(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 609 257**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/22 (2006.01)
H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04W 80/04 (2009.01)
H04W 88/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.08.2007 PCT/EP2007/058284**

(87) Fecha y número de publicación internacional: **21.02.2008 WO08019989**

(96) Fecha de presentación y número de la solicitud europea: **09.08.2007 E 07788345 (2)**

(97) Fecha y número de publicación de la concesión europea: **02.11.2016 EP 2052517**

(54) Título: **Procedimiento y sistema para proporcionar una clave específica de acceso**

(30) Prioridad:

14.08.2006 DE 102006038037

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.04.2017

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

FALK, RAINER;
HORN, GÜNTHER y
KRÖSELBERG, DIRK

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO Y SISTEMA PARA PROPORCIONAR UNA CLAVE ESPECÍFICA DE ACCESO

DESCRIPCIÓN

La invención se refiere a un procedimiento y a un sistema para proporcionar una clave específica de acceso para asegurar una transmisión de datos entre un aparato terminal móvil y un nodo de una red de acceso.

Internet, con el protocolo TCP/IP, ofrece una plataforma para el desarrollo de protocolos de niveles superiores para el ámbito móvil. Puesto que los protocolos de Internet están ampliamente difundidos, puede cubrirse con las correspondientes ampliaciones de protocolo para entornos móviles un gran círculo de usuarios. No obstante, los protocolos de Internet tradicionales no están concebidos en su origen para la utilización móvil. En la conmutación por paquetes de la Internet tradicional se intercambian los paquetes entre ordenadores fijos, que no modifican su dirección de red ni migran entre distintas subredes. En redes de radio con terminales y/u ordenadores móviles, se integran a menudo ordenadores móviles MS (Mobile Station, estación móvil) en diversas redes. El DCHP (Dynamic Host Configuration Protocol, protocolo de configuración dinámica del servidor central) posibilita, con ayuda del correspondiente servidor, la asignación dinámica de una dirección de IP y otros parámetros de configuración a un ordenador en una red. A un ordenador que está integrado en una red se le asigna automáticamente una dirección de IP libre mediante el protocolo DHCP. Cuando un ordenador móvil ha instalado DHCP, simplemente ha de entrar en la cobertura de una red local que apoya la configuración mediante el protocolo DHCP. En el protocolo DHCP es posible una adjudicación dinámica de direcciones, es decir, se asigna automáticamente para un período de tiempo determinado una dirección de IP libre. Una vez transcurrido ese tiempo, bien ha de formular de nuevo la consulta el ordenador móvil MS o bien otorgarse la dirección de IP de otra manera.

Con DHCP puede integrarse un ordenador móvil MS sin configuración manual en una red. Como premisa debe simplemente estar disponible un servidor DHCP. Un ordenador móvil MS puede así utilizar servicios de la red local y por ejemplo utilizar ficheros archivados centralmente. Pero si un ordenador móvil MS ofrece por sí mismo servicios, un potencial usuario de servicios no puede encontrar el ordenador móvil MS, ya que su dirección de IP se modifica en cada red en la que se integra el ordenador móvil. Lo mismo sucede cuando se modifica una dirección de IP durante un enlace TCP existente. Esto origina la interrupción del enlace. Por ello, para IP Móvil se asigna a un ordenador móvil MS una dirección de IP, que el mismo mantiene también en otra red. En el cambio de red de IP tradicional es necesario adaptar correspondientemente los ajustes de direcciones de IP. Una adaptación continua de mecanismos de IP y los mecanismos de configuración automáticos interrumpe el enlace existente cuando hay un cambio de la dirección de IP. El protocolo MIP (RFC2002, RFC2977, RFC3344, RFC3846, RFC3957, RFC3775, RFC3776, RFC4285), apoya la movilidad de aparatos terminales móviles. En los protocolos de IP tradicionales, debe adaptar el aparato terminal móvil MS cada vez su dirección de IP cuando cambia la subred de IP, para que los paquetes de datos direccionados hacia el aparato terminal móvil MS se enruten correctamente. Para mantener un enlace TCP existente, debe mantener el aparato terminal móvil MS su dirección de IP, ya que un cambio de dirección da lugar a una interrupción del enlace. El protocolo MIP posibilita un enlace transparente entre ambas direcciones, es decir, una dirección home (doméstica) permanente y una segunda dirección care-of (de custodia) temporal. La dirección care-of es la dirección de IP bajo la que el aparato terminal móvil MS es alcanzable en ese momento.

Un agente doméstico (Home Agent) HA representa al aparato terminal móvil MS cuando el aparato terminal móvil MS no se encuentra en la red doméstica inicial. El agente doméstico está informado continuamente sobre el lugar de estancia del ordenador móvil MS en ese momento. El agente doméstico HA es usualmente un componente de un enrutador en la red doméstica del aparato terminal móvil. Cuando el aparato terminal móvil MS se encuentra fuera de la red doméstica, pone a disposición el agente doméstico HA una función para que el aparato terminal móvil MS pueda registrarse. A continuación retransmite el agente doméstico HA los paquetes de datos direccionados hacia el aparato terminal móvil MS a la subred actual del aparato terminal móvil MS.

Un agente ajeno FA (Foreign Agent) FA se encuentra en la subred en la que se mueve el aparato terminal móvil MS. El agente ajeno FA retransmite los paquetes de datos que llegan al aparato terminal móvil MS o bien al ordenador móvil MS. El agente ajeno FA se encuentra en una llamada red ajena (Visited Network o red visitada). Usualmente el agente ajeno FA es igualmente un componente de un enrutador. El agente ajeno FA enruta todos los paquetes de datos móviles administrativos entre el aparato terminal móvil MS y su agente doméstico HA. El agente ajeno FA desempaqueta los paquetes de datos de IP tuneleados enviados por el agente doméstico HA y retransmite sus datos al aparato terminal móvil MS.

La dirección doméstica del aparato terminal móvil MS es una dirección bajo la cual puede alcanzarse permanentemente el aparato terminal móvil MS. La dirección doméstica tiene el mismo prefijo de dirección que el agente doméstico HA. La dirección care-of (de custodia) es aquella dirección de IP que utiliza el aparato terminal móvil MS en la red ajena.

El agente doméstico HA mantiene una llamada tabla de enlaces de movilidad (MBT: Mobility Binding Table). Las inscripciones en esta tabla sirven para asociar entre sí ambas direcciones, es decir, la dirección doméstica y la dirección care-of de un aparato terminal móvil MS y para derivar correspondientemente los paquetes de datos.

La tabla MBT contiene inscripciones sobre la dirección doméstica, la dirección care-of y una indicación sobre el periodo de tiempo durante el que esta asociación es válida (Life Time).

La figura 1 muestra un ejemplo de una tabla de enlaces de movilidad MBT según el estado de la técnica.

El agente ajeno FA contiene una lista de visitantes o Visitor List (VL: Visitor List) que contiene informaciones sobre los aparatos terminales móviles MS que se encuentran en ese momento en la red de IP del agente ajeno FA.

La figura 2 muestra un ejemplo de una tal lista de visitantes según el estado de la técnica.

Para que un ordenador móvil MS pueda integrarse en una red, debe informarse primeramente de si se encuentra en su red doméstica o en una red ajena. Adicionalmente, debe informarse el aparato terminal móvil MS de qué ordenador es el agente doméstico y el agente ajeno en la subred. Estas informaciones son averiguadas mediante el llamado Agent Discovery (descubridor de agentes).

Mediante el subsiguiente registro, puede comunicar el aparato terminal móvil MS su lugar de estancia actual a su agente doméstico HA. Para esto envía el ordenador móvil o el aparato terminal móvil MS al agente doméstico la dirección care-of actual. Para registrarse, envía el ordenador móvil MS una Registration Request o solicitud de registro al agente doméstico. El agente doméstico HA registra la dirección care-of en su lista y contesta con una Registration Reply o contestación de registro. Al respecto existe desde luego un problema de seguridad. Puesto que básicamente cada ordenador puede enviar a un agente doméstico HA una solicitud de registro, podría simulársele de manera sencilla a un agente doméstico HA que un ordenador se ha movido hasta otra red. Así podría un ordenador ajeno tomar todos los paquetes de datos de un ordenador móvil o aparato terminal móvil MS sin que un emisor se entere de ello. Para evitar esto, disponen el ordenador móvil MS y el agente doméstico HA de claves secretas comunes. Si retorna un ordenador móvil MS a su red doméstica, se da de baja del registro en el agente doméstico HA, ya que el ordenador móvil MS puede recibir ahora sin más todos los paquetes de datos por sí mismo. Una red de telefonía móvil debe presentar entre otras las siguientes características de seguridad. Las informaciones sólo deben hacerse accesibles a los interlocutores de comunicación deseados, es decir, los escuchas indeseados no deben tener acceso alguno a datos transmitidos. La red de telefonía móvil debe por lo tanto presentar la característica de la confidencialidad (confidentiality). Además de ello, debe existir autenticidad. La autenticidad (authenticity) permite a un interlocutor de comunicación detectar sin ninguna duda si se ha establecido una comunicación efectivamente con un interlocutor de comunicación deseado o si aparece un tercero ajeno como interlocutor de comunicación. Las autentificaciones pueden realizarse por cada mensaje o por cada enlace. Si se realiza la autentificación en base a enlaces, sólo se realiza la identificación una vez al comienzo de una sesión (session) de los interlocutores de comunicación. En el transcurso de la sesión a continuación se da por supuesto que los siguientes mensajes seguían procediendo del correspondiente emisor. Incluso cuando ya está determinada la identidad de un interlocutor de comunicación, es decir, el interlocutor de comunicación está autentificado, puede presentarse el caso de que este interlocutor de comunicación no deba acceder a todos los recursos o bien no deba utilizar todos los servicios a través de la red. La correspondiente autorización presupone en este caso una autentificación previa del interlocutor de comunicación.

