(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 362 444**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07703657 .2**
(96) Fecha de presentación : **04.01.2007**
(97) Número de publicación de la solicitud: **2103077**
(97) Fecha de publicación de la solicitud: **23.09.2009**

(54) Título: **Método y aparato para determinar un procedimiento de autentificación.**

(45) Fecha de publicación de la mención BOPI:
05.07.2011

(45) Fecha de la publicación del folleto de la patente:
05.07.2011

(73) Titular/es: **Telefonaktiebolaget LM Ericsson (publ)**
164 83 Stockholm, SE

(72) Inventor/es: **Walker, John Michael y**
Näslund, Mats

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Método y aparato para determinar un procedimiento de autentificación

Campo Técnico

La presente invención se refiere a un método y a un aparato para determinar un procedimiento de autentificación que se va a aplicar a un cliente que accede o que intenta acceder a servicios de acceso vía un dominio visitado mientras tiene un acuerdo de servicio con un dominio doméstico.

Antecedentes

En el caso de redes telefónicas celulares, un modelo operativo convencional ha evolucionado a lo largo de los años para posibilitar que los usuarios itineren fuera del dominio doméstico al cual suscriben, en los denominados dominios visitados. Este modelo permite que los usuarios itineren en dominios visitados (por ejemplo, extranjeros) mientras que asegura que los operadores del dominio visitado pueden recuperar los costes incurridos desde el dominio doméstico. Al mismo tiempo, el operador del dominio doméstico puede confiar en los operadores del dominio visitado para recargar solamente los costes en los que han incurrido realmente. Un componente clave de este modelo es un mecanismo para permitir que un dominio visitado autentifique a un usuario como abonado del dominio doméstico. El dominio visitado necesita ayuda del dominio doméstico para ejecutar en la práctica este mecanismo. El enfoque típico es proporcionar dentro del dominio doméstico un “servidor de autentificación” que mantiene las credenciales de autentificación a largo plazo para los usuarios y es la “raíz de la confianza” para el usuario. Hay provisto un “autentificador” dentro del dominio visitado y realiza la autentificación real mediante la comunicación con el servidor de autentificación y el usuario (o “cliente”).

El documento 3GPP TS 33.102 describe una arquitectura de seguridad para redes del Servicio Universal de Telecomunicaciones entre Móviles (UMTS) que es, tanto como sea posible, compatible con las redes preexistentes del GSM. TS 33.102 considera en particular el protocolo de seguridad de Acuerdo de Autentificación y de Clave (AKA, en sus siglas en inglés) que es un mecanismo para realizar la autentificación y la distribución de la clave de la sesión. AKA es un mecanismo basado en reto-respuesta que usa criptografía simétrica. Dentro de un terminal de cliente, AKA funciona típicamente en un Módulo de Identidad de Abonado de UMTS (USIM, en sus siglas en inglés) que reside en un dispositivo similar a una tarjeta inteligente. La tarjeta inteligente posee una K secreta que también se conoce como Centro de Autentificación (AuC) situado dentro del dominio doméstico del usuario. Cuando un usuario intenta registrarse en un dominio visitado, se hace funcionar el mecanismo de AKA entre el terminal de cliente y el dominio visitado, implicando el dominio doméstico como “extremo posterior”. Este procedimiento conlleva que el dominio visitado sea provisto, por la red doméstica, de un vector de autentificación que comprende una pregunta y un resultado esperado. La pregunta es remitida por el dominio visitado al terminal del cliente, que genera una respuesta a la pregunta (dentro del USIM) y devuelve esto al dominio visitado. Si la respuesta a la pregunta coincide con el resultado esperado, el dominio visitado autoriza al terminal del cliente a usar sus servicios de acceso. AKA también permite al terminal del cliente verificar que su dominio doméstico ha estado involucrado, sin duda, en el procedimiento de señalización, que a su vez permite que el terminal autentifique el dominio visitado.

