(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 662 591**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/02 (2009.01)
H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04W 80/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.10.2006 PCT/EP2006/067930**

(87) Fecha y número de publicación internacional: **10.05.2007 WO07051776**

(96) Fecha de presentación y número de la solicitud europea: **30.10.2006 E 06819187 (3)**

(97) Fecha y número de publicación de la concesión europea: **31.01.2018 EP 1943808**

(54) Título: **Procedimiento y servidor para la facilitación de una clave de movilidad**

(30) Prioridad:

04.11.2005 DE 102005052724
24.02.2006 DE 102006008745

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.04.2018

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

FALK, RAINER;
GÜNTHER, CHRISTIAN y
KRÖSELBERG, DIRK

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO Y SERVIDOR PARA LA FACILITACIÓN DE UNA CLAVE DE MOVILIDAD

DESCRIPCIÓN

La invención se refiere a un procedimiento y un servidor proxy para la facilitación de una clave de movilidad para el aseguramiento criptográfico de mensajes de señalización de movilidad para un agente inicial de una red de telefonía, en particular para usuarios anónimos.

Internet con el protocolo TCP/IP ofrece una plataforma para el desarrollo de protocolos más elevados para el sector móvil. Dado que los protocolos de internet están muy extendidos, con ampliaciones de protocolos correspondientes para entornos móviles se puede abrir un gran círculo de usuarios. No obstante, los protocolos de internet convencionales no están concebidos originalmente para un uso móvil. En la transmisión de paquetes de datos de internet convencional se intercambian los paquetes entre ordenadores estacionarios, que no modifican su dirección de red ni migran entre distintas subredes. En las redes de radio con ordenadores móviles se incluyen ordenadores móviles MS con frecuencia en distintas redes. El DHCP (Dynamic Host Configuration Protocol (protocolo de configuración dinámica de host)) posibilita con ayuda de un servidor correspondiente la asignación dinámica de una dirección IP y otros parámetros de configuración a un ordenador en una red. Un ordenador, que se incluye en una red, recibe asignada automáticamente una dirección IP libre por el protocolo DHCP. Si un ordenador móvil ha instalado el DHCP, sólo debe entrar en al alcance de una red local que asiste en la configuración a través del protocolo DHCP. En el caso del protocolo DHCP es posible una concesión de dirección dinámica, es decir, una dirección IP libre se destina automáticamente durante un tiempo determinado. Tras expirar este tiempo se debe plantear nuevamente la solicitud por el ordenador móvil o la dirección IP se puede conceder de otra manera.

Con el DHCP se puede incluir un ordenador móvil sin configuración manual en una red. Como condición sólo debe estar a disposición un servidor DHCP. Un ordenador móvil puede usar así los servicios de la red local y usar, por ejemplo, los ficheros depositados de forma centralizada. No obstante, si un ordenador móvil ofrece por sí mismo servicios, un usuario potencial de servicios puede no encontrar el ordenador móvil, ya que se modifica su dirección IP en cada red en la que se incluye el ordenador móvil. Lo mismo ocurre cuando se modifica una dirección IP durante una conexión TCP existente. Esto conduce a la interrupción de la conexión. Por ello en el caso de Mobile IP un ordenador móvil recibe asignada una dirección IP, que también la mantiene en otra red. En un cambio de red IP convencional es necesario adaptar correspondientemente los ajustes de la dirección IP. No obstante, una adaptación constante de configuraciones IP y de enrutamiento al terminal es casi imposible manualmente. En el caso de mecanismos de configuración automáticos convencionales, la conexión existente se interrumpe en un cambio de la dirección IP. El protocolo MIP (RFC 2002, RFC 2977, RFC3344, RFC3846, RFC3957, RFC3775, RFC3776, RFC4285) asiste en la movilidad de terminales móviles. En los protocolos IP convencionales, el terminal debe adaptar cada vez su dirección IP cuando cambia la subred IP, para que se enruten correctamente los paquetes de datos direccionados al terminal móvil. Para conservar una conexión TCP existente, el terminal móvil debe mantener su dirección IP, dado que un cambio de dirección conduce a una interrupción de la conexión. El protocolo MIP anula este conflicto, en tanto que le permite a un terminal o un nodo móvil (Mobile Node, MN) poseer dos direcciones IP. El protocolo MIP posibilita una conexión transparente entre las dos direcciones, a saber, una dirección doméstica permanente y una segunda dirección de custodia (care-of address). La dirección de custodia es la dirección IP bajo la que se puede localizar actualmente el terminal móvil.

Un agente inicial (Home Agent) es un representante del terminal móvil, en tanto que el terminal móvil no se queda en su red doméstica original. El agente inicial está informado constantemente sobre el paradero del ordenador móvil. El agente inicial representa habitualmente un componente de un router en la red doméstica del terminal móvil. Cuando el terminal móvil se encuentra fuera de la red doméstica, el agente inicial proporciona una función para que se pueda registrar el terminal móvil. Luego el agente inicial transmite los paquetes de datos direccionados al terminal móvil a la subred actual del terminal móvil.

Un agente externo (Foreign Agent) se encuentra en la subred en la que se mueve el terminal móvil. El agente externo transmite los paquetes de datos entrantes al terminal móvil o al ordenador móvil. El agente externo se encuentra en una así denominada red externa (Visited Network). El agente externo representa igualmente habitualmente un componente de un router. El agente externo direcciona todos los paquetes de datos móviles administrativos entre el terminal móvil y su agente inicial. El agente externo desempaqueta los paquetes de datos IP tunelados, enviados por el agente inicial y retransmite sus datos al terminal móvil.

La dirección doméstica del terminal móvil es la dirección bajo la que se puede localizar permanentemente el terminal móvil. La dirección doméstica tiene el mismo prefijo de dirección que el agente inicial. La dirección de custodia es aquella dirección IP que usa el terminal móvil en la red externa.

El agente inicial cuida una así denominada tabla de enlaces de movilidad (MBT: Mobility Binding Table). Las entradas en esta tabla sirven para asociar las dos direcciones, es decir, la dirección doméstica y la dirección de custodia, de un terminal móvil entre sí y redireccionar correspondientemente los paquetes de datos. La tabla MBT contiene las entradas sobre la dirección doméstica, la dirección de custodia y un dato sobre el lapso de

tiempo en el que es válida esta asociación (Life Time). La figura 1 muestra un ejemplo de una tabla de enlaces de movilidad según el estado de la técnica.

El agente externo (FA) contiene una lista de visitantes o Visitor List (VL: Visitor List), que contiene la información sobre los terminales móviles que se encuentran precisamente en la red IP del agente externo. La figura 2 muestra un ejemplo de una lista de visitantes de este tipo según el estado de la técnica.

Para que un ordenador móvil se pueda incluir en una red, debe averiguar en primer lugar si se encuentra en su red doméstica o una red externa. Adicionalmente el terminal móvil debe averiguar que ordenador es el agente inicial o el agente externo en la subred. Estas informaciones se determinan por el así denominado Agent Discovery (descubrimiento de agente).

Gracias al registro subsiguiente el terminal móvil puede comunicar su ubicación actual a su agente inicial. Para ello el ordenador móvil o el terminal móvil le envía al agente inicial la dirección de custodia. Para el registro el ordenador móvil envía una Registration-Request o una solicitud de registro al agente inicial. El agente inicial (HA) inscribe la dirección de custodia en su lista y responde con una Registration Reply o una respuesta de registro. Sin embargo, en este caso existe un problema de seguridad. Dado que cada ordenador le puede enviar en principio a un agente inicial una solicitud de registro, se podría simular de manera sencilla ante un agente inicial que un ordenador se ha movido a otra red. Así un ordenador externo podría hacerse cargo de todos los paquetes de datos de un ordenador móvil o terminal móvil, sin que un emisor se entere de ello. Para impedirlo, el ordenador móvil y el agente inicial disponen de claves secretas comunes. Si un ordenador móvil regresa a su red doméstica, se da de baja en el agente inicial, dado que el ordenador móvil puede recibir ahora todos los paquetes de datos por sí mismo. Una red de radio móvil debe presentar entre otros las siguientes propiedades de seguridad. Las informaciones sólo se deben hacer accesibles para interlocutores de comunicación deseados, es decir, los escuchas no deseados no tienen que obtener ningún acceso a los datos transmitidos. La red de radio móvil debe presentar así la propiedad de la confidencialidad (Confidentiality). Junto a ello se debe dar la autenticidad. La autenticidad (Authenticity) le permite a un interlocutor de comunicación constatar sin lugar a duda si se ha establecido una comunicación realmente con un interlocutor de comunicación deseado, o si una parte externa se hace pasar como interlocutor de comunicación. Las autentificaciones se pueden realizar por mensaje o por conexión. Si se autentifica sobre la base de conexiones, ahora se identifica el interlocutor de comunicación una vez al inicio de una sesión (Session). Para el desarrollo posterior de la sesión se parte de que los mensajes siguientes proceden además del emisor correspondiente. Aun cuando está fijada la identidad de un interlocutor de comunicación, es decir, el interlocutor de comunicación está autentificado, puede ocurrir el caso de que este interlocutor de comunicación no pueda acceder a todos los recursos o no pueda usar todos los servicios a través de la red. Una autorización correspondiente presupone en este caso una autentificación anterior del interlocutor de comunicación.

