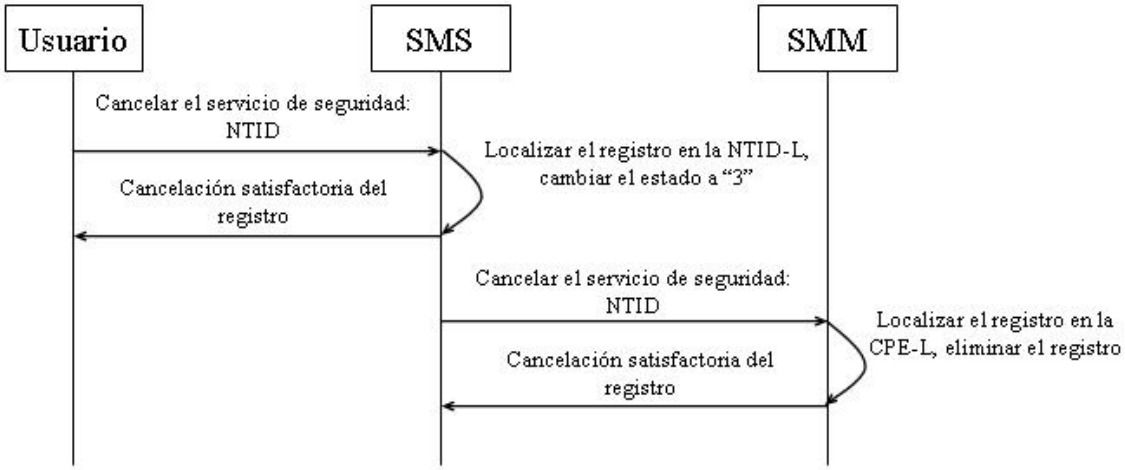
Usuario
SMS
SMM
Cancelar el servicio de seguridad: NTID
Localizar el registro en la NTID-L, cambiar el estado a "3"
Cancelación satisfactoria del registro
Cancelar el servicio de seguridad: NTID
Localizar el registro en la CPE-L, eliminar el registro
Cancelación satisfactoria del registro

FIG. 14

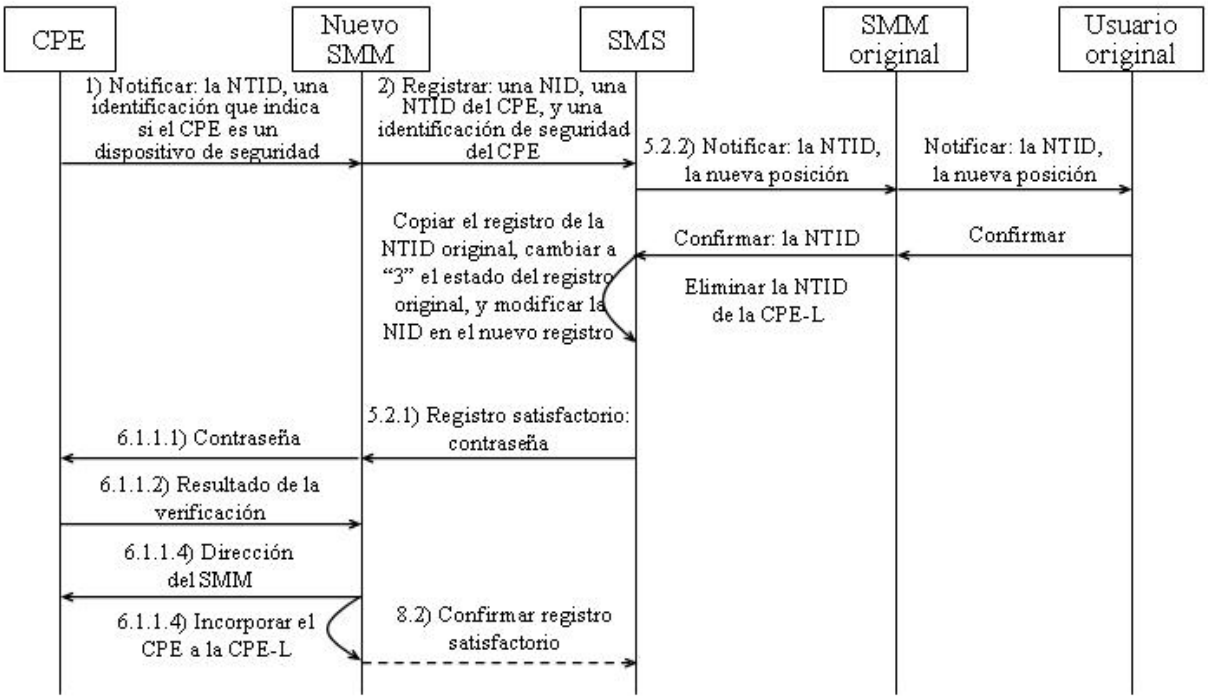
CPE
Nuevo SMM
SMS
SMM original
Usuario original
1) Notificar: la NTID, una identificación que indica si el CPE es un dispositivo de seguridad
2) Registrar: una NID, una NTID del CPE, y una identificación de seguridad del CPE
5.2.2) Notificar: la NTID, la nueva posición
Notificar: la NTID, la nueva posición
Copiar el registro de la NTID original, cambiar a "3" el estado del registro original, y modificar la NID en el nuevo registro
Confirmar: la NTID
Confirmar
Eliminar la NTID de la CPE-L
5.2.1) Registro satisfactorio: contraseña
6.1.1.1) Contraseña
6.1.1.2) Resultado de la verificación
6.1.1.4) Dirección del SMM
6.1.1.4) Incorporar el CPE a la CPE-L
8.2) Confirmar registro satisfactorio

FIG. 15