En redes de datos móviles deben recorrer los mensajes largos trayectos a través de interfaces de aire y son así fácilmente alcanzables por potenciales atacantes. En redes de datos móviles e inalámbricas juegan por lo tanto los aspectos de seguridad un papel especial. Un medio esencial para aumentar la seguridad en redes de datos son las técnicas de codificación. Mediante la codificación es posible transmitir datos a través de vías de comunicación inseguras, por ejemplo a través de interfaces de aire, sin que terceros no autorizados tengan acceso a los datos. Para la codificación se transforman los datos, es decir, el llamado texto explícito, con ayuda de un algoritmo de codificación en texto cifrado (chiffre). El texto codificado puede transportarse a través del canal de transmisión inseguro y a continuación decodificarse o descifrarse.

Como tecnología de acceso inalámbrico muy prometedora se propone WiMax (Worldwide Interoperability for Microwave Access, interoperabilidad a nivel mundial para acceso por microondas) como nuevo estándar, que para la transmisión por radio utiliza IEEE 802.16. Con WiMax debe cubrirse con estaciones emisoras una zona de hasta 50 km con velocidades de datos superiores a 100 MBits por segundo.

La figura 3 muestra un modelo de referencia para una red de radio WiMax. Un aparato terminal móvil MS se encuentra en la zona 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 de servicio de conectividad visitada) o red intermedia con una red doméstica HCSN (Home Connectivity Service Network, red de servicio de conectividad doméstica). Las distintas redes están conectadas entre sí mediante interfaces o bien puntos de referencia R. El agente doméstico HA de la estación móvil MS se encuentra en la red doméstica (HCSN) o en una de las redes visitadas (VCSN).

WiMax apoya dos variantes de realización de IP móviles, la llamada Client MIP (CMIP, MIP cliente), en la que la propia estación móvil MS realiza la función de cliente MIP y Proxy-MIP (PMIP), en la que la función MIP-Client está realizada mediante la red de acceso WiMax ASN. La funcionalidad prevista para ello en la ASN se denomina Proxy Mobile Node (PMN) o PMIP-Client. De esta manera puede utilizarse MIP también con estaciones móviles MS que por sí mismas no apoyan ningún MIP.

La figura 4 muestra el establecimiento de un enlace en Proxy-MIP (PMIP) cuando el agente doméstico HA se encuentra en la red visitada VCSN, según el estado de la técnica.

Tras establecerse un enlace por radio entre el aparato terminal móvil MS y una estación de base BS, tiene lugar primeramente una autentificación del acceso. La función de la autentificación, de la autorización y de la contabilidad se realiza mediante los llamados servidores AAA (AAA: Authentication, Authorization and Accounting). Entre el aparato terminal móvil MS y el servidor AAA de la red doméstica (HAAA) se intercambian mensajes de autentificación, mediante los cuales se obtienen la dirección del agente doméstico HA y una clave de autentificación. El servidor de autentificación en la red doméstica contiene los datos del perfil del abonado. El servidor AAA recibe un mensaje de consulta de autentificación, que contiene una identidad del abonado del aparato terminal móvil. El servidor AAA genera, una vez realizada con éxito la autentificación de acceso, una clave MSK (MSK: Master Session Key, clave maestra de sesión) para proteger el tramo de transmisión de datos entre el aparato terminal móvil MS y la estación de base BS de la red de acceso ASN. Esta clave MSK es transmitida por el servidor AAA de la red doméstica a través de la red intermedia CSN a la red de acceso ASN.

Tras la autentificación de acceso, tal como puede observarse en la figura 4, se configura el servidor DHCP-Proxy en la red de acceso ASN. En el caso de que la dirección de IP y la configuración host (del servidor central) ya estén contenidas en el mensaje de respuesta AAA, se descarga toda la información en el servidor DCHP-Proxy.

Tras realizarse la autentificación y la autorización con éxito, envía la estación móvil o el aparato terminal móvil MS un mensaje DHCP Discovery (descubridor) y se realiza una asignación de direcciones de IP.

Cuando se integra un aparato terminal móvil MS en una red, posiblemente tenga que poder informarse el aparato terminal móvil MS de si se encuentra en una red doméstica o en una red ajena. Además, debe informarse el aparato terminal móvil MS de qué ordenador es el agente doméstico o el agente ajeno en la correspondiente red. Estas informaciones se averiguan mediante el llamado Agent Discovery (descubridor de agentes). Hay dos tipos de Agent Discovery, a saber, los llamados Agent Advertisement (anuncio de agente) y Agent Solicitation (solicitud de agente).

En el Agent Advertisement envían los agentes, es decir, los agentes domésticos o agentes ajenos, periódicamente mensajes de broadcast (difusión general) a todos los ordenadores o aparatos terminales móviles de la subred. Cada ordenador que en un determinado espacio de tiempo escucha los mensajes de broadcast, puede identificar así los agentes en la correspondiente subred.

Si se activa de nuevo un aparato terminal móvil MS, en general no es práctico esperar al siguiente Agent Advertisement. El aparato terminal móvil MS debe saber inmediatamente en qué subred se encuentra en ese momento. En la llamada Agent Solicitation, envía por lo tanto el aparato terminal móvil MS una solicitud a todos los ordenadores de la correspondiente subred de realizar un Agent Advertisement. El aparato terminal móvil MS puede forzar mediante Agent Solicitation que se den a conocer inmediatamente los agentes, con lo que el tiempo de espera se acorta considerablemente. También se realiza una Agent Solicitation cuando falta el Agent Advertisement, por ejemplo cuando hay una pérdida de un paquete (Packet Loss) o un cambio de red. Con ayuda del Agent Discovery puede detectar también un aparato terminal móvil MS si se encuentra en su red doméstica o en una red ajena. En base a la información del paquete dentro de un mensaje de Agent Advertisement, detecta el aparato terminal móvil MS su agente doméstico HA. Si recibe el aparato terminal móvil MS paquetes de mensajes de una red ajena, entonces puede detectar adicionalmente si su lugar de estancia se ha modificado desde el último Advertisement. Si no recibe el aparato terminal móvil MS ningún mensaje de Advertisement, entonces supone el aparato terminal móvil MS a priori que se encuentra en la red doméstica y que el agente doméstico HA está averiado. El aparato terminal móvil MS intenta entonces tomar contacto con el enrutador de la red, para confirmar esta suposición. Si no se encuentra el aparato terminal móvil MS en su red doméstica, intenta a continuación alcanzar un servidor DHCP y recibir una dirección de la subred. Si esto se realiza con éxito, utiliza el aparato terminal móvil MS esta dirección como la llamada dirección Colocated Care-of (de custodia de reubicación) y toma contacto con el agente doméstico HA. La dirección Colocated Care-of es una dirección asignada al aparato terminal móvil MS en la red ajena, que también se transmite al agente doméstico HA.

Se distingue entre gestión de movilidad basada en la red (PMIP) y gestión de movilidad basada en aparatos terminales (CMIP). En la gestión de movilidad basada en aparatos terminales CMIP apoya al aparato terminal IP Móvil (MIP).

La figura 4 muestra el establecimiento del enlace en una gestión de movilidad tradicional basada en la red (PMIP), mientras que la figura 5 representa el establecimiento de un enlace en una gestión de movilidad tradicional basada en aparatos terminales (CMIP).

Al establecerse un enlace entre el aparato terminal móvil MS y la red, envía el servidor de autentificación de la red doméstica (H-AAA), una vez realizada con éxito la autentificación del abonado, un mensaje de confirmación de autentificación (SUCCESS). El mensaje de confirmación de autentificación señaliza al cliente de la autentificación que la autentificación del abonado ha terminado con éxito.

En el Proxy-MIP o gestión de movilidad basada en la red (PMIP) no apoya el aparato terminal IP Móvil o bien el correspondiente software MIP no está activado en el aparato terminal móvil MS.

Por el contrario, en el Client-MIP (CMIP) o en la gestión de movilidad basada en aparatos terminales viene apoyado el Mobile-IP por el correspondiente aparato terminal o bien la estación móvil MS.

En el Proxy-MIP detecta el aparato terminal móvil MS sólo una dirección de IP asignada por el servidor DHCP. La dirección care-of del aparato terminal móvil MS no es conocida por aparato terminal móvil MS, sino por el cliente PMIP, el agente ajeno FA, así como el agente doméstico HA. Por el contrario, detecta el aparato terminal móvil MS en el Client-MIP sus dos direcciones de IP, es decir, tanto la dirección doméstica (Home Address) como también la dirección care-of (de custodia).

Tal como puede observarse en las figuras 4, 5, tiene lugar tras la asignación de direcciones de IP un registro MIP. En el registro MIP es informado el agente doméstico HA sobre el lugar actual de estancia del aparato terminal móvil MS. Para su registro, envía el aparato terminal móvil MS o bien el correspondiente cliente PMIP una solicitud de registro a un agente doméstico HA, que contiene la dirección care-of actual. El agente doméstico HA inscribe la dirección care-of en una lista gestionada por él mismo y contesta con una respuesta de registro (Registration Reply). Puesto que básicamente todo ordenador puede enviar a un agente doméstico HA una solicitud de registro, puede simulársele de manera sencilla a un agente doméstico HA que un ordenador o un aparato terminal móvil MS se ha movido hasta otra red. Para evitar esto, dispone tanto el aparato terminal móvil MS como también el agente doméstico HA de una clave secreta común, es decir, una llamada clave móvil IP (MIP-KEY).

En el Proxy-MIP (PMIP) se transmite la solicitud de registro (MIPRRQ) de un cliente PMIP dentro de la red de acceso ASN a través de un agente ajeno FA al agente doméstico HA. El agente doméstico HA se hace asignar por el correspondiente servidor de autentificación H-AAA una clave para el abonado y transmite ésta con la respuesta de registro MIP (MIP Registration Reply), tal como se representa en la figura 4.