El vector de autentificación de AKA es bueno solamente para un intento de acceso por el cliente. Si el terminal del cliente elimina posteriormente su registro del dominio visitado (por ejemplo, el terminal es apagado), se requiere un nuevo vector de autentificación para cualquier registro posterior. El documento TS 33.102 permite que el dominio doméstico proporcione al dominio visitado un conjunto de vectores de autentificación en el primer registro, posibilitando que el dominio visitado realice múltiples autentificaciones para un terminal del cliente dado sin tener que contactar con el dominio doméstico para cada registro individual.

La autentificación en las redes 2G se maneja usando un enfoque de pregunta y respuesta similar a AKA.

Los enfoques de 2G y de 3G con respecto a la seguridad posibilitan la movilidad (local) y los traspasos puesto que el dominio doméstico no necesita estar implicado en nuevas autenticaciones subsiguientes. Por ejemplo, en el caso de un terminal que transfiere a un acceso de 2G desde un acceso de 3G (donde ambos accesos pertenecen al mismo operador), un usuario puede ser autentificado/autorizado implícitamente en el acceso nuevo por la reutilización de las claves de la sesión previamente utilizadas. Sin embargo, delegar la responsabilidad para la autentificación ante la red visitada puede no ser siempre satisfactorio para el dominio doméstico, ya que el dominio doméstico debe confiar “ciegamente” en que el dominio visitado no está haciendo una reivindicación falsa en cuanto a la presencia del cliente en el dominio visitado, o que el cliente está recibiendo el pago por los servicios, etc. Aunque este modelo de confianza ha funcionado bien para operadores de red establecidos, puede no aplicarse a configuraciones de redes futuras como se va a discutir más abajo.

En el caso de la Internet, el IETF ha creado bajo el encabezamiento de Autentificación, Autorización y Contabilidad (AAA, en sus siglas en inglés), un conjunto de protocolos para conseguir la autentificación de un usuario dentro de un dominio visitado. Los protocolos implementados actualmente incluyen el RADIO y el DIAMETER. Un escenario de Internet típico podría conllevar que un usuario que procure usar un punto caliente de una WLAN (situado por ejemplo en un *Internet-café* o en un terminal del aeropuerto) como red de acceso, cuando el usuario es un abonado de una red de banda ancha del Proveedor de Servicios de Internet (ISP). En el modelo de IETF, la autentificación es

realizada en el dominio doméstico, es decir, el servidor del autentificador y de la autentificación están ambos en el dominio doméstico. Aunque esto puede ser satisfactorio para el dominio doméstico, conduce a un comportamiento por debajo del óptimo debido a la cabecera de señalización y perjudica el traspaso suave/la movilidad dentro del dominio visitado.

Se observa que cuando el dominio de acceso es una red inalámbrica, un terminal inalámbrico puede comunicar con un cliente/autentificador de AAA dentro del dominio de acceso, con el cliente de AAA comunicando con el servidor de AAA del dominio doméstico. La señalización de autentificación de extremo a extremo puede ser transportada usando el Protocolo Extensible de Autentificación (EAP, en sus siglas en inglés) que es una trama de autentificación más que un método real de autentificación. Uno de los papeles del EAP es implementar un método de autentificación entre puntos de extremo. El método de EAP-AKA es un ejemplo de tal método de autentificación. En este enfoque, por lo tanto, los datos de AKA estarán contenidos dentro de mensajes de EAP que están, a su vez, contenidos dentro de los mensajes de DIAMETER (para el cliente de AAA a la pata del servidor de AAA). [UMTS AKA, como se ha descrito más arriba, es un protocolo específico de 3GPP que no utiliza AAA y tramas de EAP y no se debe confundir con EAP-AKA, aunque, por supuesto, el mecanismo real de AKA es común a ambos.]

Esta “arquitectura” de protocolo actual está ilustrada en la figura 1, en la que la red de acceso inalámbrica es una red de 802.11 (WLAN) y el punto de extremo de AKA está en el dominio doméstico. El cliente/autentificador de AAA dentro de la red inalámbrica comprende la señalización del EAP, y convierte el EAP de la señalización de AAA en el EAP sobre la LAN. El cliente/autentificador de AAA es transparente al AKA. Se observa que uno o más servidores próximos de AAA pueden estar presentes entre las redes visitada y doméstica.