En el caso de redes de datos móviles, los mensajes deben recorrer trayectos más largos a través de interfaces aéreas y por consiguiente son fácilmente localizables por agresores potenciales. En el caso de redes de datos móviles e inalámbricas, los aspectos de seguridad desempeñan por ello un papel especial. Las técnicas de encriptación representan un medio esencial para el aumento de la seguridad en las redes de datos. Mediante la encriptación es posible transmitir datos a través de vías de comunicación inseguras, por ejemplo, a través de interfaces aéreas, sin que terceros no autorizados logren acceso a los datos. Para el encriptado se transforman los datos, es decir, el así denominado texto no codificado en texto cifrado con la ayuda de un algoritmo de encriptación. El texto encriptado se puede transportar a través del canal de transmisión de datos inseguro y desencriptarse o descifrarse a continuación.

Como una tecnología de acceso inalámbrica muy prometedora se propone WiMax (Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas)) como nuevo estándar que se usa para la transmisión de radio IEEE 802.16. Con WiMax se deben atender gracias estaciones emisoras un área de hasta 50 km con tasas de datos de por encima de 100 Mbit por segundo.

La figura 3 muestra un modelo de referencia para una red de radio WiMax. Un terminal móvil MS se sitúa en el área de una red de acceso (ASN: Access Serving Network (red de servicio de acceso)). La red de acceso ASN está conectada a través de al menos una red visitada (Visited Connectivity Service Network, VCSN (red visitada de servicio de conectividad)) o red intermedia con una red doméstica HCSN (Home Connectivity Service Network (red doméstica de servicio de conectividad). Las distintas redes están conectadas entre sí a través de interfaces o puntos de referencia R. El agente inicial HA de la estación móvil MS se sitúa en la red doméstica HCSN o en una de las redes visitadas VCSN.

WiMax asiste en dos variantes de realización de Mobile IP, así denominado MIP de cliente (CMIP), en el que la estación móvil misma realiza la función de cliente MIP y proxy MIP (PMIP), en el que la función de cliente MIP se realiza por la red de acceso WiMax. La funcionalidad prevista para ello en la ASN se designa como nodo móvil proxy (Proxy Mobile Node, PMN) o como cliente PMIP. De este modo MIP también se puede usar con estaciones móviles que no asisten en sí ningún MIP.

La figura 4 muestra el establecimiento de conexión en el caso de proxy MIP cuando el agente inicial se sitúa en la red visitada según el estado de la técnica.

Después de un establecimiento de conexión de radio entre el terminal móvil y una estación base se realiza en primer lugar una autentificación de acceso. La función de la autentificación, la autorización y la contabilidad se realiza mediante un así denominado servidor AAA (AAA: Authentication Autorización and Accounting). Entre el terminal móvil MS y el servidor AAA de la red doméstica (HAAA) se intercambian mensajes de autentificación mediante los que se obtienen la dirección del agente inicial y una clave de autentificación. El servidor de autentificación en la red doméstica contiene los datos de perfil del usuario. El servidor AAA contiene un mensaje de solicitud de autentificación, que contiene una identidad de usuario del terminal móvil. El servidor AAA genera después de la autentificación satisfactoria una clave MSK (MSK: Master Session Key (clave de sesión maestro)) para la protección el trayecto de transmisión de datos entre el terminal móvil MS y la estación base de la red de acceso ASN. Esta clave MSK se transmite del servidor AAA de la red doméstica a través de la red intermedia CSN a la red de acceso ASN.

Después de la autentificación de acceso se configura, según se puede ver en la figura 4, el servidor proxy DHCP en la red de acceso ASN. Si la dirección IP y la configuración host ya está contenida en el mensaje de respuesta AAA, toda la información se descarga en el servidor proxy DHCP.

Después de la autentificación y autorización satisfactorias, la estación móvil o el terminal móvil MS envía un mensaje de descubrimiento DHCP y se realiza una asignación de dirección IP.

Si la red de acceso ASN asiste tanto en la movilidad PMIP como también CMIP, el agente externo informa a la función de entrega ASN, en tanto que envía un mensaje de texto de movilidad R3. En redes, que sólo puede favorecer el PMIP, se puede prescindir de ello. Después de que se ha leído la dirección doméstica, ésta se le retransmite al cliente PMIP.

A continuación se realiza un registro MIP. En el registro se le informa al agente inicial sobre la ubicación actual del terminal móvil. Para el registro el ordenador móvil envía la solicitud de registro al agente inicial, que contiene la dirección de custodia actual. El agente inicial inscribe la dirección de custodia en una lista gestionada por él y responde con una respuesta de registro (Registration Reply). Dado que cada ordenador puede enviar en principio a un agente inicial una solicitud de registro, se podría simular de manera sencilla ante un agente inicial que un ordenador se ha movido a otra red. Para impedirlo tanto el ordenador móvil como también el agente inicial disponen de una clave común secreta, a saber, una clave MIP. Si el agente inicial (HA) no conoce la clave MIP, la configura para que se comunique con un servidor AAA doméstico.

Tras la conclusión del establecimiento de conexión representado en la figura 4, el terminal móvil ha obtenido una dirección doméstica y está registrado en el agente inicial.

Sin embargo, el establecimiento de conexión representado en la figura 4 no es posible cuando el servidor AAA doméstico no proporciona los atributos o datos esperados por el protocolo WiMax. Si, por ejemplo, en el caso del servidor AAA doméstico se trata de un servidor 3GPP u otro servidor AAA, que no asiste el interfuncionamiento WiMax, entonces éste no es capaz de poner a disposición los atributos de datos necesarios para el registro MIP, en particular la dirección doméstica y una clave criptográfica. El agente inicial HA no obtiene por consiguiente ninguna clave MIP (MSK: Master Session Key) y rechaza el usuario.

El documento de trabajo IETF (borrador de internet) de Nakhjiri et. al., “EAP based Proxy Mobile IP key bootstrapping for WiMAX” da a conocer producir una clave común entre un nodo móvil y un agente inicial, de modo que se puedan transmitir los mensajes de registro MIP autentificados, y explica los principios para ello.

La publicación de la conferencia de Daehyon et al., “Architecture for 3G and 802.16 Wireless Networks Integration with QoS Support” propone una arquitectura de red que conecta una red 3G con una red 802-16 y a este respecto proporciona un respaldo de calidad de servicio para aplicaciones multimedia.

El documento WO 2007/011995 A1 da a conocer un sistema para la manipulación de registros de Mobile IP seguros usando un nodo móvil proxy y un servidor AAA, y detalla los procesos entre los nodos móviles proxy, agente inicial y servidor de seguridad, en particular con vistas a una clave PMN-HA.

El documento del estándar IETF (RFC 3846) de Johansson et al., "Mobile IPv4 Extension for Carrying Network Access Identifiers" propone una extensión de soporte NAI que se puede usar en solicitudes y respuestas de registro de Mobile IP.

El documento del estándar IETF (RFC 4004) de Calhoun et al., “Diameter Mobile IPv4 Application” muestra el uso de un servidor proxy AAA, que actúa en representación para cada servidor AAA que pudiera usar el agente inicial.

El objetivo de la presente invención es crear un procedimiento para la facilitación de una clave de movilidad para una red de telefonía móvil, en la que el servidor de autentificación de la red doméstica no asista ningún registro MIP.

Este objetivo se consigue según la invención mediante un procedimiento con las características indicadas en la reivindicación 1.

La invención crea un procedimiento para la facilitación al menos de una clave de movilidad para el aseguramiento criptográfico de mensajes de señalización de movilidad para un agente inicial con las siguientes etapas, a saber:

- establecimiento de una conexión de radio entre un terminal móvil de usuario y una red de acceso, en donde un servidor proxy de autentificación de una red intermedia retransmite para la autentificación del usuario al menos un mensaje de autentificación, que contiene una identidad de usuario, entre la red de acceso y una red doméstica del usuario y en el caso de autentificación satisfactoria por un servidor de autorización de la red doméstica se le asigna a la identidad del usuario una clave de movilidad específica al grupo, cuando la identidad de usuario contenida en el mensaje de autentificación ya está almacenada en el servidor proxy de autentificación;
- recepción por el agente inicial de un mensaje de solicitud de registro que procede de un terminal de usuario, que contiene una identidad de usuario;
- envío de un mensaje de solicitud de clave para una clave de movilidad por el agente inicial al servidor proxy de autentificación correspondiente; en donde el mensaje de solicitud de clave contiene la identidad de usuario contenida en el mensaje de solicitud de registro; y
- facilitación de una clave de movilidad por el servidor proxy de autentificación para el agente inicial, cuando la identidad de usuario contenida en el mensaje de clave concuerda con una de las identidades de usuario almacenadas por el servidor proxy de autentificación.