En la gestión de movilidad basada en aparatos terminales (CMIP), se dirige el mensaje de solicitud de registro (MIPRRQ) directamente desde el aparato terminal móvil MS a través del agente ajeno FA al agente doméstico HA, tal como se representa en la figura 5.

En redes de acceso WiMax se utiliza, junto a Mobile-IP (CMIP) también Proxy-Mobile-IP (PMIP), para permitir una gestión de movilidad para clientes que no disponen por sí mismos de ninguna funcionalidad Mobile-IP-Client. En PMIP se prevé en la red de acceso un Proxy-Mobile-IP-Client, que asume la señalización MIP en representación del cliente. Estos protocolos de movilidad se utilizan en WiMax para una transferencia (handover) entre dos redes de acceso ASN o bien entre dos proveedores de red de acceso NAP. El correspondiente agente doméstico WiMax puede encontrarse entonces a elección en una red doméstica WiMax HCSN o en una red WiMax visitada (VCSN). En WiMax se presupone que en la red doméstica HCSN se encuentra un servidor doméstico AAA, que conoce la clave criptográfica compartida con el usuario a largo plazo, así como otros parámetros de utilización.

Durante el registro consulta el agente doméstico WiMax en el servidor AAA doméstico WiMax parámetros de seguridad, por ejemplo claves criptográficas temporales. Éstas se necesitan para que sólo pueda registrarse un cliente autorizado en el agente doméstico y para proteger la señalización MIP. Como parte del protocolo de autentificación y acuerdo de claves, que ejecuta el aparato terminal móvil con el servidor de autentificación puede deducir también el aparato terminal móvil estos parámetros de seguridad. Entonces se deduce y aporta en una red de acceso WiMax, a partir de la llamada clave EMSK (Extended Master Session Key, clave de sesión maestra ampliada) un AMSK o bien Mobile-IP-Root-Key (MIP-RK, clave de raíz de IP móvil). A partir de esta Mobile-IP-Root-Key se deducen a continuación otras claves para proteger las distintas secciones de comunicación entre el nodo móvil y/o el agente ajeno FA y el agente doméstico HA. Las distintas variantes de Mobile-IP como Mobile-IP V6 y Mobile-IP V4 se deducen entonces en cada caso mediante una clave propia para el caso Client-Mobile-IP y el caso Proxy-Mobile-IP.

En redes de acceso WiMax tradicionales no se apoya un interworking (interacción) o colaboración con otras redes.

La figura 6 muestra la interacción entre una red de acceso WiMax y una red doméstica 3GPP según el estado de la técnica. Tal como puede observarse en la figura 6, está previsto en la red de acceso WiMax un servidor proxy de autentificación (A-AA-Relay), que presenta una Interworking-Unit (unidad de interacción) IWU como interfaz con la red doméstica 3GPP. El servidor proxy de autentificación asume en el caso de la interacción con la red 3GPP la generación de claves y la deducción de claves, que es necesaria en el marco del registro en la red del abonado, para activar para el abonado o bien el aparato terminal móvil Proxy-Mobile-IP. En el Proxy-Mobile-IP se encuentra un Proxy-Mobile-IP-Client en la pasarela (gateway) ASN o bien servidor proxy de autentificación de la red doméstica WiMax WiMax-CSN. Esta red doméstica WiMax WiMax-CSN está conectada con la red 3GPP, tal como puede verse en la figura 6. En el Proxy-Mobile-IP es por lo tanto posible que la unidad de interworking IWU genere una clave Mobile-IP (MIP-Key) en el registro en la red, para asegurar la sección entre el Proxy-Mobile-IP-Client y el agente doméstico. El Proxy-Mobile-IP-Client se encuentra entonces con preferencia en la pasarela ASN y forma así parte de la infraestructura de acceso. Por lo tanto no es necesario en el Proxy-Mobile-IP modificar el servidor de autentificación 3GPP o bien el servidor de autentificación 3GPP no tiene que cumplir las especificaciones de la red de acceso WiMax.

En el Client-Proxy-Mobile-IP no se apoya desde luego una interacción entre la red de acceso WiMax y la red doméstica 3GPP. No existe actualmente ningún protocolo adecuado para retransmitir parámetros de seguridad al cliente o bien al aparato terminal móvil. La razón de ello reside en que el aparato terminal móvil deduce estos parámetros de seguridad en la forma de proceder tradicional a partir del protocolo de autentificación y acuerdo de claves.

El documento WO2004/049672, considerado como el estado más próximo de la técnica, da a conocer un procedimiento para proporcionar una clave para asegurar una transmisión de datos entre el aparato terminal móvil y una red de acceso, deduciendo el aparato terminal y la red de acceso las claves independientemente una de otra a partir de datos del servidor de autentificación.

Es por ello el objetivo de la presente invención lograr un procedimiento y un sistema para proporcionar una clave específica de acceso para asegurar una transmisión de datos entre un aparato terminal móvil y un nodo de una red de acceso, que también permitan Client-IP (CMIP) cuando el servidor de autentificación de la red doméstica no apoye una gestión de movilidad (Mobility-Management). La invención logra un procedimiento para proporcionar una clave específica de la red de acceso para asegurar una transmisión de datos entre un aparato terminal móvil y un nodo de una red de acceso, generando en una autentificación del aparato terminal móvil un servidor de autentificación una clave de sesión, de la que se deriva una clave de base y se transmite a un Interworking-Proxy-Server (servidor intermediario de interacción), que a partir de la clave de base transmitida deduce la clave específica de la red de acceso y la proporciona al nodo de la red de acceso.

En una forma de realización preferente del procedimiento correspondiente a la invención, se constituye la clave de sesión mediante una MSK (Master Session Key, clave de sesión maestra) o una EMSK (Extended Master Session Key, clave de sesión maestra ampliada).

En el procedimiento correspondiente a la invención se incluye así una Master Session Key local (MSK o bien EMSK), que por razones de seguridad no debe abandonar el servidor de autentificación (AAA) de la red doméstica, para deducir de ello una pseudo-clave o clave de base, que a continuación se transmite a un Interworking-Proxy-Server, deduciendo el Interworking-Proxy-Server a partir de la clave de base recibida la necesaria clave específica de acceso en función de la jerarquía de claves predeterminada y la proporciona para el correspondiente nodo de la red de acceso.

En una forma de realización del procedimiento correspondiente a la invención se encuentra el servidor de autentificación en una red doméstica del aparato terminal móvil.

En una forma de realización del procedimiento correspondiente a la invención se deduce la clave de base a partir de la clave de sesión mediante una primera función de derivación predeterminada.

Esta primera función de derivación se forma con preferencia mediante una función de derivación HMAC-SHA1, HMAC-SHA256, HMAC-MD5, SHA1, SHA256 o una función de derivación MD5.

En una forma de realización preferente del procedimiento correspondiente a la invención se realiza la derivación de la clave de base en función de la clave de sesión y de una cadena de caracteres (string).

En una forma de realización del procedimiento correspondiente a la invención se realiza la autentificación del aparato terminal móvil en el servidor de autentificación mediante un protocolo EAP.

En otra forma de realización del procedimiento correspondiente a la invención se realiza la autentificación del aparato terminal móvil en el servidor de autentificación mediante un protocolo UMTS-AKA.

En una forma de realización alternativa del procedimiento correspondiente a la invención se realiza la autentificación del aparato terminal móvil en el servidor de autentificación mediante un protocolo HTTP-Digest-AKA.

En otra forma de realización del procedimiento correspondiente a la invención se realiza la transmisión de datos entre el servidor de autentificación y el Interworking-Proxy-Server mediante un protocolo de diámetro (Diameter) o un protocolo de radio (Radius).

En una forma de realización preferente del procedimiento correspondiente a la invención se forma la red de acceso mediante una red WiMax.

En una forma de realización preferente del procedimiento correspondiente a la invención se forma la red doméstica mediante una red 3GPP.

En una forma de realización preferente del procedimiento correspondiente a la invención se deduce a partir de la clave de base transmitida a través del Interworking-Proxy-Server mediante una segunda función de derivación una clave Mobile-IP-Root-Key.

Entonces se forma la segunda función de derivación con preferencia mediante una función de derivación HMAC-SHA1, HMAC-SHA256, HMAC-MD5, SHA1, SHA256 o una función de derivación MD5.

En una forma de realización preferente del procedimiento correspondiente a la invención se deduce a partir de la Mobile-IP-Root-Key deducida mediante una tercera función de derivación la clave específica de acceso para asegurar una transmisión de datos entre el aparato terminal móvil y el nodo de una red de acceso.

Esta tercera función de derivación es con preferencia una función de derivación HMAC-SHA1, HMAC-SHA256, HMAC-MD5, SHA1, SHA256 o una función de derivación MD5.

En una forma de realización del procedimiento correspondiente a la invención se deduce para las distintas secciones de transmisión de datos entre el nodo de la red de acceso y el aparato terminal móvil en cada caso una clave correspondiente específica del acceso.

En una forma de realización del procedimiento correspondiente a la invención genera el aparato terminal móvil en la autentificación igualmente la clave de sesión y deduce de la misma la clave específica de acceso.

La invención logra además un servidor de autentificación para proporcionar una clave de base, a partir de la que puede deducirse una clave específica de acceso para asegurar una sección de transmisión de datos entre un aparato terminal móvil y un nodo de una red de acceso, generando el servidor de autentificación en una autentificación del aparato terminal móvil una clave de sesión y deduciendo de ella mediante una función de derivación la clave de base y proporcionándola a un Interworking-Proxy-Server.