Las normas de la comunicación están evolucionando para proporcionar la integración de diferentes dominios de acceso heterogéneos en una sola red lógica. Esto dará como resultado dominios de acceso basados en 3GPP (por ejemplo, GPRS, UMTS, LTE) y dominios de acceso no basados en 3GPP (por ejemplo, Wimax, WLAN, banda ancha por línea fija, etc.) que se unen para formar una red lógica (ver, por ejemplo, 3GPP 3GPP TR 23.882). Un dominio doméstico utilizará probablemente AAA (por ejemplo, DIAMETER) y EAP, y múltiples métodos de EAP (tales como EAP AKA, EAP SIM, EAP TLS, etc.) para comunicarse con los diferentes dominios de acceso y terminales. Es, sin embargo, inevitable que un dominio doméstico dado situará diferentes niveles de confianza en diferentes dominios de acceso. Por ejemplo, un nivel de confianza elevado podría estar situado en un dominio de acceso de 3G, mientras un nivel de confianza muy bajo puede estar situado en una WLAN de un café de Internet.

El documento WO02/069605 describe un método y un sistema para la delegación de los procedimientos de seguridad mediante un dominio doméstico a un segundo dominio. Esto implique que el dominio doméstico envíe una clave y un número aleatorio al segundo dominio, con el número aleatorio siendo enviado a un nodo móvil, después de que el segundo dominio pueda autentificar al nodo móvil.

El borrador del IETF „Localised Key Management for AAA in Mobile IPv6“ („Gestión de claves localizadas para AAA en IPv6 móvil“), Miyoung Kim et al, octubre, 2002, describe un modo de distribuir una clave segura para optimizar un procedimiento de autentificación de "AAA" para un nodo móvil itinerante. Las operaciones para generar y sincronizar claves son delegadas a un servidor de AAA en el dominio visitado.

El documento "Research Issues for Fast Authentication in Inter-Domain Handover" („Aspectos investigativos para la autentificación rápida en el traspaso entre dominios“), Wireless World Research Forum, H. Wang etal, febrero, 2004, describe varios enfoques para conseguir autentificación rápida que sigue al traspaso entre dominios de un terminal inalámbrico de usuario.

El documento WO03/06564 describe un mecanismo para proporcionar a un cliente acceso a un servidos seguro, y hace uso de un servidor de autentificación. El mecanismo emplea señalización enviada a través de Internet.

Resumen

Según un primer aspecto de la presente invención hay provisto un servidor para manejar la autentificación de los clientes que son abonados de un dominio doméstico dentro del cual está situado el servidor, caracterizado porque el servidor comprende medios (6, 7) para determinar si un cliente que está unido a un dominio visitado va a ser autentificado por el dominio doméstico o por dicho dominio visitado, usando esta decisión un conocimiento del tipo de seguridad de red usada en una red de acceso del dominio visitado, y para señalizar el resultado de dicho dominio visitado, en el que, en el caso de que el cliente vaya a ser autentificado por el dominio doméstico, dicho resultado es un resultado de autentificación de la red doméstica y, en el caso de que el cliente va a ser autentificado por el dominio visitado, dicho resultado incluye datos de autentificación del dominio doméstico para uso por el dominio visitado para autentificar al cliente.

Formas de realización de la presente invención introducen una flexibilidad dinámica en el procedimiento de autentificación. Ahora es posible que el dominio doméstico determine dónde va a tener lugar la autentificación, basándose en propiedades estáticas tales como la suscripción del cliente, y en propiedades cambiantes tales como la identidad de la red visitada. Esto tiene como resultado una arquitectura de servicio que optimiza las vías de señalización cuando es apropiado, mientras mantiene la seguridad financiera.

El servidor puede comprender una memoria para almacenar los datos de autentificación para dichos clientes. El servidor está dispuesto, en caso de que determine que la red visitada va a ser responsable de la autentificación, generar datos de la sesión y enviar esto a dicha red visitada. Cuando la red visitada es una red de 3G, estos datos pueden comprender un vector de autentificación.