En una forma de realización preferida del procedimiento según la invención, el servidor proxy de autentificación genera en el caso de autentificación satisfactoria por el servidor de autentificación de la red doméstica una clave de movilidad específica al usuario y la asigna a la identidad de usuario, cuando la identidad de usuario contenida en el mensaje de autentificación todavía no está almacenada en el servidor proxy de autentificación.

En una forma de realización preferida del procedimiento según la invención se borra una clave de movilidad específica al usuario generada después de un corto lapso de tiempo predeterminado por el servidor proxy de autentificación.

En una forma de realización preferida del procedimiento, una clave de movilidad específica al usuario generada se borra por el servidor proxy de autentificación después de su facilitación para el agente inicial.

En una forma de realización preferida del procedimiento según la invención, la clave de movilidad específica al grupo se borra después de un largo lapso de tiempo predeterminado por el servidor proxy de autentificación.

En una forma de realización preferida del procedimiento según la invención, el servidor proxy de autentificación actualiza un sello de tiempo correspondiente a la identidad de usuario y pone una bandera correspondiente, que indica que la clave de movilidad correspondiente es una clave de movilidad específica al grupo, cuando la identidad de usuario contenida en el mensaje de autentificación ya está almacenada en el servidor proxy de autentificación.

En una forma de realización preferida del procedimiento según la invención, la clave de movilidad se genera al azar por el servidor proxy de autentificación.

En una forma de realización preferida del procedimiento según la invención, el servidor de autentificación de la red doméstica transmite en el caso de autentificación satisfactoria una clave MSK contenida en un mensaje de autentificación a través del servidor proxy de autentificación a un cliente de autentificación de la red de acceso.

En una forma de realización alternativa del procedimiento según la invención, la clave de movilidad no se genera al azar por el servidor proxy de autentificación, sino que se deriva por el servidor proxy de autentificación de la clave MSK transmitida.

En una forma de realización del procedimiento según la invención, la clave de movilidad forma una parte de la clave MSK transmitida.

En una forma de realización alternativa del procedimiento según la invención, la clave de movilidad es idéntica a la clave MSK transmitida.

En una forma de realización del procedimiento según la invención, los mensajes de autentificación se transmiten según un protocolo de transmisión de datos Radius.

En una forma de realización alternativa del procedimiento según la invención, los mensajes de autentificación se transmiten según un protocolo de transmisión de datos Diameter.

En una forma de realización preferida del procedimiento según la invención, la red de acceso se forma por una red de acceso WiMax ASN.

En una forma de realización preferida del procedimiento según la invención, la red de acceso se forma por una red intermedia WiMax CSN.

En una primera forma de realización del procedimiento según la invención, la red doméstica es una red 3GPP.

En una forma de realización alternativa del procedimiento según la invención, la red doméstica se forma por una red que proporciona una infraestructura AAA para usuarios WLAN (red WLAN).

En una forma de realización preferida del procedimiento según la invención, la identidad de usuario se forma por un identificador de acceso de red NAI (Network Access Identifier).

En una forma de realización preferida del procedimiento según la invención, la clave de movilidad se le proporciona adicionalmente a un cliente PMIP de la red de acceso.

En una forma de realización preferida del procedimiento según la invención están presentes varias redes intermedias entre la red de acceso y la red doméstica.

En una primera forma de realización del procedimiento según la invención, el agente inicial se sitúa en la red doméstica.

En una forma de realización alternativa del procedimiento según la invención, el agente inicial se sitúa en una de las redes intermedias.

En una primera forma de realización del procedimiento según la invención, el servidor proxy de autentificación está previsto en la red doméstica.

En una forma de realización alternativa del procedimiento según la invención, el servidor proxy de autentificación está previsto en una de las redes intermedias.

La invención crea además un servidor proxy de autentificación para la facilitación de una clave de movilidad para un aseguramiento criptográfico de mensajes de señalización de movilidad, en donde el servidor proxy de autentificación le asocia después de la autentificación satisfactoria de un usuario mediante un mensaje de autentificación, que contiene una identidad de usuario, a la identidad de usuario una clave de movilidad específica al grupo, cuando la identidad de usuario correspondiente ya está almacenada en el servidor proxy de autentificación.

A continuación se describen formas de realización preferidas del procedimiento según la invención y del servidor proxy de autentificación según la invención en referencia a las figuras adjuntas para la explicación de las características esenciales para la invención.

Muestran:

Figura 1 un ejemplo de una tabla de enlaces de movilidad según el estado de la técnica;

Figura 2 un ejemplo para una lista de visitantes según el estado de la técnica;

Figura 3 una estructura de red de referencia para una red de radio WiMax;

Figura 4 un establecimiento de conexión en una red Wi-Max convencional según el estado de la técnica;

Figura 5 una estructura de red según una forma de realización preferida del procedimiento según la invención;

Figura 6 un diagrama de desarrollo para la explicación del modo de funcionamiento del procedimiento según la invención;

Figura 7 otro diagrama de desarrollo para la explicación del modo de funcionamiento del procedimiento según la invención;

Figura 8 un diagrama para la explicación del modo de funcionamiento del procedimiento según la invención.

Figura 9 un ejemplo de una tabla que está almacenada en una forma de realización preferida del servidor proxy de autentificación según la invención.

Según se puede reconocer de la figura 5, un terminal móvil 1 está conectado a través de una interfaz inalámbrica 2 con una estación base 3 de una red de acceso 4. En el caso del terminal móvil 1 se trata de un terminal móvil cualquiera, por ejemplo, un portátil, una PDA, un teléfono móvil u otro terminal móvil. La estación base 3 de la red de acceso 4 está conectada con una pasarela de red de acceso 6 a través de una línea de transmisión de datos 5. En el ordenador de la pasarela de acceso 6 están integradas preferentemente otras funcionalidades, en particular un agente externo 6A, un cliente PMIP 6B, un servidor de cliente AAA 6C y un servidor proxy DHCP 6D. El agente externo 6A es un router que pone a disposición servicios de enrutamiento para el terminal móvil 1. Los paquetes de datos dirigidos al terminal móvil 1 se transmiten de forma tunelada y se desempaquetan por el agente externo 6A.

La pasarela 6 de la red de acceso 4 está conectada con un ordenador 8 de una red intermedia 9 a través de una interfaz 7. El ordenador 8 contiene un servidor DCHP 8A, un agente inicial 8B y un servidor proxy AAA 8C. El agente inicial 8B es el representante del terminal móvil 1, cuando éste no se sitúa en su red doméstica original. El agente inicial 8B está informado constantemente sobre el paradero del ordenador móvil 1. Los paquetes de datos para el terminal móvil 1 se transmiten en primer lugar al agente inicial y se transfiere desde el agente inicial de forma tunelada al agente externo 6A. A la inversa los paquetes de datos, que se emiten por el terminal móvil 1, se pueden enviar directamente al interlocutor de comunicación correspondiente. Los paquetes de datos del terminal móvil 1 contienen a este respecto la dirección doméstica como dirección de remitente. La dirección doméstica tiene el mismo prefijo, es decir, la dirección de red y dirección de subred, que el agente inicial 8B. Los paquetes de datos, que se envían a la dirección doméstica del terminal móvil 1, se interceptan por el agente inicial 8B y se transmiten de forma tunelada del agente inicial 8B a la dirección de custodia del terminal móvil 1 y finalmente se reciben en el punto final del túnel, es decir, por el agente externo 6A o el mismo terminal móvil.

El ordenador 8 de la red intermedia 9 está conectado con un servidor de autentificación 11 de una red doméstica 12 a través de otra interfaz 10. En el caso de una red doméstica 12 se trata, por ejemplo, una red 3GPP para UMTS. En una forma de realización, en el caso del servidor 11 se trata un servidor de autentificación de una red WLAN. El servidor de autentificación 11 representada en la figura 5 no asiste un registro MIP.

En cuanto el servidor proxy AAA 8C del ordenador 8 reconoce que el servidor AAA 11 de la red doméstica 12 no asiste un MIP (CMIP/PMIP), la facilitación de una clave de movilidad para el aseguramiento criptográfica de mensajes de señalización de movilidad para el agente inicial 8B se realiza según el procedimiento según la invención. El servidor proxy AAA 8B reconoce la falta de asistencia CMIP/PMIP, por ejemplo, porque no se proporcionan los atributos MIP por el servidor 11 de la red doméstica 12 a una solicitud. Para el aseguramiento criptográfico de los mensajes de señalización de movilidad se necesita una clave de movilidad común (clave MIP) para el agente inicial 8B y el terminal móvil 1 para el caso PMIP o una clave de movilidad común para el agente inicial 8B y un cliente PMIP 6B para el caso PMIP. Si la red doméstica 12 es apta al interfuncionamiento WiMax, el agente inicial 8B obtiene esta clave MIP por el servidor AAA de la red doméstica 12. Sin embargo, según está representado en la figura 5, si el servidor AAA 11 no es capaz de poner a disposición los atributos MIP necesarios a la solicitud correspondiente del agente inicial 8B, se activa el procedimiento según la invención. El servidor 3GPP AAA 11, según está representado en la figura 5, dado que no puede interpretar la solicitud del agente inicial 8B, no puede proporcionar ninguna clave criptográfica correspondiente para el aseguramiento de los mensajes de señalización de movilización. En el procedimiento según la invención, el servidor de autentificación 11 de la red doméstica 12 no apto a WiMax se deja de forma invariable y la clave de movilidad se le proporciona por el servidor proxy AAA 8C al agente inicial 8B. Después de que se ha reconocido que el servidor de autentificación 11 de la red doméstica 12 no proporciona ninguna clave de movilidad, una así denominada funcionalidad proxy Home MIP se activa y para esta sesión AAA se aplica un juego de datos por el servidor proxy de autentificación 8C. La funcionalidad requerida PMIP/CMIP no se pone a disposición así según la invención por el servidor de autentificación 11 de la red doméstica 12, sino mediante el servidor proxy AAA de la red intermedia 9, que se sitúa en el camino de comunicación entre el servidor de autentificación 11 de la red 3GPP y la pasarela 6 de la red de acceso 4.