La invención logra además un Interworking-Proxy-Server para proporcionar una clave específica del acceso para asegurar una transmisión de datos entre un aparato terminal móvil y un nodo de una red de acceso, deduciendo el Interworking-Proxy-Server a partir de una clave de base transmitida por un servidor de autentificación la clave específica de la red de acceso y proporcionándola al nodo de la red de acceso.

La invención logra además un sistema de transmisión de datos con varias redes de acceso y al menos una red doméstica del aparato terminal móvil, generando un servidor de autentificación de la red doméstica cuando se autentifica un aparato terminal móvil una clave de sesión y deduciendo de la misma una clave de base común, que se transmite a las redes de acceso que disponen de respectivos Interworking-Proxy-Server, deduce la clave específica de acceso, de las que al menos hay una, a partir de la clave de base transmitida, que está prevista en cada caso para asegurar una sección de transmisión de datos entre el aparato terminal móvil y un nodo de la correspondiente red de acceso.

A continuación se describirán formas de realización preferentes del procedimiento correspondiente a la invención y del sistema correspondiente a la invención para proporcionar la clave específica de la red de acceso para asegurar una transmisión de datos entre un aparato terminal móvil y un nodo de una red de acceso con referencia a las figuras adjuntas para explicar características esenciales de la invención.

Se muestra en:

figura 1 una tabla de registros de movilidad según el estado de la técnica;
figura 2 una lista de visitantes según el estado de la técnica;
figura 3 un modelo de referencia para una red de radio WiMax;
figura 4 el establecimiento de un enlace en Proxy-Mobile-IP (PMIP) según el estado de la técnica;
figura 5 el establecimiento de un enlace en Client- CMIP (CMIP) según el estado de la técnica;
figura 6 un diagrama de bloques para representar la interacción (interworking) entre una red de acceso WiMax y una red 3GPP según el estado de la técnica;
figura 7 un diagrama secuencial con una posible forma de realización del sistema correspondiente a la invención para proporcionar una clave específica de la red de acceso;
figura 8 un diagrama de señales para representar una forma posible de realización del procedimiento correspondiente a la invención para proporcionar una clave específica de la red de acceso;
figura 9 otro diagrama de señales para representar una forma posible de realización del procedimiento correspondiente a la invención para proporcionar una clave específica de la red de acceso.

La figura 7 muestra una arquitectura de red en la que puede aplicarse el procedimiento correspondiente a la invención para proporcionar una clave específica de la red de acceso. Un aparato terminal móvil 1 (MS = Mobile Station, estación móvil) está conectado a través de una interfaz R1 a una red de acceso 2 (ASN = Access Service Network, red de servicio de acceso). La red de acceso 2 está conectada a través de una interfaz R3 a una red visitada 3(VVCSN = Visited Connectivity Service Network, red de servicio de conectividad visitada). Esta red visitada 3 está conectada a su vez a través de una interfaz R5 con una red doméstica 4 (HCSN = Home Connectivity Service Network, red de servicio de conectividad doméstica).

Si se mueve el aparato terminal móvil 1 desde una primera red de acceso 2 hasta una segunda red de acceso 2', se realiza una transferencia (handover) entre la primera y la segunda red de acceso. Esta transferencia (handover) se denomina en la especificación WiMax "Macro Mobility Management" (macrogestión de movilidad) o también "R3 Mobility" o bien "Inter ASN Mobility". La red visitada 3 y la red doméstica 4 están conectadas en cada caso a una red de un Access Service Provider (ASP, proveedor de servicios de acceso) o a Internet.

Cada red de acceso 2 incluye varias estaciones de base 6, que a su vez están conectadas a través de una interfaz R6 a un nodo de pasarela ASN (ASN-Gateway) 5. El nodo de pasarela ASN 5 representado en la figura 6 incluye un autentificador 5A, un agente ajeno MIP 5B y opcionalmente un PMIP-Client 5C, así como opcionalmente una Interworking-Proxy-Unit (unidad intermediaría de interacción) 7. En cada red visitada 3 se encuentra un servidor AAA 3A, tal como se representa en la figura 6. En la red doméstica 4 se encuentra igualmente un servidor de

autentificación 4A, así como un agente doméstico 4B. En una posible forma de realización alternativa se encuentra la Interworking-Proxy-Unit 7 en la red doméstica 4.

Por el lado del aparato terminal móvil 1 hay que distinguir dos casos. El propio aparato terminal móvil 1 apoya Mobile IP y presenta un CMIP-Client propio o el aparato terminal móvil 1 no apoya Mobile IP y necesita un PMIP-Client 5C en el nodo de pasarela (gateway) 5 de la red de acceso 2.

La figura 8 muestra un diagrama de señales para describir una forma posible de realización del procedimiento correspondiente a la invención, encontrándose la Interworking-Unit 7 en una primera forma de realización en la red de acceso 2 o en una forma de realización alternativa en la red doméstica 4. En el procedimiento correspondiente a la invención se proporciona una clave específica de la red de acceso para asegurar una transmisión de datos entre el aparato terminal móvil 1 y cualquier nodo de la red de acceso 2, generando en la autentificación del aparato terminal móvil 1 el servidor de autentificación 4A, que se encuentra en la red doméstica del aparato terminal móvil 4, una clave de sesión y deduciendo de esta clave de sesión una clave de base, que se transmite al Interworking-Proxy-Server 7, como el representado en la figura 7. El Interworking-Proxy-Server 7 deduce de la clave de base recibida la necesaria clave específica del acceso mediante una función de derivación y la proporciona para el correspondiente nodo de la red de acceso 2. La clave de sesión, de la que se deduce la clave de base transmitida, es en una forma de realización una MSK(Master Session Key, clave de sesión maestra) o una EMSK (Extended Master Session Key, clave de sesión maestra ampliada). Tal como se representa en la figura 8, deduce el servidor de autentificación 4A una pesudo-clave EMSK y/o una clave de base común mediante una función de derivación HMAC-SHA1 a partir de la Extended Master Session Key EMSK. En una forma de realización alternativa se forma esta función de derivación mediante una función de derivación HMAC-SHA256, una función de derivación HMAC-MD5, una función de derivación SHA1, una función de derivación SHA256 o una función de derivación MD5. La clave de base o pseudo-clave deducida se transmite en un mensaje EAP-Success junto con la Master Session Key MSK a la Interworking-Unit 7, que por ejemplo está configurada como Interworking-Proxy-Server.

En una forma de realización posible del procedimiento correspondiente a la invención se realiza la deducción de la clave de base y/o de la pseudo-clave PEMSK en función de la clave de sesión MSK y/o EMSK y adicionalmente de una cadena de caracteres o String, es decir, según una de las variantes:

PEMSK = H(MSK, EMSK, "String"),
PEMSK = H(MSK, "String"),
PEMSK = H(EMSK, "String").

En el ejemplo de realización representado en la figura 8 se realiza la autentificación del aparato terminal móvil 1 mediante un protocolo de transmisión de datos EAP. En una forma de realización alternativa se realiza la autentificación del aparato terminal móvil en un servidor de autentificación 4A mediante un protocolo UMTS-AKA o mediante un protocolo HTTP-Digest-AKA. La transmisión de datos entre el servidor de autentificación 4A y el Interworking-Proxy-Server 7 se realiza con preferencia mediante un protocolo Diameter o Radius.

La clave de base o pseudo-clave deducida es una etapa intermedia en la jerarquía de claves. Esta clave de base puede enviarse como clave de base común también a diversos Interworking-Proxy-Server 7, que están previstos en diversas redes de acceso 2. Las redes de acceso 2 son por ejemplo redes WiMax. La red doméstica 4 en la que se encuentra el servidor de autentificación 4A, es por ejemplo una red 3GPP.

Tan pronto como el Interworking-Proxy-Server 7, tal como puede verse en la figura 8, ha recibido la clave de base PEMSK transmitida, forma el mismo mediante una segunda función de derivación una Mobile-IP-Root-Key IMP-RK. En la segunda función de derivación pueden formarse igualmente una función de derivación HMAC-SHA1, HMAC-SHA256, HMAC-MD5, SHA1, SHA256 o una función de derivación MD5. En otras formas de realización pueden utilizarse también otras funciones de derivación o bien funciones de derivación de clave (Key-Derivation-Functions) KDF. De una Mobile-IP-Root-Key MIP-RK así deducida pueden deducirse en función de la jerarquía de claves otras claves específicas de la red de acceso para asegurar una transmisión de datos entre el aparato terminal móvil 1 y un nodo de la red de acceso 2. También esta tercera función de derivación puede ser por ejemplo una función de derivación HMAC-SHA1, HMAC-SHA256, HMAC-MD5, SHA1, SHA256 o una función de derivación MD5.

La Mobile-IP-Root-Key MIP-RK se utiliza para a partir de la misma generar claves de aplicación y/o claves específicas de la red de acceso, por ejemplo:

MN.-HA-MIP4 = H (MIP-RK, "String" |HA-IP)
MN-HA-CMIP6 = H(MIP-RK, "String" |HA-IP)
MN-FA = H(MIP-RK, "String" |FA-IP) y
FA-H = H(MIP-RK, "String" |FA-IP|HA-IP |NONCE).

El símbolo "|" significa la concatenación de las cadenas parciales de símbolos.

Al respecto puede adicionalmente modificarse la derivación de claves en el sentido de que para PMIPV4 y CMIPV4 se deriven claves separadas, por ejemplo:

MN-HA-CMIP4 = H(MIP-RK, "CMIP4MNHA" |HA-IP)

MN-HA-PMIP4 = H(MIP-RK, "PMIP4MNHA" |HA-IP).

Para cada una de las diversas secciones de transmisión de datos entre nodos de la red de acceso 2 y el aparato terminal móvil 1 pueden deducirse de esta forma respectivas claves específicas de la red de acceso a partir de la Mobile-IP-Root-Key, que a su vez se deduce de la clave de base transmitida.