En ciertas realizaciones de la invención, el servidor comprende una interfaz para comunicar con los dominios visitados, primeros medios de tratamiento para recibir, vía dicha interfaz, una petición de registro enviada por un dominio visitado en relación con uno de dichos clientes, y segundos medios de tratamiento para determinar si la petición va a ser autentificada por el dominio doméstico o por el dominio visitado. Los segundos medios de tratamiento están dispuestos, en el caso anterior, para autenticar la petición y señalizar el resultado al dominio visitado vía dicha interfaz, y, en el último caso, señalizar la petición al dominio visitado.

Dichos primeros medios de tratamiento pueden, además, estar dispuestos para recibir vía dicha interfaz una petición desde una red visitada para transferir la decisión de autentificación desde un dominio a otro, en el caso de un cliente previamente autentificado. Dichos segundos medios de tratamiento están dispuestos para tomar otra determinación y para notificar consiguientemente la red visitada.

El servidor puede comprender medios para determinar que una decisión previa para delegar un procedimiento de autentificación al dominio visitado va a ser revocada, y para señalizar esa decisión al dominio visitado.

Se observa que el procedimiento de autentificación que puede ser delegado al dominio visitado puede ser un procedimiento de segundo nivel. Un procedimiento de primer nivel puede ser llevado a cabo por el dominio doméstico basándose, por ejemplo, en el terminal y/o en la identidad del usuario, antes de conducir el procedimiento de segundo nivel en el dominio doméstico o, si está delegado, en el dominio visitado.

Según un segundo aspecto de la presente invención hay provisto un método para autentificar a un cliente unido a un dominio visitado, en el que el cliente es un abonado de un dominio doméstico, comprendiendo el método:

enviar una petición de autentificación desde el dominio visitado al dominio doméstico con respecto a dicho cliente;

caracterizado por las operaciones de

en el dominio doméstico, determinar si el cliente va a ser autentificado por el dominio doméstico o por dicho dominio visitado;

en el caso de que el cliente vaya a ser autentificado por el dominio doméstico, llevar a cabo dicha autentificación en el dominio doméstico y señalizar el resultado de esta autentificación al dominio visitado; y

en el caso de que el cliente vaya a ser autentificado por el dominio visitado, enviar datos de autentificación desde el dominio doméstico al dominio visitado, y usar dichos datos en el dominio visitado para autentificar al cliente.

En el caso del protocolo de AAA, dicha petición de autentificación puede ser una Petición de DIAMETER. En el caso de que la autentificación vaya a ser realizada por el dominio doméstico, esto es señalado al dominio visitado enviando un NACK. El resultado de la autentificación es señalado posteriormente al dominio visitado enviando un mensaje de ACEPTACIÓN/RECHAZO. La autentificación implica el intercambio de una consulta y de una respuesta entre el dominio doméstico y el cliente. En el caso en el que la autentificación se vaya a realizar por la red visitada, esto es señalizado al dominio visitado enviando un mensaje de ACK, junto con datos de autentificación. Un intercambio de consulta y de respuesta se realiza entre el cliente y el dominio visitado.

Breve descripción de los dibujos

La figura 1 ilustra diferentes capas de protocolo implicadas en un procedimiento de autentificación para un terminal inalámbrico unido a una red visitada;

La figura 2 ilustra esquemáticamente una arquitectura de sistema de comunicaciones que comprende dominios visitado y doméstico;

Las figuras 3a y 3b son diagramas de flujo que ilustran los procesos de decisión de autentificación realizados con un servidor de autentificación de un dominio doméstico;

La figura 4 muestra la señalización relacionada con la autentificación para el caso en el que un dominio doméstico toma la decisión de no delegar la responsabilidad de la autentificación a un dominio visitado;

La figura 5 muestra la señalización asociada con el caso en el que un dominio doméstico decide delegar la responsabilidad de la autentificación a un dominio visitado durante un período limitado o un número de intentos;

La figura 6 muestra la señalización asociada con la delegación de la responsabilidad de la autentificación a un dominio visitado, con la decisión subsiguiente de revocar ese permiso;

La figura 7 es un diagrama de señalización que ilustra un caso en el que un dominio visitado elige pedir una transferencia de responsabilidad de la autentificación de nuevo a un dominio doméstico;

La figura 8 es un diagrama de señalización que ilustra un caso en el que un dominio visitado elige pedir una transferencia de responsabilidad de la autentificación a éste, desde el dominio doméstico;

La figura 9 ilustra un flujo de señalización en el caso en el que un cliente se une a un dominio de acceso basado en la futura Evolución a Largo Plazo del 3GPP (LTE, en sus siglas en inglés); y

La figura 10 muestra un flujo de señalización en el caso en el que un cliente está unido a un dominio de acceso de I-WLAN.