La figura 6 muestra un diagrama de desarrollo para la autentificación de un terminal móvil 1 en una forma de realización del procedimiento según la invención.

Después de una etapa de inicio, en una etapa S1 se establece en primer lugar una conexión de radio entre el terminal móvil 1 y una estación base 3 de la red de acceso 4 en la etapa S1. A continuación en la etapa S2 se transmiten los mensajes de autentificación entre la red de acceso 4 y la red doméstica 12 mediante el servidor proxy de autentificación 8C de la red intermedia 9. Los mensajes de autentificación contienen una identidad de usuario para la identificación del terminal móvil 1 correspondiente. En el caso de la identidad de usuario se trata, por ejemplo, de un identificador de acceso de red NAI. Alternativamente la identidad de usuario se forma, por ejemplo, por una dirección doméstica del terminal móvil 1. Los mensajes de autentificación transmitidos por el

servidor proxy AAA 8C llegan al servidor de autentificación 11 de la red doméstica 12. El servidor de autentificación 11 de la red doméstica 12 realiza entonces la autentificación del usuario. Si la autentificación es satisfactoria, el servidor de autentificación 11 envía un mensaje correspondiente a través del servidor proxy de autentificación 8C de la red intermedia 9 a la red de acceso 4. En la etapa S3 el servidor proxy de autentificación 8C de la red intermedia 9 examina si la autentificación se ha terminado satisfactoriamente por el servidor de autentificación 11 de la red doméstica 12. Lo reconoce, por ejemplo, en una comunicación de éxito correspondiente (comunicación de "success") del servidor de autentificación 11. Si el servidor proxy de autentificación 8C reconoce mediante los mensajes transmitidos por la red doméstica 12 a la red de acceso 4 que la autentificación de un usuario se ha terminado de forma satisfactoria, mediante el servidor proxy de autentificación 8C se examina en la etapa S4, si la identidad de usuario contenida en el mensaje de autentificación ya está almacenada en el servidor proxy de autentificación 8C.

Si la identidad de usuario ya está almacenada de forma intermedia en el servidor proxy de autentificación 8C, a la identidad de usuario se le asocia en la etapa S5 una clave de movilidad específica al grupo. A este respecto se actualiza preferentemente un sello de tiempo correspondiente a la identidad de usuario y además se pone una bandera correspondiente, que indica que la clave de movilidad correspondiente es una clave de movilidad específica al grupo. A las identidades de usuario idénticas o iguales se les proporciona por consiguiente una clave de movilidad idéntica o específica al grupo mediante el servidor proxy de autentificación 8C. Esto posibilita el uso de identidades de usuario anónimas o identificadores de red anónimos NAI (Network Access Identifier). Una identidad de usuario es anónima cuando no está asociada de forma unívoca a un usuario determinado. Una identidad de usuario anónima de este tipo suena, por ejemplo, "user@vodafone.com" según se muestra en la primera línea de la tabla representada en la figura 9. La clave de movilidad específica al grupo, puesta a disposición para la identidad de usuario anónima se lee en el ejemplo representado en la figura 9 como "12AF". El tipo de clave de la clave de movilidad está caracterizado como específica al grupo a través de una bandera o carácter indicador correspondiente "group specific key".

Si en la etapa S4 se constata que la identidad de usuario contenida en el mensaje de autentificación todavía no está almacenado en el servidor proxy de autentificación 8C, en la etapa S6 se genera una clave de movilidad específica al usuario y se le asocia a la identidad de usuario correspondiente. La clave correspondiente se caracteriza como específica al usuario y se actualiza el sello temporal correspondiente. En el ejemplo representado en la figura 9, en la primera aparición de la identidad de usuario "glyn@isarpatent.com" se genera la clave de movilidad específica al usuario "14BC" y se caracteriza como clave específica al usuario "user specific key". En una forma de realización preferida, la clave de movilidad específica al usuario se deriva por el servidor proxy de autentificación 8C de una clave MSK transmitida, que está contenida en el mensaje de autentificación, que se transmite a través del servidor proxy de autentificación 8C hacia un cliente de autentificación 6C de la red de acceso

En una forma de realización preferida del procedimiento según la invención, la clave de movilidad específica al grupo asociada a la etapa S5 se genera al azar por el servidor proxy de autentificación 8C. En el ejemplo representado en la figura 9, al aparecer de nuevo la identidad de usuario "glyn@isarpatent.com" se genera, en una primera forma de realización, otra clave de movilidad específica al usuario generada al azar o la clave de movilidad específica al usuario ya presente "14BC" se caracteriza, en una forma de realización alternativa, al aparecer de nuevo la identidad de usuario como clave específica al usuario, en tanto que la bandera "user specific key" se sobrescribe por la bandera "group specific key".

Mediante el procedimiento según la invención se garantiza que no se produzca una colisión o conflictos cuando dos usuarios usan al azar o de forma deseada la misma identidad de usuario.

En una forma de realización preferida del procedimiento según la invención, la clave de movilidad específica al usuario genera en la etapa S6 se borra por un lapso de tiempo corto predeterminado, por ejemplo después de algunos segundos, usando un sello de tiempo por parte del servidor proxy de autentificación 8C.

El borrado de la clave de movilidad específica al grupo de los participantes anónimos se realiza después de un lapso de tiempo esencialmente más largo de, por ejemplo, algunos segundos o no se realiza en absoluto. Es necesario que se pueden registrar simultáneamente varios usuarios PMIP, que usan la misma identidad de usuario anónima.

En una forma de realización alternativa del procedimiento según la invención, la clave de movilidad específica al grupo no se genera al azar, sino que se preconfigura de forma fija.

En el procedimiento según la invención todos los usuarios anónimos contienen asociada la misma clave de movilidad. Mediante el procedimiento según la invención es posible usar identidades de usuario anónimas en el marco de la autentificación de la solicitud en una red WiMax. De este modo es posible la asistencia de identidades de usuario anónimas o NAI anónimos. El procedimiento según la invención permite además una simplificación de complejidad significativa de la gestión de las relaciones de seguridad requeridas para Mobile IP y PMIP. Esto conduce a una necesidad de almacenamiento dinámica claramente reducida.

Según se puede reconocer por la figura 7, cuando después de la etapa de inicio el agente inicial 8B obtiene en un instante posterior un mensaje de solicitud de registro, el agente inicial 8B envía en la etapa S8 un mensaje de solicitud de clave correspondiente a su servidor proxy de autentificación 8C. En el mensaje de solicitud de registro obtenido está contenida una identidad de usuario de un terminal móvil 1. El mensaje de solicitud de clave generado acto seguido correspondiente del agente inicial 8B al servidor proxy de autentificación 8C contiene igualmente esta identidad de usuario. El servidor proxy de autentificación 8C examina en la etapa S9 si la identidad de usuario contenida en el mensaje de solicitud de clave concuerda con una de las identidades de usuario almacenadas por él en la etapa S4. Si éste es el caso, el servidor proxy de autentificación 8C pone a disposición en la etapa S10 una clave de movilidad para el aseguramiento criptográfico de mensajes de aseguramiento de movilidad. El servidor proxy de autentificación 8C transmite la clave de movilidad proporcionada al agente inicial 8B. Preferentemente la clave de movilidad también se le transmite a un servidor de cliente de autentificación 6D de la red de acceso 4.

La clave de movilidad proporcionada en la etapa S10 se genera al azar en una primera forma de realización del procedimiento según la invención mediante el servidor proxy de autentificación 8C.

En una forma de realización alternativa, la clave de movilidad (clave MIP) se deriva por el servidor proxy de autentificación 8C de una clave MSK (Master Session Key), que ha retransmitido el servidor proxy de autentificación 8C del servidor de autentificación 11 a la red de acceso 4. A este respecto, la clave MIP se puede derivar de la clave MSK según una función de derivación de clave cualquiera, por ejemplo, mediante una función hash. La función hash reduce los datos de cualquier tamaño a una así denominada huella digital. SHA-1 representa un ejemplo para una función hash de este tipo. A este respecto los datos se derivan de como máximo 2^{64} bits a 160 bits. MD5 es una función hash alternativa. MD5 divide como SHA-1 la entrada en bloques del tamaño de 500 bits y genera valores hash de 128 bits de tamaño.