En el procedimiento correspondiente a la invención se amplía la derivación de clave realizada hasta ahora en el marco de un registro en la red basado en EAP de un abonado tal que el Interworking-Proxy-Server 7 proporciona claves adecuadas para CMIP a la red de acceso, que dado el caso también pueden utilizarse para PMIP. En el procedimiento correspondiente a la invención se deduce la clave de base y/o la pseudo-clave a partir de la MSK y/o de la EMSK y/u otro input, por ejemplo una cadena de caracteres mediante una función de derivación de clave KDF adecuada, por medio del servidor de autentificación.

La figura 9 muestra un diagrama de señales para describir el principio básico del procedimiento correspondiente a la invención. En la autentificación de un aparato terminal móvil 1 mediante un protocolo de autentificación y acuerdo de claves, por ejemplo EAP basado en radio (Radius) o diámetro (Diameter), genera un servidor de seguridad o un servidor de autentificación 4A en una primera red una clave de base y/o una pseudo-clave PTKS o una clave criptográfica pseudo-temporal sobre la base de la clave criptográfica temporal TKS, por ejemplo una Master Session Key MSK y/o EMSK. La pseudo-clave deducida con una función de derivación se transmite a continuación a un Interworking-Proxy-Server 7, que por ejemplo se encuentra en una segunda red, deduciéndose a su vez para cada servidor de aplicación y/o nodo 8, 9 a partir de otra función de derivación una clave específica de la red de acceso. Cada servidor de aplicación 8, 9 recibe a continuación del Interworking-Proxy-Server 7 la clave específica de la red de acceso para él deducida. Mediante la clave transmitida queda a continuación protegida criptográficamente la sección de transmisión de datos entre el aparato terminal 1 y el correspondiente servidor de aplicación 8, 9.

Con el procedimiento correspondiente a la invención es posible utilizar servidores de autentificación, por ejemplo servidores WLAN o 3GGP para redes de acceso WiMax, no teniendo que aportar los servidores de autentificación la funcionalidad CMIP/PMIP que espera la red de acceso WiMax, sino solamente teniendo que ampliarse en la funcionalidad para deducir una clave de base a partir de la clave de sesión. El procedimiento correspondiente a la invención ofrece además la ventaja de que en una red WiMax también se apoya el caso de CMIP y con ello se evita cualquier limitación relativa a la macromovilidad. En el procedimiento correspondiente a la invención no debe modificarse ni someterse la red WiMax, a excepción de prever un Interworking-Proxy-Server 7, en la red WiMax a ninguna otra modificación. El aparato terminal móvil 1, el servidor de autentificación, así como el Interworking-Proxy-Server 7 saben qué clave de base o pseudo-clave utilizan. De esta manera es posible apoyar distintas claves MIP (variantes bootstrapping o de arranque) dentro de la red WiMax. En el procedimiento correspondiente a la invención se transforma material de claves, que por ejemplo procede de una red 3GPP, en material de claves para la red WiMax, pudiendo utilizar las redes WiMax la clave constituida, sin que se realice una adaptación.

En una forma de realización del procedimiento correspondiente a la invención se establece la funcionalidad de autentificación según la invención fuera de la red WiMax, por ejemplo en la red 3GPP. El procedimiento correspondiente a la invención permite una futura interacción (interworking) WiMax-3GPP sin que debido a ello tengan que aceptarse limitaciones en la red WiMax. Otra ventaja adicional del procedimiento correspondiente a la invención consiste en que puede ampliarse fácilmente al interworking entre diversas redes, así como para proporcionar claves para cualesquiera aplicaciones. En el procedimiento correspondiente a la invención sólo tiene que saber el Interworking-Proxy-Server 7 qué claves específicas de la aplicación tienen que proporcionarse y cómo han de deducirse las mismas. Por lo tanto en el procedimiento correspondiente a la invención no es necesario que ya el servidor de autentificación doméstico pueda generar para todas las distintas redes conectadas las respectivas claves necesarias. Correspondientemente es relativamente sencillo en el procedimiento correspondiente a la invención conectar distintas redes de manera flexible a la red doméstica.

En el procedimiento correspondiente a la invención genera el aparato terminal móvil 1 en la autentificación igualmente la clave de sesión y deduce de la forma correspondiente la clave específica de la red de acceso.

REIVINDICACIONES

1. Procedimiento para proporcionar una clave específica de red de acceso para asegurar una transmisión de datos entre un aparato terminal móvil (1) y un nodo de una red de acceso (2),
en el que durante una autentificación del aparato terminal móvil (1) un servidor de autentificación (4A) genera una clave de sesión, de la que se deduce una clave de base y se transmite a un Interworking-Proxy-Server (servidor intermediario de interacción) (7), que deduce a partir de la clave de base transmitida la clave específica de la red de acceso y la proporciona al nodo de la red de acceso (2) y
en el que el aparato terminal móvil (1) genera durante la autentificación igualmente la clave de sesión y deduce de ella la clave específica de la red de acceso.

2. Procedimiento según la reivindicación 1,
en el que la clave de sesión se constituye mediante una clave MSK (Master Session Key, clave de sesión maestra) o mediante una clave EMSK (Extended Master Session Key, clave de sesión maestra ampliada).

3. Procedimiento según la reivindicación 1,
en el que se deduce la clave de base a partir de la clave de sesión mediante una primera función de derivación predeterminada.

4. Procedimiento según la reivindicación 3,
en el que la primera función de derivación se forma mediante una función de derivación HMAC-SHA1, HMAC-SHA256, HMAC-MD5, SHA1, SHA256 o MD5.

5. Procedimiento según la reivindicación 1,
en el que la derivación de la clave de base se realiza en función de la clave de sesión y de una cadena de caracteres (string).

6. Procedimiento según la reivindicación 1,
en el que la autentificación del aparato terminal móvil se realiza en el servidor de autentificación mediante un protocolo EAP.

7. Procedimiento según la reivindicación 1,
en el que la autentificación del aparato terminal móvil se realiza en el servidor de autentificación mediante un protocolo UMTS-AKA.

8. Procedimiento según la reivindicación 1,
en el que la autentificación del aparato terminal móvil en el servidor de autentificación se realiza mediante un protocolo HTTP-Digest-AKA.

9. Procedimiento según la reivindicación 1,
en el que la transmisión de datos entre el servidor de autentificación y el Interworking-Proxy-Server se realiza mediante un protocolo de diámetro (Diameter) o un protocolo de radio (Radius).

10. Procedimiento según la reivindicación 1,
en el que la red de acceso se forma mediante una red WiMax.

11. Procedimiento según la reivindicación 1,
en el que la red doméstica del aparato terminal móvil se forma mediante una red 3GPP.

12. Procedimiento según la reivindicación 1,
en el que se deduce a partir de la clave de base transmitida a través del Interworking-Proxy-Server mediante una segunda función de derivación una clave Mobile-IP-Root-Key.

13. Procedimiento según la reivindicación 12,
en el que la segunda función de derivación se forma mediante una función de derivación HMAC-SHA1, HMAC-SHA256, HMAC-MD5, SHA1, SHA256 o MD5.

14. Procedimiento según la reivindicación 13,
en el que se deduce a partir de la Mobile-IP-Root-Key deducida mediante una tercera función de derivación la clave específica de la red de acceso para asegurar una transmisión de datos entre el aparato terminal móvil y el nodo de una red de acceso.

15. Procedimiento según la reivindicación 14,
en el que la tercera función de derivación se forma mediante una función de derivación HMAC-SHA1, HMAC-SHA256, HMAC-MD5, SHA1, SHA256 o una función de derivación MD5.

16. Procedimiento según la reivindicación 1,

en el que para las distintas secciones de transmisión de datos entre nodos de la red de acceso (2) y el aparato terminal móvil (1) se deduce en cada caso una clave correspondiente específica de la red de acceso.

17. Servidor de autentificación (4A) para proporcionar una clave de base, a partir de la que puede deducirse una clave específica de la red de acceso para asegurar una sección de transmisión de datos entre un aparato terminal móvil (1) y un nodo de una red de acceso (2), estando configurado el servidor de autentificación (4A) para en una autentificación del aparato terminal móvil (1) generar una clave de sesión y deducir de ella mediante una función de derivación la clave de base y proporcionarla a un Interworking-Proxy-Server (7).

18. Servidor de autentificación según la reivindicación 17,
en el que la función de derivación se forma mediante una función de derivación HMAC-SHA1, HMAC-SHA256, HMAC-MD5, SHA1, SHA256 o una función de derivación MD5.

19. Interworking-Proxy-Server (7) para proporcionar una clave específica de red de acceso para asegurar una transmisión de datos entre un aparato terminal móvil (1) y un nodo de una red de acceso (2), configurado para derivar a partir de una clave de base transmitida por un servidor de autentificación (4A) la clave específica de la red de acceso y proporcionarla al nodo de la red de acceso (2).

20. Sistema de transmisión de datos con varias redes de acceso (2) y al menos una red doméstica (4) de un aparato terminal móvil (1),
en el que un servidor de autentificación (4A) de la red doméstica (4) está configurado para cuando se autentifica un aparato terminal móvil (1) generar una clave de sesión y deducir de la misma una clave de base común y transmitirla a las redes de acceso (2) que disponen de respectivos Interworking-Proxy-Server (7), que están equipados para deducir al menos una clave específica de acceso a partir de la clave de base transmitida, que está prevista en cada caso para asegurar una sección de transmisión de datos entre el aparato terminal móvil (1) y un nodo de la correspondiente red de acceso (2) y
en el que el aparato terminal móvil (1) está configurado para generar durante la autentificación igualmente la clave de sesión y deducir de ella la clave específica de la red de acceso.