Descripción detallada

En la figura 2 hay ilustrada una arquitectura genérica de dominio visitado/dominio doméstico que permite la itineración de los abonados (denominados más abajo “clientes”) del dominio doméstico en el dominio visitado. Un servidor 1 de autentificación está situado dentro del dominio doméstico 2 y mantiene las credenciales de autentificación para el largo plazo de los clientes del dominio doméstico. El servidor de autentificación puede actuar, también, como autentificador para los clientes que buscan registrarse con los dominios visitados que incluyen el dominio ilustrado 3. Un autentificador 4 independiente está situado dentro del dominio visitado 3. La figura 2 ilustra un cliente 5 unido al dominio visitado 3.

El servidor 1 de autentificación recibe peticiones de acceso desde un dominio visitado vía una interfaz 6, con lo cual los medios de tratamiento 7 del servidor de autentificación toman decisiones como si las autenticaciones van a ser realizadas dentro del dominio doméstico o pueden ser delegadas al dominio visitado. El servidor puede determinar, también, que las autenticaciones son compartidas entre los dominios doméstico y visitado. Por ejemplo, puede determinar que solamente la primera autentificación va a ser realizada por el dominio doméstico y que las subsiguientes autenticaciones son delegadas al dominio visitado, o que solamente cada décima autentificación va a ser realizada por el dominio doméstico, etc. El servidor toma estas decisiones basándose en cierta información disponible. Esta información puede incluir, por ejemplo, una o más de lo que sigue; identidad del operador visitado, tipo de red de acceso, identidad del usuario, tipo de seguridad de red que se está utilizando en la red de acceso del dominio visitado, tipo de autentificación de usuario que se está llevando a cabo, Nombre de Punto de Acceso (APN, en sus siglas en inglés) seleccionado, Calidad de Servicio (QoS, en sus siglas en inglés) requerida, reglas de carga, tipo de suscripción, tipo de terminal, localización del usuario (por ejemplo, se podrían considerar ciertas áreas geográficas menos seguras desde el punto de vista de las telecomunicaciones).

La figura 3a es un diagrama de flujo que ilustra el procedimiento de decisión de la delegación tomada por el servidor de autentificaciones dentro del dominio doméstico, a saber, evaluar los criterios de entrada (operación 1), establecer las condiciones de delegación de la autentificación (operación 2), y enviar la respuesta de delegación de la autentificación al dominio visitado (operación 3). La figura 3b es un diagrama de flujo que ilustra un procedimiento de decisión de revocación de la delegación tomado por el servidor de autentificaciones. Sobre la base de criterios de entrada recibidos nuevamente (por ejemplo, recibidos desde el dominio visitado), el servidor de autentificaciones evalúa los criterios para tomar la decisión de revocación (operación 4), y envía una revocación de autentificación al dominio visitado (operación 5).

En el caso que el protocolo de AAA de DIAMETER (RFC 3588 del IETF) es utilizado entre los dominios visitado y doméstico, la petición de acceso es llevada típicamente por un mensaje de Petición de DIAMETER enviado entre un cliente de AAA (posiblemente vía un servidor próximo (*proxy*) de AAA) en el dominio visitado y un servidor de HSS/AAA dentro del dominio doméstico. El servidor de autentificación doméstico responde, bien enviando un mensaje de Respuesta de DIAMETER que contiene un AVP (par valor atributo, en sus siglas en inglés) DIAMETER con datos de autentificación para ser utilizados por el dominio visitado, o enviando al dominio visitado un mensaje especial de “NACK”, informando al dominio visitado para permitir que el procedimiento de autentificación siga entre el cliente y el dominio doméstico. Dependiendo sobre la respuesta que recibe, el dominio visitado bien sólo reenvía señalización de autentificación relacionada con la autentificación (por ejemplo, señalización de EAP AKA), o usa los datos de autentificación recibidos desde el dominio doméstico para iniciar algo o toda la señalización de la autentificación subsiguiente con el cliente. Se observa que, en el caso del método de autentificación de AKA, el vector de autentificación de AKA, es decir (RAND, XRES, AUTN, Ck, Ik) contiene toda la información que el dominio visitado necesita para asumir el papel de autentificador.