En una forma de realización alternativa, la clave de movilidad puesta a disposición se forma por una parte de la clave MSK 12 recibida por el servidor proxy de autentificación 8C.

En otra forma de realización alternativa, la clave de movilidad proporcionada es idéntica a la clave MSK transmitida.

En formas de realización preferidas, los mensajes de autentificación se transmiten según el protocolo Radius o Diameter.

En el procedimiento según la invención, la red intermedia 9 ofrece la funcionalidad Home MIP si no se asiste por la red doméstica 12. De este modo también es posible hacer posible en redes domésticas, que no asisten ningún MIP, por ejemplo en redes 3GPP, una macromovilidad en base a MIP. MIP se usa dentro de la red de acceso 4 y de la red intermedia 9, para realizar una entrega entre las distintas redes de acceso 4. En el caso del registro MIP del agente externo 6A, el agente inicial 8B de la red intermedia 9 solicitud la clave de movilidad del servidor proxy de autentificación 8C correspondiente. A este respecto usa la identidad de usuario correspondiente, es decir, por ejemplo, una identificación de acceso de red NAI (Network Access Identifier) o la dirección doméstica del terminal móvil 1. Este mensaje de solicitud de clave se responde por el servidor proxy de autentificación 8C de forma local si se aplica un juego de datos correspondiente. Para que el servidor proxy de autentificación 8C pueda poner a disposición la clave correspondiente, está diseñado de manera que interpreta los mensajes, que se intercambian entre el servidor de autentificación 11 de la red doméstica 12 y un autentificador en la red de acceso 4 durante la autentificación de la red móvil 1.

El agente inicial 8B se sitúa preferentemente, según se representa en la figura 5, en la red intermedia 9. En una forma de realización alternativa, el agente inicial 8B se sitúa en la red doméstica 12.

En una forma de realización alternativa del procedimiento según la invención se usa como funcionalidad IP móvil Mobile IPV6 [RFC3775].

En una forma de realización preferida del procedimiento según la invención, la clave de movilidad se solicitud por el agente inicial 8B sólo una vez mediante un mensaje de solicitud de clave del servidor proxy de autentificación 8C.

Con el procedimiento según la invención se posibilita el uso de servidores AAA heredados, como por ejemplo servidores WLAN o 3GPP para redes WiMax, aunque estos servidores no proporcionan la funcionalidad CMIP/PMIP esperada por las redes WiMax. Con el procedimiento según la invención, pese al uso de servidores AAA heredados en la red doméstica 12 es posible una macromovilidad basada en PMIP. Un operador de red de una red WLAN o 3GPP no debe asistir en sí por ello PMIP y puede posibilitar a sus clientes un roaming / interfuncionamiento con redes de radio WiMax. Con el procedimiento según la invención es posible en particular permitir el interfuncionamiento WiMax con la asistencia PMIP también terminales sin asistencia de Mobile IP. En

particular el procedimiento según la invención posibilita un interfuncionamiento WiMax 3GPP de forma análoga al acceso IP directo WLAN especificado actualmente.

La figura 8 muestra un diagrama de flujo de mensajes de una forma de realización preferida del procedimiento según la invención. En la forma de realización representada en la figura 8, la red de acceso 4 y la red intermedia 9 se compone de una red WiMax. La red doméstica 12 se forma por una red 3GPP. El servidor proxy de autentificación 8C previsto en la red intermedia asocia a la estación móvil MS2 la misma clave de movilidad específica al grupo que la estación móvil MS1, cuando la identidad de usuario contenida en el mensaje de autentificación para la segunda estación móvil MS2 ya está almacenada en el servidor proxy de autentificación 8C de la red WiMax 2. El mensaje de solicitud de clave, que contiene la identidad de usuario, se responde en el procedimiento según la invención por el servidor proxy de autentificación 8C de la red intermedia 9. El procedimiento según la invención posibilita por consiguiente una gestión de macromovilidad en redes WiMax sin asistencia de la red doméstica.

La figura 9 muestra un ejemplo de una tabla, que está almacenada preferentemente dentro del servidor proxy de autentificación 8C de la red intermedia 9, para la clarificación del procedimiento según la invención.

REIVINDICACIONES

1. Procedimiento para la facilitación al menos de una clave de movilidad para el aseguramiento criptográfico de mensajes de señalización de movilidad para un agente inicial con las siguientes etapas:

(a) establecimiento de una conexión de radio entre un terminal móvil de usuario (1) y una red de acceso (4),
en donde un servidor proxy de autentificación (8C) de una red intermedia (9) retransmite para la autentificación del usuario al menos un mensaje de autentificación, que contiene una identidad de usuario, entre la red de acceso (4) y una red doméstica (12) del usuario y en el caso de autentificación satisfactoria por un servidor de autorización (11) de la red doméstica (12) se le asigna a la identidad del usuario una clave de movilidad específica al grupo, cuando la identidad de usuario contenida en el mensaje de autentificación ya está almacenada en el servidor proxy de autentificación (8C);
(b) recepción por el agente inicial (8B) de un mensaje de solicitud de registro procedente del terminal de usuario (1), que contiene una identidad de usuario;
(c) envío de un mensaje de solicitud de clave para una clave de movilidad por el agente inicial (8B) al servidor proxy de autentificación (8C) correspondiente;
en donde el mensaje de solicitud de clave contiene la identidad de usuario contenida en el mensaje de solicitud de registro; y
(d) facilitación de una clave de movilidad por el servidor proxy de autentificación (8C) para el agente inicial (8B),

- cuando se reconoce que el servidor de autentificación (11) de la red doméstica (12) no proporciona una clave de movilidad, y
- cuando la identidad de usuario contenida en el mensaje de solicitud de clave concuerda con una de las identidades de usuario almacenadas por el servidor proxy de autentificación (8C).

2. Procedimiento según la reivindicación 1,
en donde el servidor proxy de autentificación (8C) genera una clave de movilidad específica al usuario en el caso de autentificación satisfactoria por el servidor de autentificación (11) de la red doméstica (12) y la asocia a la identidad de usuario, cuando la identidad de usuario contenida en el mensaje de autentificación todavía no está almacenada en el servidor proxy de autentificación (8C).

3. Procedimiento según la reivindicación 1,
en donde una clave de movilidad específica al usuario generada se borra por el servidor proxy de autentificación (8C) después de un corto lapso de tiempo predeterminado.

4. Procedimiento según la reivindicación 1,
en donde una clave de movilidad específica al usuario generada se borra por el servidor proxy de autentificación (8C) después de su facilitación para el agente inicial (8B).

5. Procedimiento según la reivindicación 1,
en donde una clave de movilidad específica al grupo se borra por el servidor proxy de autentificación (8C) después de un largo lapso de tiempo predeterminado.

6. Procedimiento según la reivindicación 1,
en donde, cuando la identidad de usuario contenida en el mensaje de autentificación ya está almacenada en el servidor proxy de autentificación (8C), el servidor proxy de autentificación (8C) actualiza un sello de tiempo correspondiente a la identidad de participante y pone una bandera correspondiente, que muestra que la clave de movilidad correspondiente es una clave de movilidad específica al grupo.

7. Procedimiento según la reivindicación 1,
en donde la clave de movilidad específica al grupo se genera al azar por el servidor proxy de autentificación (8C).

8. Procedimiento según la reivindicación 1,
en donde el servidor de autentificación (11) de la red doméstica (12) transmite en el caso de autentificación satisfactoria una clave de Master Session Key, clave MSK, contenida en el mensaje de autentificación, a través del servidor proxy de autentificación (8C) hacia un cliente de autentificación (6C) de la red de acceso (4).

9. Procedimiento según la reivindicación 8,
en donde la clave de movilidad específica al cliente se deriva por el servidor proxy de autentificación (8C) de la clave MSK transmitida.

10. Procedimiento según la reivindicación 9,

en donde la clave de movilidad específica al usuario forma una parte de la clave MSK transmitida.

11. Procedimiento según la reivindicación 9,
en donde la clave de movilidad específica al usuario es idéntica a la clave MSK transmitida.

12. Procedimiento según la reivindicación 9,
en donde la clave de movilidad específica al usuario se deriva por una función de derivación de clave criptográfica o por una función hash criptográfica.

13. Procedimiento según la reivindicación 1,
en donde el al menos un mensaje de autentificación se transmite según un protocolo de transmisión de datos RADIUS.

14. Procedimiento según la reivindicación 1,
en donde el al menos un mensaje de autentificación se transmite según un protocolo de transmisión de datos Diameter.

15. Procedimiento según la reivindicación 1,
en donde la red de acceso (4) se forma por una red de acceso WIMAX (ASN).

16. Procedimiento según la reivindicación 1,
en donde la red intermedia (9) se forma por una red intermedia WIMAX (CSN).

17. Procedimiento según la reivindicación 1,
en donde la red doméstica (12) se forma por una red 3GPP.

18. Procedimiento según la reivindicación 1,
en donde la red doméstica se forma por una red WLAN.

19. Procedimiento según la reivindicación 1,
en donde la identidad de usuario se forma por un identificador de acceso de red Network Access Identifier, NAI.