21. Sistema de transmisión de datos según la reivindicación 20,
en el que para cada nodo de la red de acceso (2) se deduce la correspondiente clave específica de la red de acceso mediante el Interworking-Proxy-Server (7) a partir de la clave de base transmitida.

FIG 1 **Estado de la técnica**

Tabla de enlaces de movilidad

Dirección doméstica	Dirección de custodia	Duración (ms)
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 custodia	Dirección de los medios	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

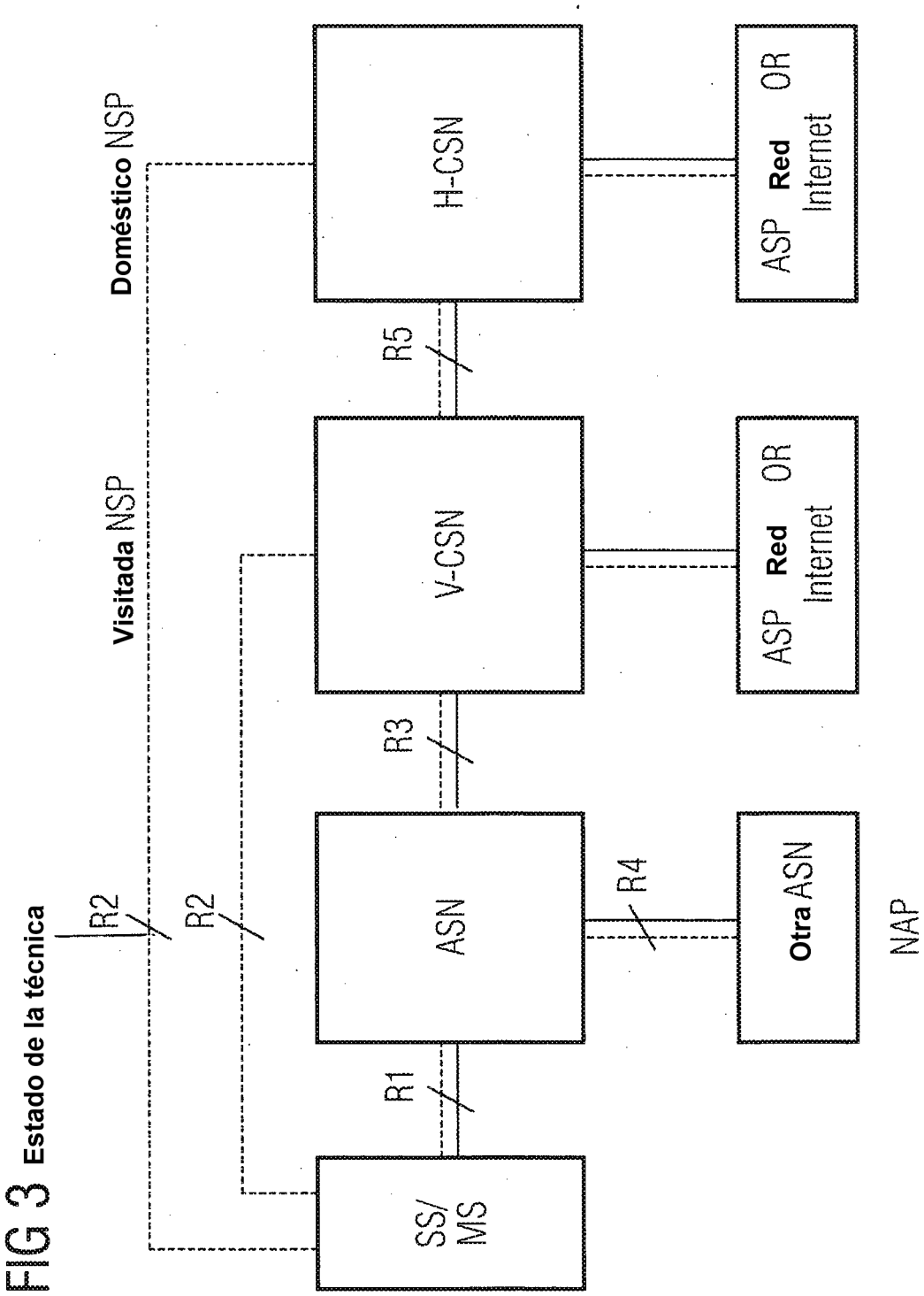


FIG 4
Estado de la técnica

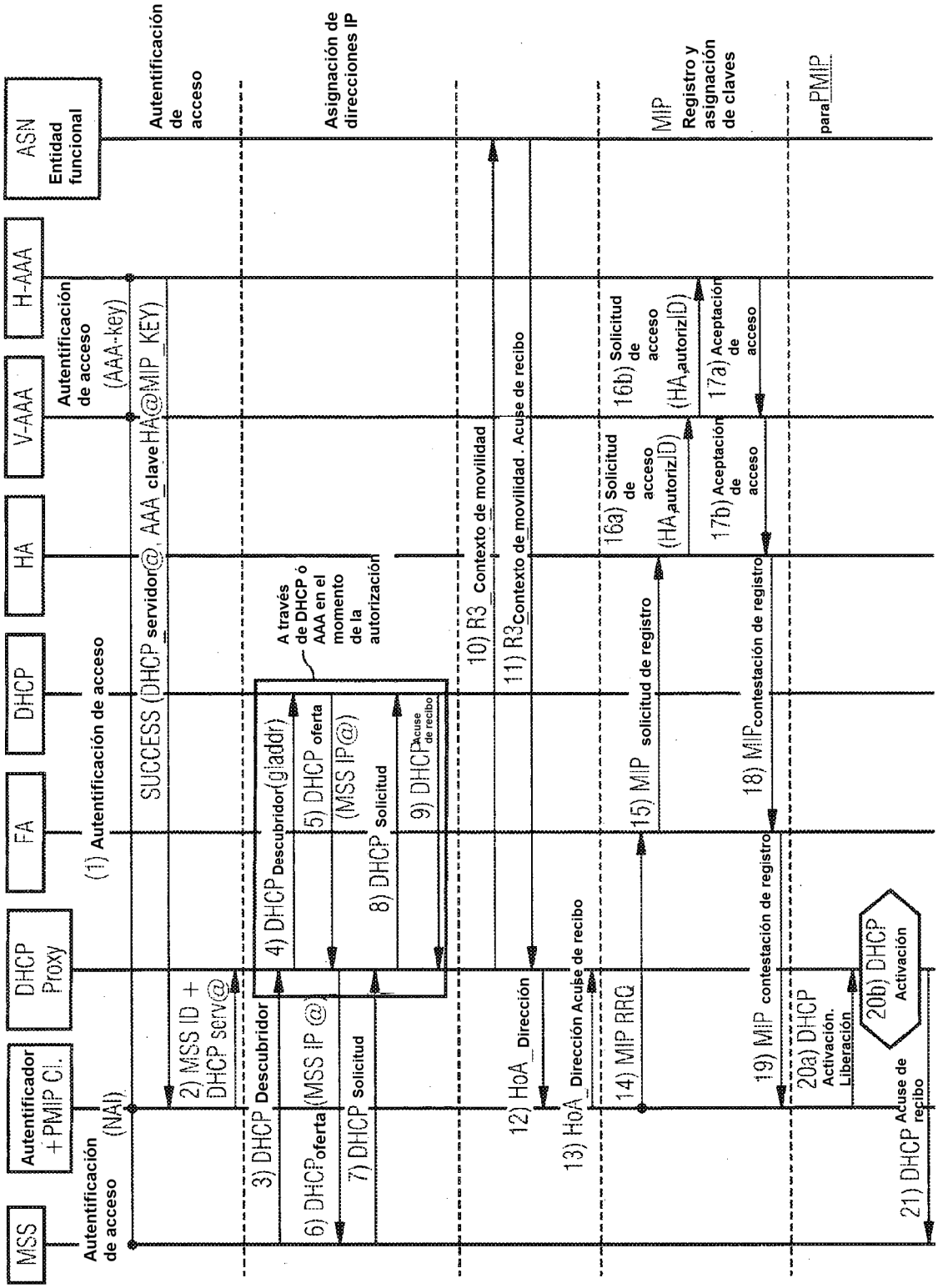


FIG 5 Estado de la técnica