Si la decisión era delegar la autentificación al dominio visitado, el dominio doméstico todavía tiene la opción de “revocar” la delegación, en cuyo caso, cualquier (re-) autentificación subsiguiente tendrá lugar en el dominio doméstico. DIAMETER soporta peticiones iniciadas por el servidor que pueden ser utilizadas para este fin. El operador del dominio doméstico puede también delegar la autentificación al dominio visitado durante un tiempo limitado o un número limitado de re-autenticaciones solamente, después del cual el dominio visitado debe retransmitir la señalización de la autentificación de nuevo al dominio doméstico (por lo menos hasta que el dominio

doméstico delega una vez, de nuevo, la responsabilidad de la autentificación al dominio visitado). El operador del dominio doméstico puede también decidir que cada autentificación N-sima se debe retransmitir por este dominio visitado de nuevo al dominio doméstico. Cualquiera de estas aproximaciones crea “puntos de prueba” en los cuales el dominio doméstico puede elegir continuar o cambiar la política aplicada a la autentificación. Como DIAMETER requiere generalmente el mantenimiento de la información del estado de la sesión (por ejemplo, con el fin de contabilidad), esta información de estado puede ser extendida con la información que posibilita el dominio visitado para decidir cuándo realizar la autentificación localmente y cuando diferirla al dominio doméstico.

Se apreciará que el procedimiento descrito aquí ofrece al dominio visitado la oportunidad de rehusar “borrar” datos de autentificación que ya tiene, y de continuar para tomar el papel de autentificador incluso si el dominio doméstico revoca los derechos delegados. Sin embargo, en tal circunstancia, la red visitada no puede garantizarse que será pagado para los servicios utilizados. En todo caso, el propio cliente puede elegir no continuar.

La figura 4 muestra la autentificación relacionada con la señalización para el caso en el que el dominio doméstico toma la decisión de no delegar la responsabilidad de la autentificación al dominio visitado. Esto se puede ejecutar en la práctica usando el protocolo de AAA de DIAMETER. La petición inicial Req (IDc) se suplementa con el IDv en el servidor visitado de AAA, y se envía al servidor doméstico de HSS/AAA (posiblemente vía un servidor próximo de AAA). Lo último determina (basándose en la información disponible y en las políticas) que no se permite ninguna delegación, y devuelve un NACK al servidor visitado de AAA. El procedimiento de respuesta a la pregunta se conduce luego entre el autentificador doméstico de HSS/AAA y el cliente.

La figura 5 muestra la señalización asociada en el caso en el que el dominio doméstico decide delegar la responsabilidad de la autentificación por un período limitado o por un número de intentos. Después de recibir la petición, el servidor doméstico de AAA proporciona datos de autentificación al autentificador visitado de AAA. Este último almacena los datos recibidos y procede a autentificar al cliente usando los datos recibidos y un procedimiento de pregunta-respuesta. Pueden realizarse una o más autentificaciones por parte del dominio visitado antes de que deba revertir al dominio doméstico para un refresco (o negación) de la delegación.

La figura 6 muestra la señalización asociada en el caso en el que el dominio doméstico delega la responsabilidad de la autentificación al dominio visitado, pero decide, subsiguientemente, revocar ese permiso. El dominio doméstico hace esto mediante el envío de un mensaje de Revocar (IDc) al autentificador visitado de AAA. Esto forzará, típicamente, al cliente a volver a autentificarse en el dominio doméstico.