20. Procedimiento según la reivindicación 1,
en donde la clave de movilidad se le proporciona adicionalmente a un cliente Proxy Mobile IP, cliente PIMIP, (6B) de la red de acceso (4).

21. Procedimiento según la reivindicación 1,
en donde varias redes intermedias (9) se encuentran entre la red de acceso (4) y la red doméstica (12).

22. Procedimiento según la reivindicación 21,
en donde el agente inicial (8B) está previsto en la red doméstica (12) o en una de las redes intermedias (9).

23. Procedimiento según la reivindicación 21,
en donde el servidor proxy de autentificación (8C) está previsto en la red doméstica (12) o en una de las redes intermedias (9).

24. Servidor proxy de autentificación (8C) de una red intermedia (9)
para la autentificación de un usuario,
para la retransmisión al menos de un mensaje de autentificación, que contiene una identidad de usuario, entre una red de acceso (4) y una red doméstica (12) del usuario,
para la recepción de un mensaje de solicitud de clave para una clave de movilidad de un agente inicial (8B),
para la facilitación de la clave de movilidad para un aseguramiento criptográfico de mensajes de señalización de movilidad para un agente inicial, cuando se reconoce que un servidor de autentificación (11) de la red doméstica (12) no proporciona una clave de movilidad,
en donde el servidor proxy de autentificación (8C), después de una autentificación satisfactoria de un usuario mediante un mensaje de autentificación que contiene una identidad de usuario, le asocia a la identidad de usuario una clave de movilidad específica al grupo, cuando la identidad de usuario correspondiente ya está almacenada en el servidor proxy de autentificación (8C).

25. Servidor proxy de autentificación (8C) según la reivindicación 24,
en donde el servidor proxy de autentificación (8C) genera una clave de movilidad específica al usuario en el caso de autentificación satisfactoria de un usuario mediante un mensaje de autentificación que contiene una identidad de usuario y asocia la identidad de usuario correspondiente cuando la identidad de usuario obtenida en el mensaje de autentificación todavía no está almacenada en el servidor proxy de autentificación (8C).

26. Servidor proxy de autentificación (8C) según la reivindicación 25,
en donde una clave de movilidad específica al usuario generada se borra por el servidor proxy de autentificación (8C) después de un corto lapso de tiempo predeterminado.

27. Servidor proxy de autentificación (8C) según la reivindicación 25,
en donde una clave de movilidad generada específica al usuario se borra por el servidor proxy de autentificación (8C) después de su facilitación para el agente inicial.

28. Servidor proxy de autentificación (8C) según la reivindicación 24,
en donde una clave de movilidad específica al grupo se borra por el servidor proxy de autentificación (8C) antes de un largo lapso de tiempo predeterminado.

29. Servidor proxy de autentificación (8C) según la reivindicación 24,
en donde, cuando la identidad de usuario contenida en el mensaje de autentificación ya está almacenada en el servidor proxy de autentificación (8C), el servidor proxy de autentificación (8C) actualiza un sello de tiempo correspondiente a la identidad de participante y pone una bandera correspondiente, que muestra que la clave de movilidad correspondiente es una clave de movilidad específica al grupo.

30. Servidor proxy de autentificación (8C) según la reivindicación 24,
en donde el servidor proxy de autentificación (8C) genera al azar la clave de movilidad.

31. Servidor proxy de autentificación (8C) según la reivindicación 24,
en donde el servidor proxy de autentificación (8C) está conectado con un servidor de autentificación (11) de una red doméstica (12).

32. Servidor proxy de autentificación (8C) según la reivindicación 24,
en donde el servidor proxy de autentificación (8C) deriva la clave de movilidad de una clave Master Session Key, clave MSK, entregada por el servidor de autentificación (11) de la red doméstica (12).

33. Servidor proxy de autentificación (8C) según la reivindicación 24,
en donde la red doméstica (12) es una red 3GPP.

34. Servidor proxy de autentificación (8C) según la reivindicación 24,
en donde la red doméstica (12) es una red WLAN.

35. Servidor proxy de autentificación (8C) según la reivindicación 24,
en donde el servidor proxy de autentificación (8C) es un servidor proxy de autentificación WIMAX.

FIG 1

Estado de la técnica

Tabla de enlaces de movilidad

Dirección doméstica	Dirección de custodia	Duración
131.192.180.42	129.142.23.42	100
213.123.24.140	172.23.142.49	150
...	...	...

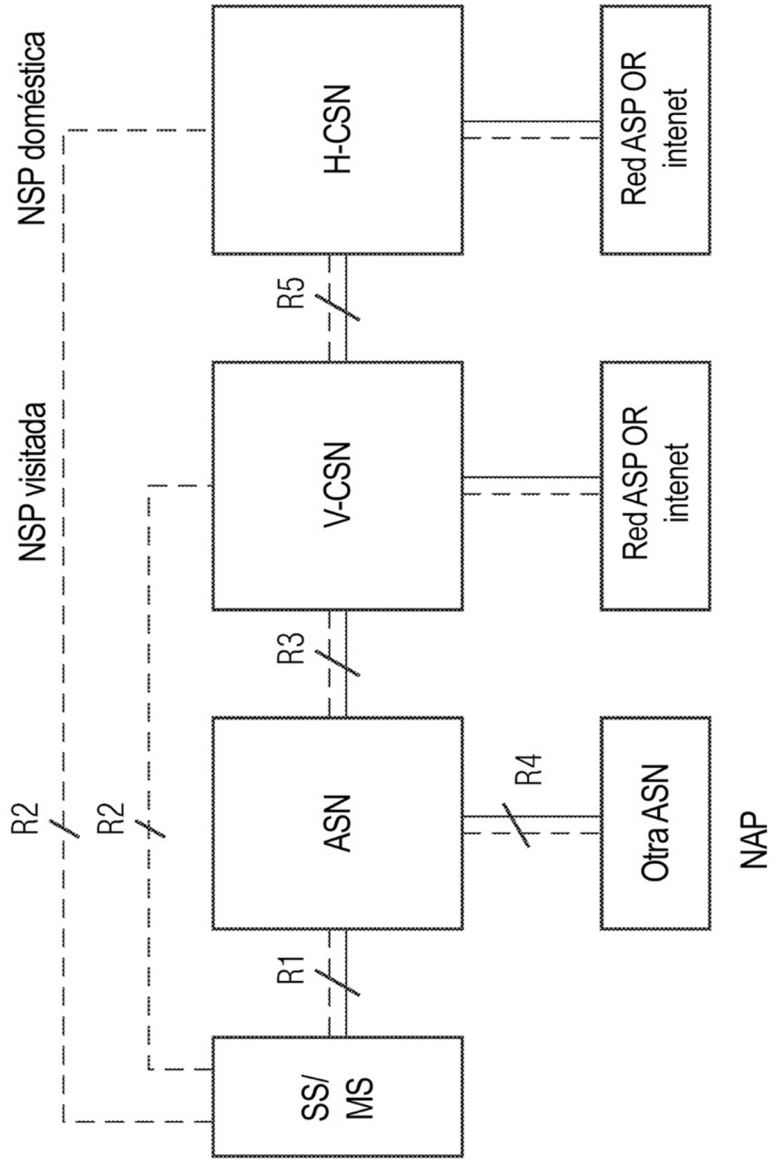
FIG 2

Estado de la técnica

Lista de visitantes

Dirección doméstica	Dirección de agente inicial	Dirección de medio	Duración
131.192.180.42	129.142.23.42	08-00-46-26-75-6A	100
213.123.24.140	172.23.142.49	00-02-B3-77-43-00	150
...	...	...	...