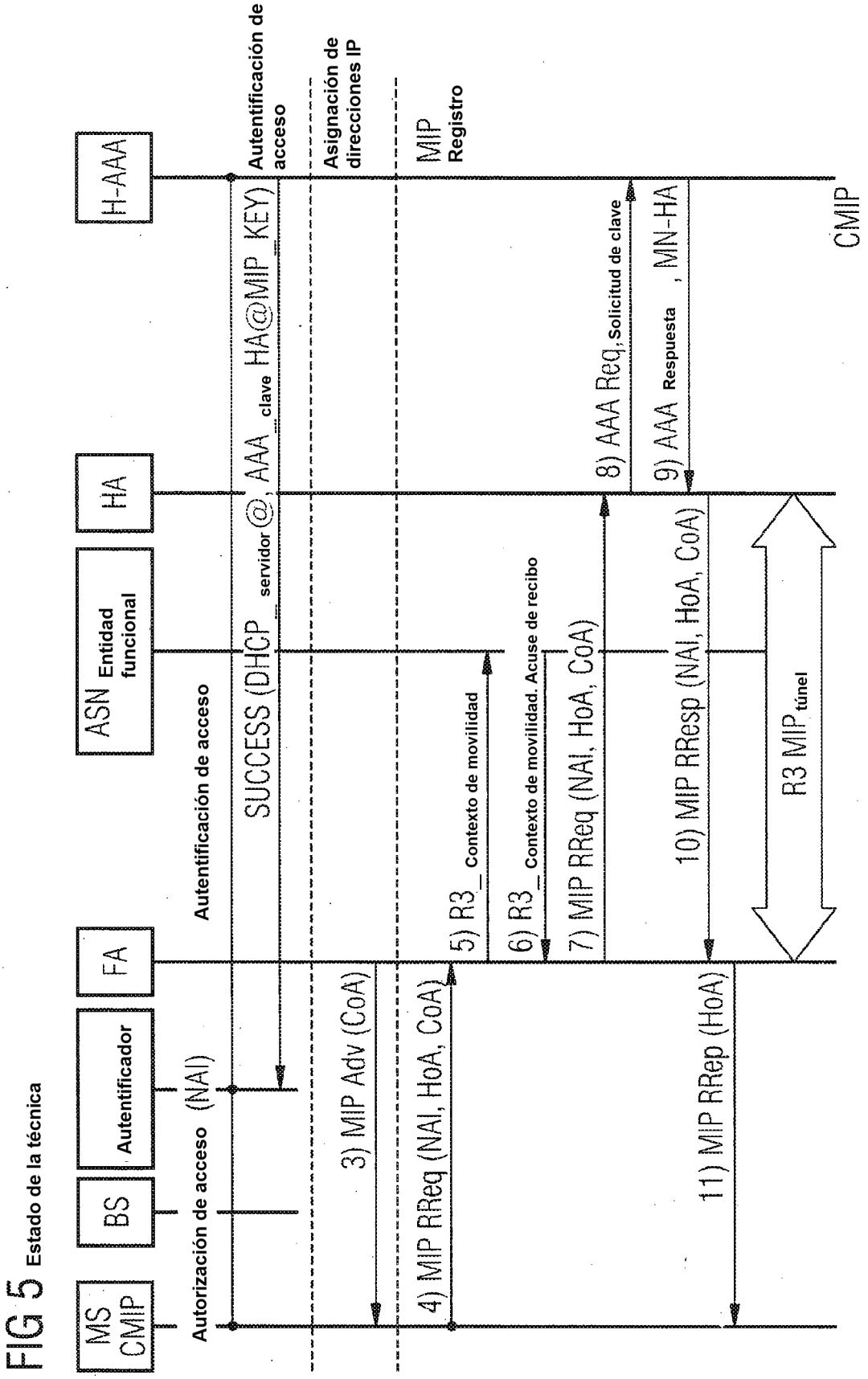


FIG 6 **Estado de la técnica**

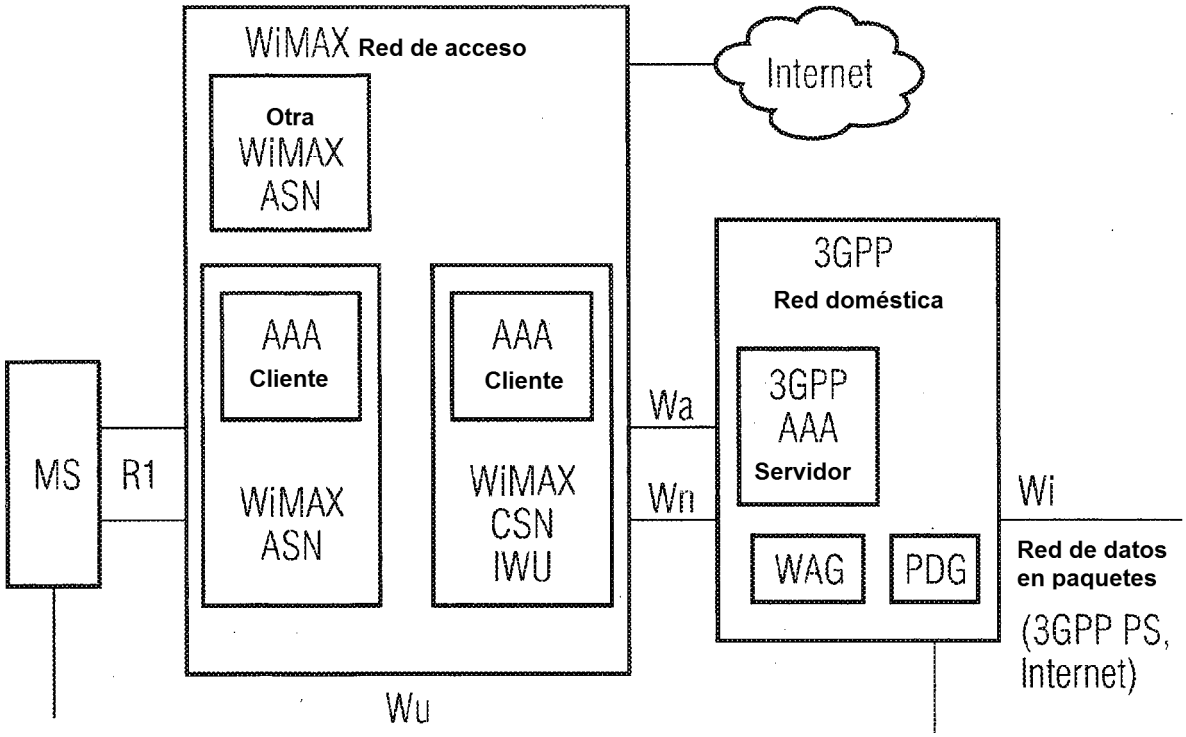


FIG 7

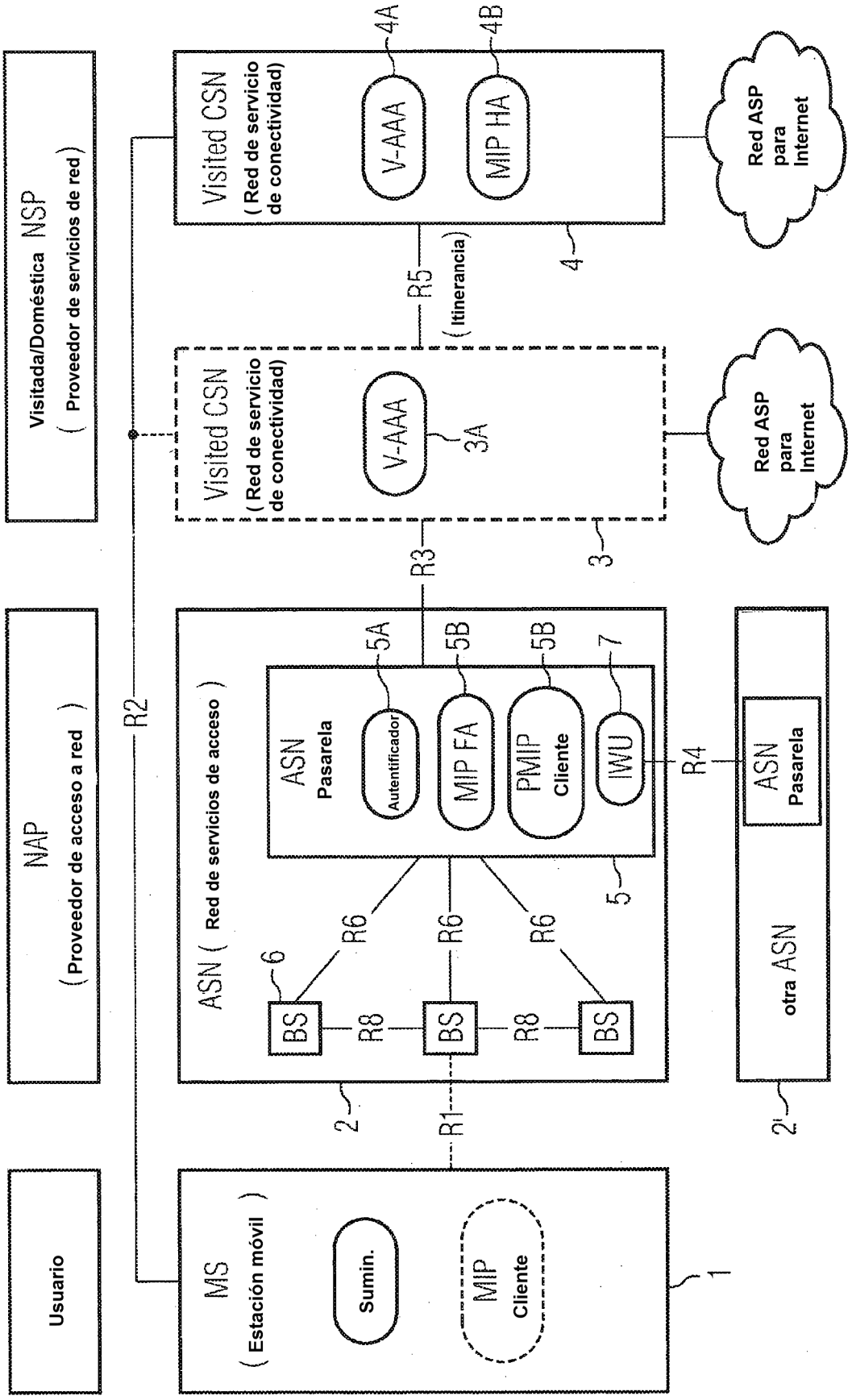

Usuario
NAP
(Proveedor de acceso a red)
Visitada/Doméstica NSP
(Proveedor de servicios de red)
MS
(Estación móvil)
Sumin.
MIP Cliente
1
ASN (Red de servicios de acceso)
ASN Pasarela
Autentificador
MIP FA
PMIP Cliente
IWU
5A
5B
5B
7
5
BS
BS
BS
6
R6
R6
R6
R8
R8
2
R1
R2
R3
R4
otra ASN
ASN Pasarela
2'
Visited CSN
(Red de servicio de conectividad)
V-AAA
3A
3
Visited CSN
(Red de servicio de conectividad)
V-AAA
MIP HA
4A
4B
4
R5
(Itinerancia)
Red ASP para Internet
Red ASP para Internet