Es posible que, en algunos casos, un dominio visitado al cual se ha delegado previamente la responsabilidad de la autentificación (o el cual está configurado para proporcionar autentificación por defecto), pueda pedir que el dominio doméstico cambie el dominio de la autentificación. Esto puede darse, por ejemplo, en las circunstancias siguientes:

El dominio visitado desea reducir su carga de señalización de la autentificación;

El dominio visitado quiere asegurarse de que el dominio doméstico sea consciente, continuamente, de la presencia de su usuario itinerante en el dominio visitado; o

El cliente pide un APN o una QoS que el dominio visitado juzga que requiere autentificación en el dominio doméstico.

Un diagrama de señalización que ilustra este procedimiento se muestra en la figura 7.

La figura 8 muestra un diagrama de señalización que ilustra el caso en el que el dominio doméstico ha determinado que debe ser responsable de la autentificación del cliente, y el dominio visitado, subsiguientemente, pide que la responsabilidad de la autorización sea transferida desde el dominio doméstico al dominio visitado. Esta situación puede presentarse, por ejemplo, cuando un cliente pide un local de APN al dominio visitado o tiene lugar el desglose local, y en cuyos casos el dominio visitado prefiere autentificar al propio cliente.

Haciendo referencia ahora a la figura 9, esta ilustra un flujo de señalización en el caso en el que el cliente (UE) está unido a un dominio de acceso basado en la futura Evolución a Largo Plazo (LTE) del 3GPP (considerando aquí OFDM, Rel8). Típicamente, AAA de DIAMETER se desplegará entre los dominios doméstico y visitado. Aquí, la autentificación inicial del usuario se realiza usando AKA, con el autentificador estando ejecutado en la práctica en el MME dentro del dominio visitado (el “VPLMN”). El HSS dentro del dominio doméstico (el “HPLMN”) proporciona el vector de autentificación necesario para el MME tras la recepción de la petición. La clave de la sesión incluida en el vector de autentificación es pasada por el MME al eNB vía el UPE. El flujo ilustra el caso en el que el HPLMN decide, subsiguientemente, revocar el permiso de autentificación dado previamente al VPLMN, con lo cual el MME envía una AUTH_REQUEST al cliente. El procedimiento de pregunta y respuesta se conduce luego entre el cliente y el HPLMN y, asumiendo que tiene éxito, las claves de la sesión son enviadas desde el HPLMN doméstico al VPLMN.

La figura 10 muestra un flujo de señalización en el caso en el que el cliente está unido a un dominio de acceso de I-WLAN. Típicamente, en el caso de un dominio de acceso de WLAN, la autentificación sería realizada dentro del dominio doméstico. Sin embargo, en este ejemplo, tras la recepción de la EAP_RESPONSE (IMSI), el dominio

doméstico elige delegar la responsabilidad de la autentificación al dominio de acceso. En el caso ilustrado, es el IASA en el VPLMN el que actúa como autentificador después de la delegación. En principio, sin embargo, este papel podría ser realizado por el Nodo de Acceso (AN, en sus siglas en inglés) aunque este enfoque sería menos seguro.

La persona experta en la materia apreciará que pueden hacerse varias modificaciones a las realizaciones descritas más arriba sin apartarse del alcance de la presente invención.

REIVINDICACIONES

1. Un servidor para gestionar la autentificación de los clientes que son abonados de un dominio doméstico dentro del cual está situado el servidor, caracterizado porque el servidor comprende medios (6, 7) para determinar si un cliente que está unido a un dominio visitado va a ser autentificado por el dominio doméstico o por dicho dominio visitado, usando para esta decisión un conocimiento del tipo de seguridad de red que se está usando en una red de acceso del dominio visitado, y para señalar el resultado a dicho dominio visitado, en el que, en el caso de que el cliente va a ser autentificado por el dominio doméstico, dicho resultado es un resultado de autentificación de la red doméstica y, en el caso de que el cliente va a ser autentificado por el dominio visitado, dicho resultado incluye datos de autentificación del dominio doméstico para uso por el dominio visitado para autentificar al cliente.

2. Un servidor según la reivindicación 1 y que comprende una memoria para almacenar datos de autentificación para dichos clientes.

3. Un servidor según la reivindicación 1 o la 2 y que está dispuesto, en caso de que determine que la red visitada va a ser responsable de la autentificación, para generar datos de sesión y enviar esto a dicha red visitada.