FIG 3
Estado de la técnica



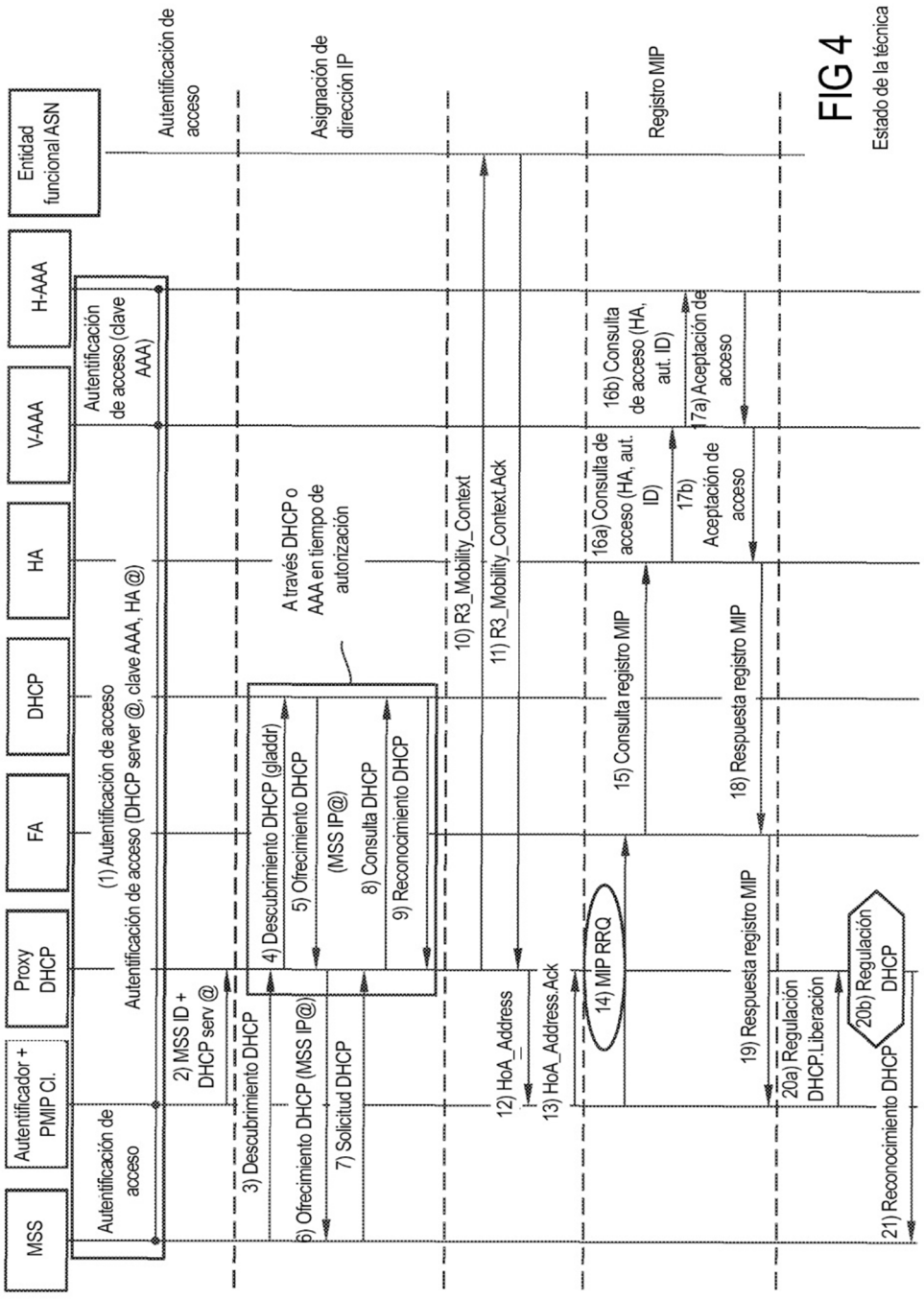


FIG 4
Estado de la técnica

FIG 5

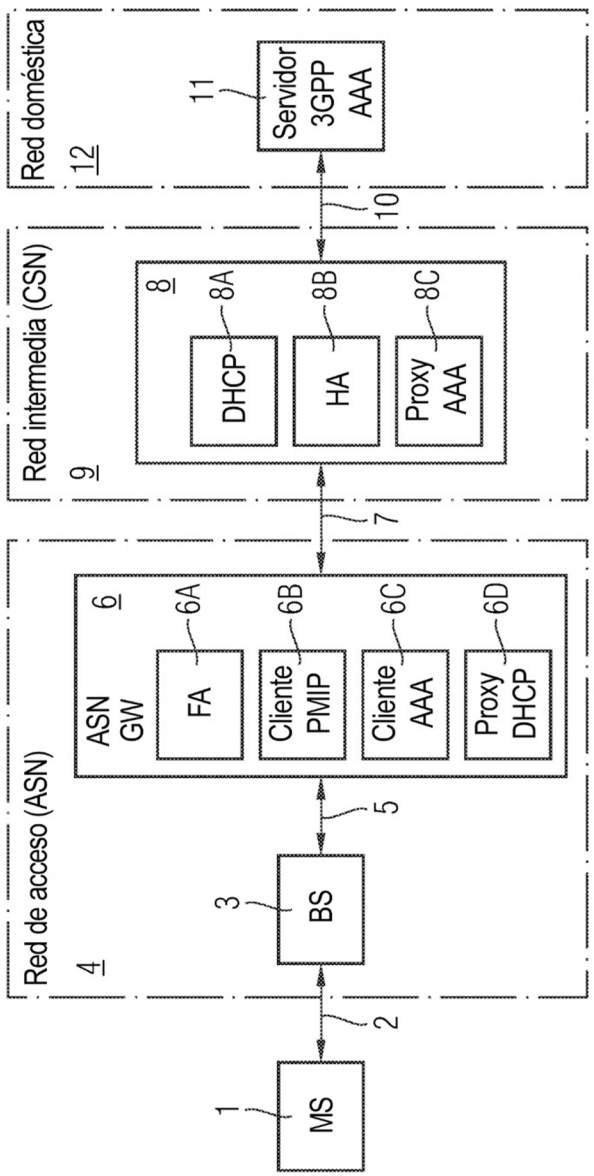

Red de acceso (ASN)
4
Red intermedia (CSN)
9
Red doméstica
12
MS
1
2
BS
3
5
ASN GW
6
6A
FA
6B
Cliente PMIP
6C
Cliente AAA
6D
Proxy DHCP
7
8
8A
DHCP
8B
HA
8C
Proxy AAA
10
11
Servidor 3GPP AAA

FIG 6

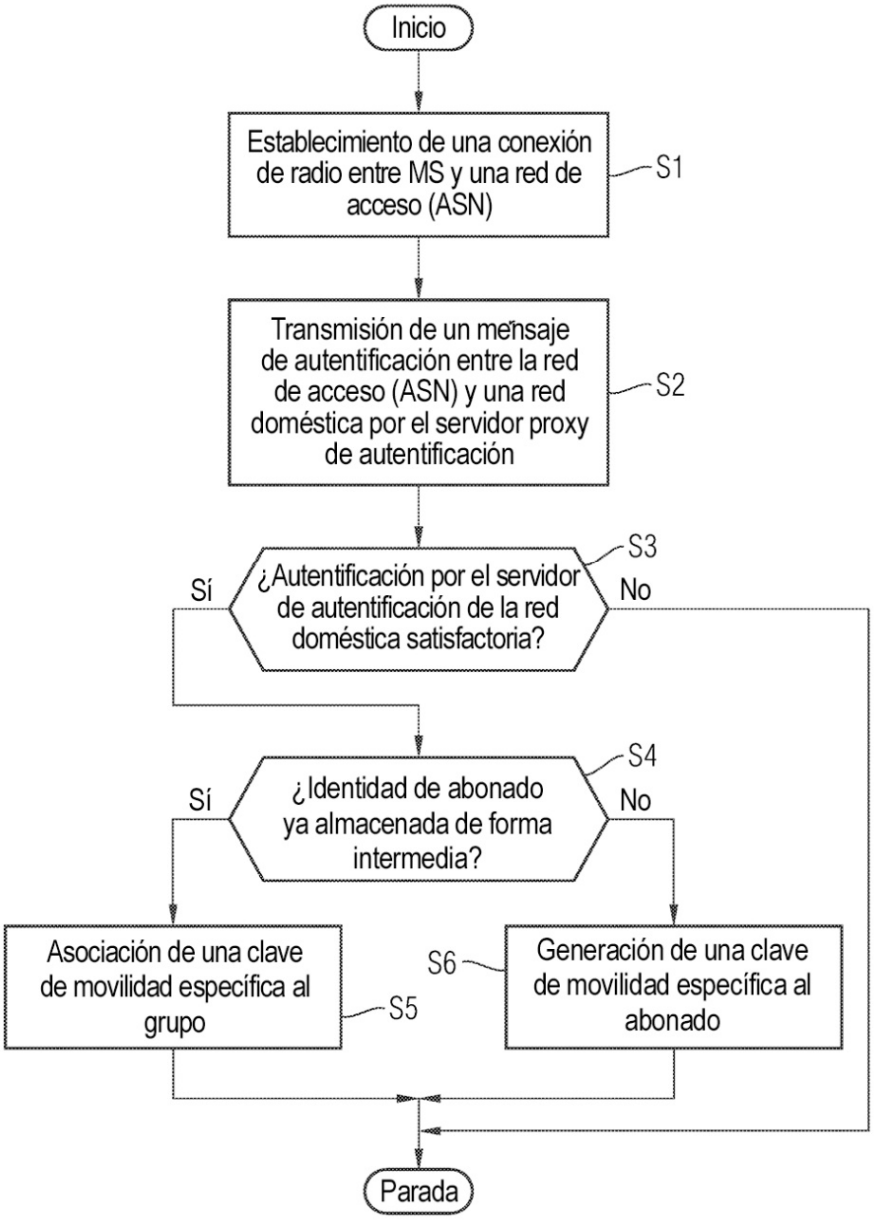

Inicio
Establecimiento de una conexión de radio entre MS y una red de acceso (ASN)
S1
Transmisión de un mensaje de autentificación entre la red de acceso (ASN) y una red doméstica por el servidor proxy de autentificación
S2
S3
¿Autentificación por el servidor de autentificación de la red doméstica satisfactoria?
Sí
No
S4
¿Identidad de abonado ya almacenada de forma intermedia?
Sí
No
Asociación de una clave de movilidad específica al grupo
S5
S6
Generación de una clave de movilidad específica al abonado
Parada