FIG 8

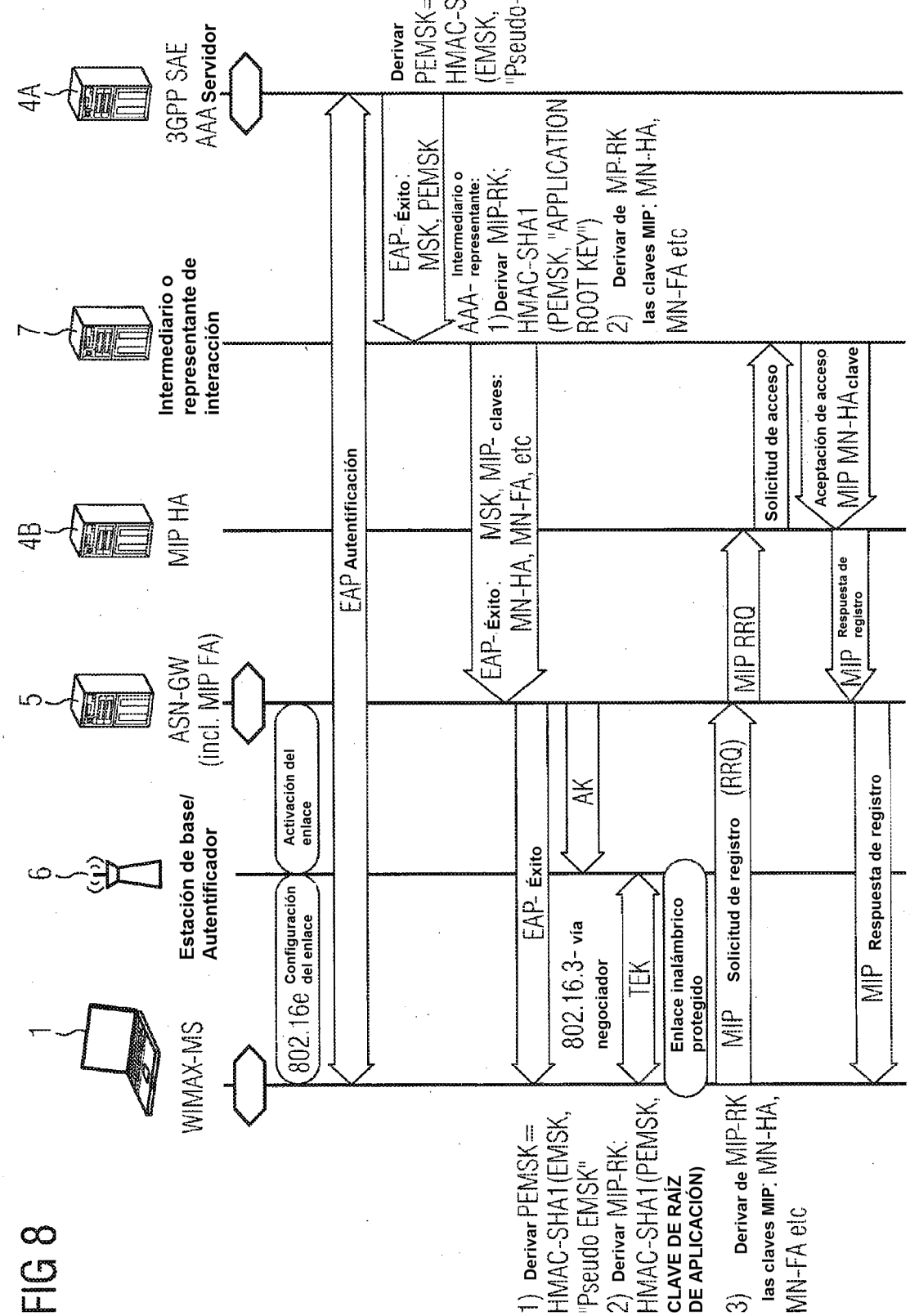
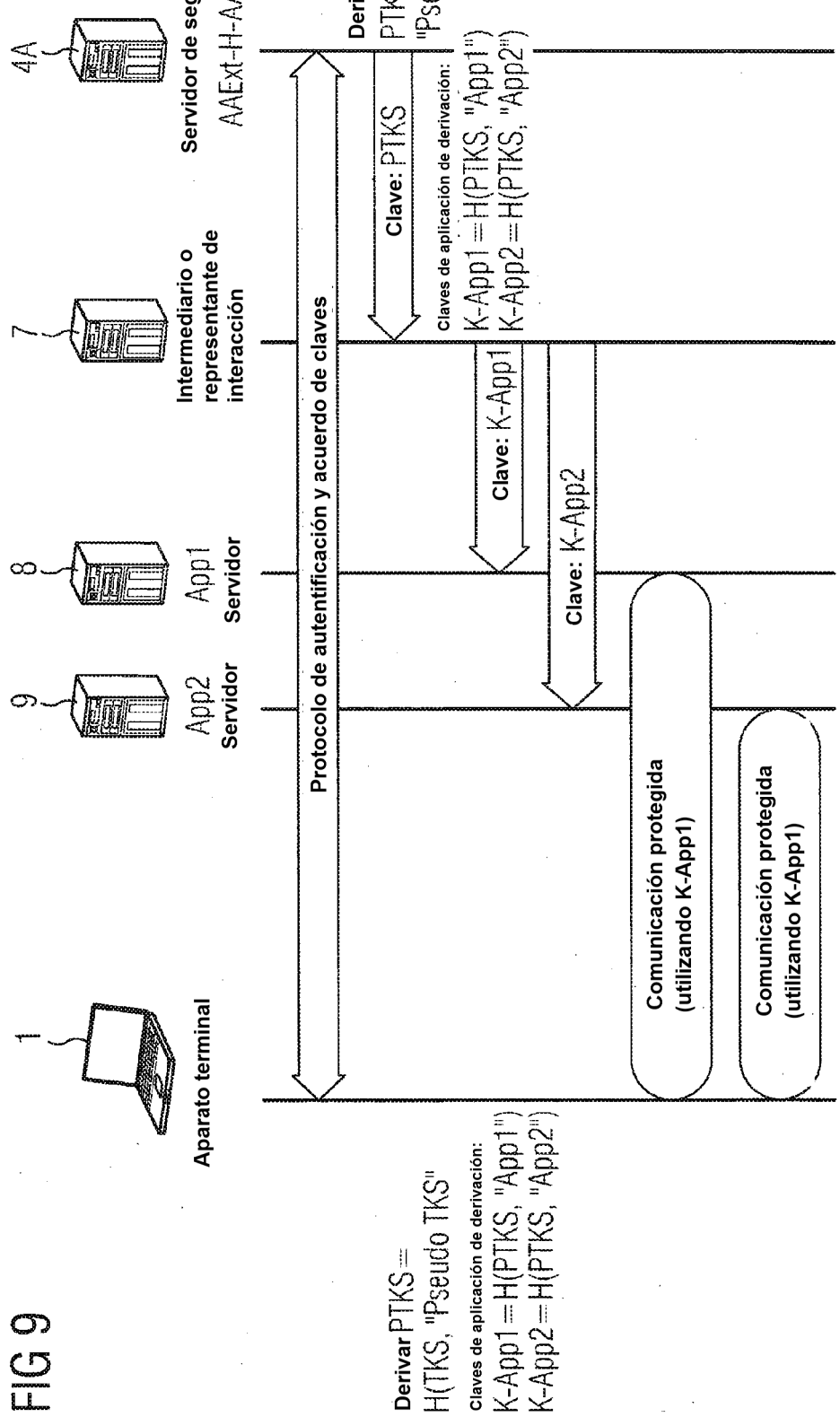

1
WIMAX-MS
6
Estación de base/ Autentificador
5
ASN-GW (incl. MIP FA)
4B
MIP HA
7
Intermediario o representante de interacción
4A
3GPP SAE AAA Servidor
802.16e Configuración del enlace
Activación del enlace
EAP Autentificación
Derivar PEMSK= HMAC-SHA1 (EMSK, "Pseudo-EMSK")
EAP- Éxito: MSK, PEMSK
AAA- Intermediario o representante: 1) Derivar MIP-RK; HMAC-SHA1 (PEMSK, "APPLICATION ROOT KEY") 2) Derivar de MP-RK las claves MIP: MN-HA, MN-FA etc
EAP- Éxito: MSK, MIP- claves: MN-HA, MN-FA, etc
MIP RRQ
Solicitud de acceso
Aceptación de acceso
MIP MN-HA clave
MIP Respuesta de registro
EAP- Éxito
802.16.3- vía negociador
AK
TEK
Enlace inalámbrico protegido
MIP Solicitud de registro (RRQ)
MIP Respuesta de registro
1) Derivar PEMSK = HMAC-SHA1 (EMSK, "Pseudo EMSK"
2) Derivar MIP-RK: HMAC-SHA1 (PEMSK, CLAVE DE RAÍZ DE APLICACIÓN)
3) Derivar de MIP-RK las claves MIP: MN-HA, MN-FA etc

FIG 9


1
Aparato terminal
9
App2
Servidor
8
App1
Servidor
7
Intermediario o representante de interacción
4A
Servidor de seguridad
AAExt-H-AAA
Protocolo de autentificación y acuerdo de claves
Derivar PTKS=H(TKS, "Pseudo-TKS")
Clave: PTKS
Claves de aplicación de derivación:
K-App1=H(PTKS, "App1")
K-App2=H(PTKS, "App2")
Clave: K-App1
Clave: K-App2
Comunicación protegida (utilizando K-App1)
Comunicación protegida (utilizando K-App1)
Derivar PTKS= H(TKS, "Pseudo TKS"
Claves de aplicación de derivación:
K-App1=H(PTKS, "App1")
K-App2=H(PTKS, "App2")