FIG 7

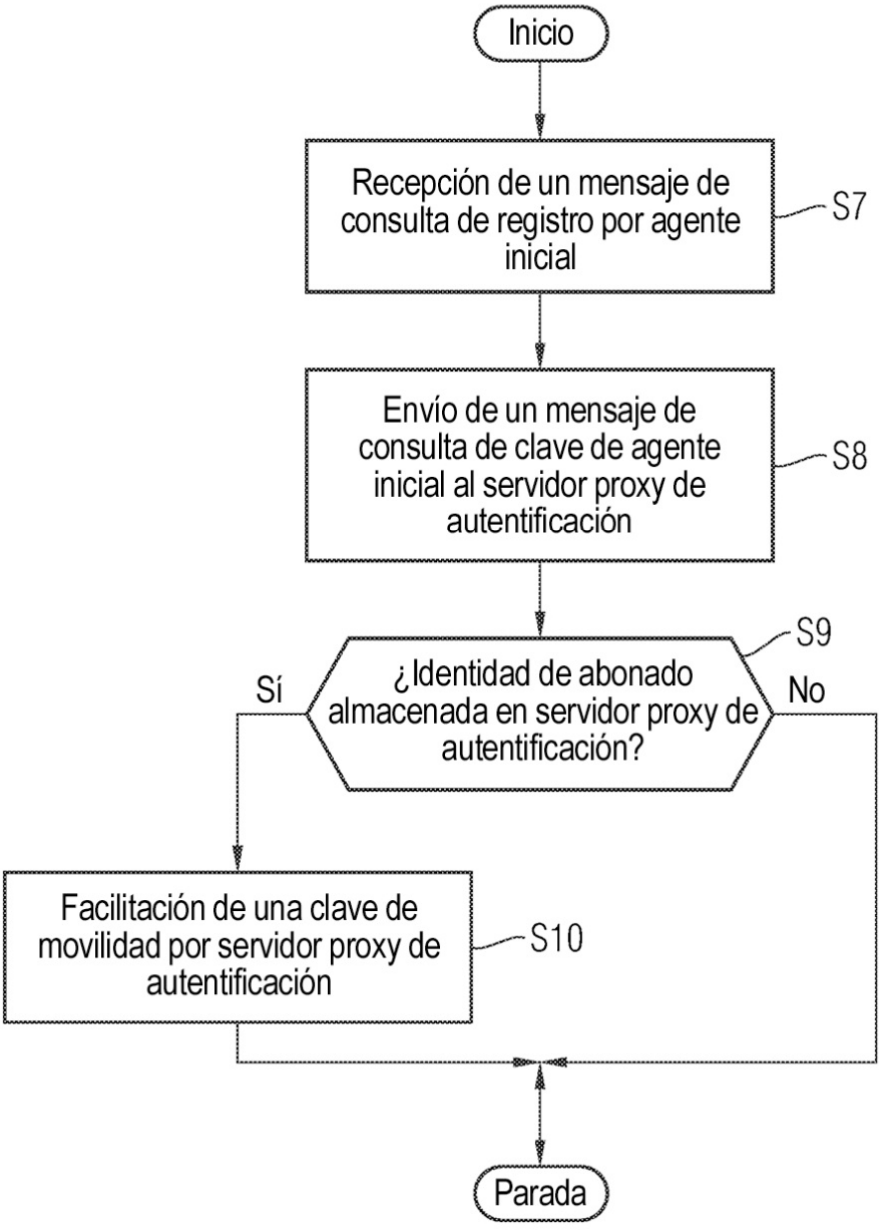

Inicio
Recepción de un mensaje de consulta de registro por agente inicial
S7
Envío de un mensaje de consulta de clave de agente inicial al servidor proxy de autentificación
S8
S9
¿Identidad de abonado almacenada en servidor proxy de autentificación?
Sí
No
Facilitación de una clave de movilidad por servidor proxy de autentificación
S10
Parada

FIG 8

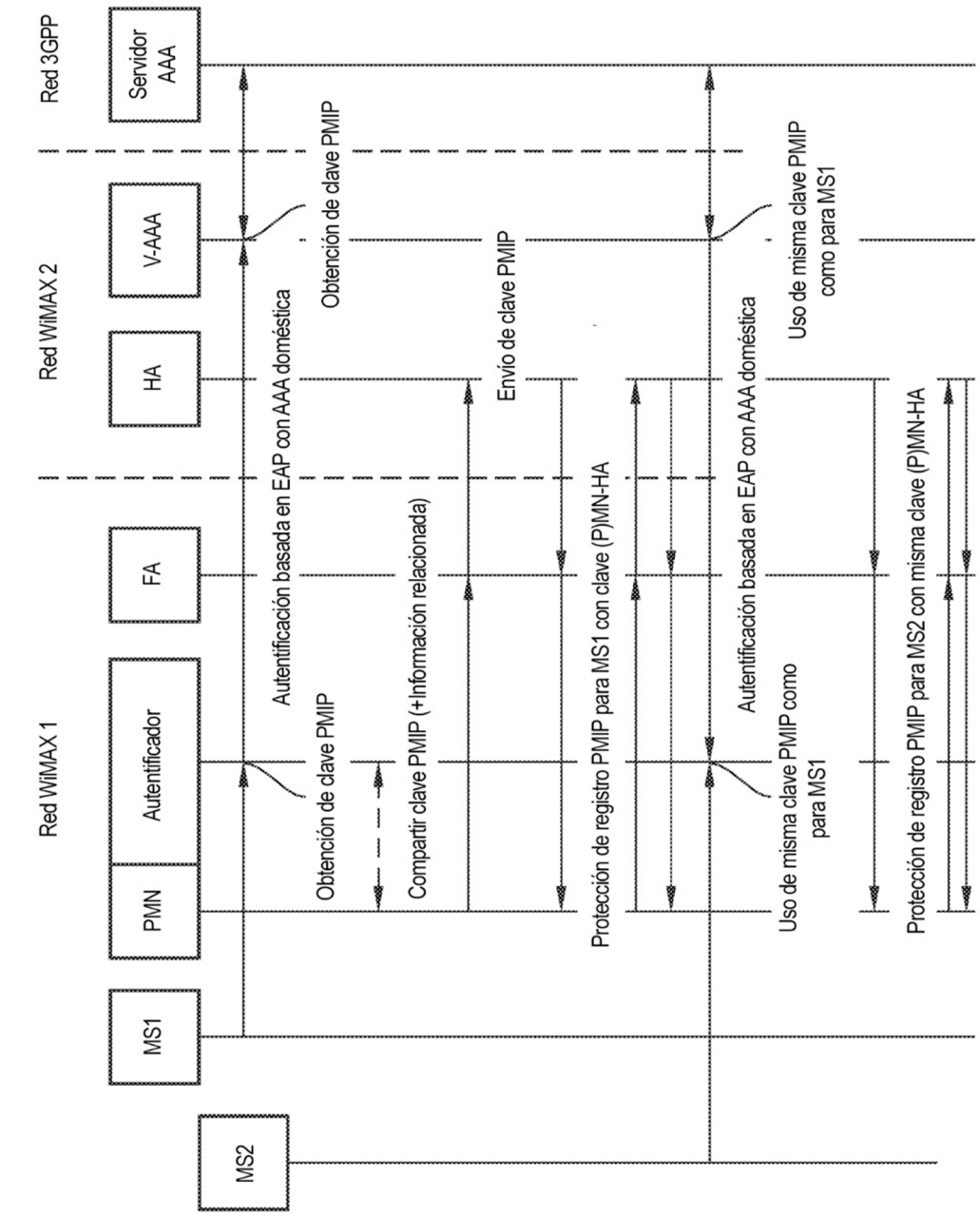

Red WiMAX 1
Red WiMAX 2
Red 3GPP
MS2
MS1
PMN
Autentificador
FA
HA
V-AAA
Servidor AAA
Autentificación basada en EAP con AAA doméstica
Obtención de clave PMIP
Obtención de clave PMIP
Compartir clave PMIP (+ Información relacionada)
Envío de clave PMIP
Protección de registro PMIP para MS1 con clave (P)MN-HA
Autentificación basada en EAP con AAA doméstica
Uso de misma clave PMIP como para MS1
Uso de misma clave PMIP como para MS1
Protección de registro PMIP para MS2 con misma clave (P)MN-HA

FIG 9

Identidad de abonado	Clave de movilidad	Tipo de clave	Sello de tiempo
user@vodafone.com	1 2 A F	Clave específica al grupo	17.2.2006 13^{10}
Glyn@isarpatent.com	1 4 B C	Clave específica al usuario	18.2.2006 9^{14}