4. Un servidor según la reivindicación 3, en el que dichos datos de sesión son un vector de la autentificación.

5. Un servidor según una cualquiera de las reivindicaciones precedentes y que comprende una interfaz (6) para comunicar con los dominios visitados, primeros medios de tratamiento (7) para recibir vía dicha interfaz una petición de registro enviada por un dominio visitado en relación con uno de dichos clientes, y segundos medios de tratamiento (7) para determinar si la petición va a ser autentificada por el dominio doméstico o por el dominio visitado, estando los segundos medios de tratamiento dispuestos, en el caso anterior, para autentificar la petición y señalar el resultado al dominio visitado vía dicha interfaz, y, en el último caso, señalar al dominio visitado vía dicha interfaz que el dominio visitado va a ser responsable de la autentificación de la petición.

6. Un servidor según la reivindicación 5, en el que dichos primeros medios de tratamiento (7) están dispuestos para recibir vía dicha interfaz una petición desde una red visitada para transferir la decisión de autentificación desde un dominio a otro, en el caso de un cliente previamente autentificado, y dichos segundos medios de tratamiento están dispuestos para hacer otra determinación y para notificar a la red visitada, consiguientemente.

7. Un servidor según una cualquiera de las reivindicaciones precedentes y que está dispuesto para determinar que una decisión previa de delegar un procedimiento de autentificación al dominio visitado va a ser revocada, y para señalar esa decisión al dominio visitado.

8. Un servidor según una cualquiera de las reivindicaciones precedentes y que está dispuesto para comunicar con dicho dominio visitado usando un protocolo de AAA.

9. Un servidor según la reivindicación 8, en el que dicho protocolo de AAA es RADIO o DIAMETER.

10. Un servidor según una cualquiera de las reivindicaciones precedentes y que está dispuesto para comunicar con dicho cliente usando el Protocolo de Autentificación Extensible.

11. Un servidor según la reivindicación 10, en el que el método de autentificación es EAP- AKA.

12. Un servidor según una cualquiera de las reivindicaciones 1 a 9 y que está dispuesto para comunicar con dicho cliente usando UMTS AKA.

13. Un método de autentificar a un cliente unido a un dominio visitado, en el que el cliente es un abonado de un dominio doméstico, comprendiendo el método:

enviar una petición de autentificación desde el dominio visitado al dominio doméstico en relación con dicho cliente;

caracterizado por las operaciones de,

en el dominio doméstico, determinar si el cliente va a ser autentificado por el dominio doméstico o por dicho dominio visitado, usando para esta decisión un conocimiento del tipo de seguridad de red que se está usando en una red de acceso del dominio visitado;

en caso de que el cliente vaya a ser autentificado por el dominio doméstico, llevar a cabo dicha autentificación en el dominio doméstico y señalizar el resultado de esta autentificación al dominio visitado; y

en caso de que el cliente vaya a ser autentificado por el dominio visitado, enviar datos de autentificación desde el dominio doméstico al dominio visitado, y usar dichos datos en el dominio visitado para autentificar al cliente.

14. Un método según la reivindicación 13, en el que el dominio doméstico y el dominio visitado se comunican usando un protocolo de AAA, y el dominio doméstico y el cliente se comunican usando el Protocolo de Autentificación Extensible.

15. Un método según la reivindicación 14, en el que el método de EAP-AKA es utilizado para autentificar al cliente.

16. Un método según la reivindicación 13, en el que el método de AKA de UMTS es utilizado para autentificar al cliente.

17. Un método según una cualquiera de las reivindicaciones 13 a 16, en el que dicha operación de determinar si el cliente va a ser autentificado por el dominio doméstico o por el dominio visitado utiliza por lo menos uno de:

- identidad del operador visitado,
- tipo de red de acceso,
- identidad de usuario,
- tipo de autentificación del usuario que se está realizando,
- Nombre de Punto de Acceso (APN) seleccionado,
- requisito de Calidad del Servicio (QoS),
- reglas de carga,
- tipo de suscripción,
- tipo de terminal,
- localización del usuario
- si es, o no, una autentificación inicial.

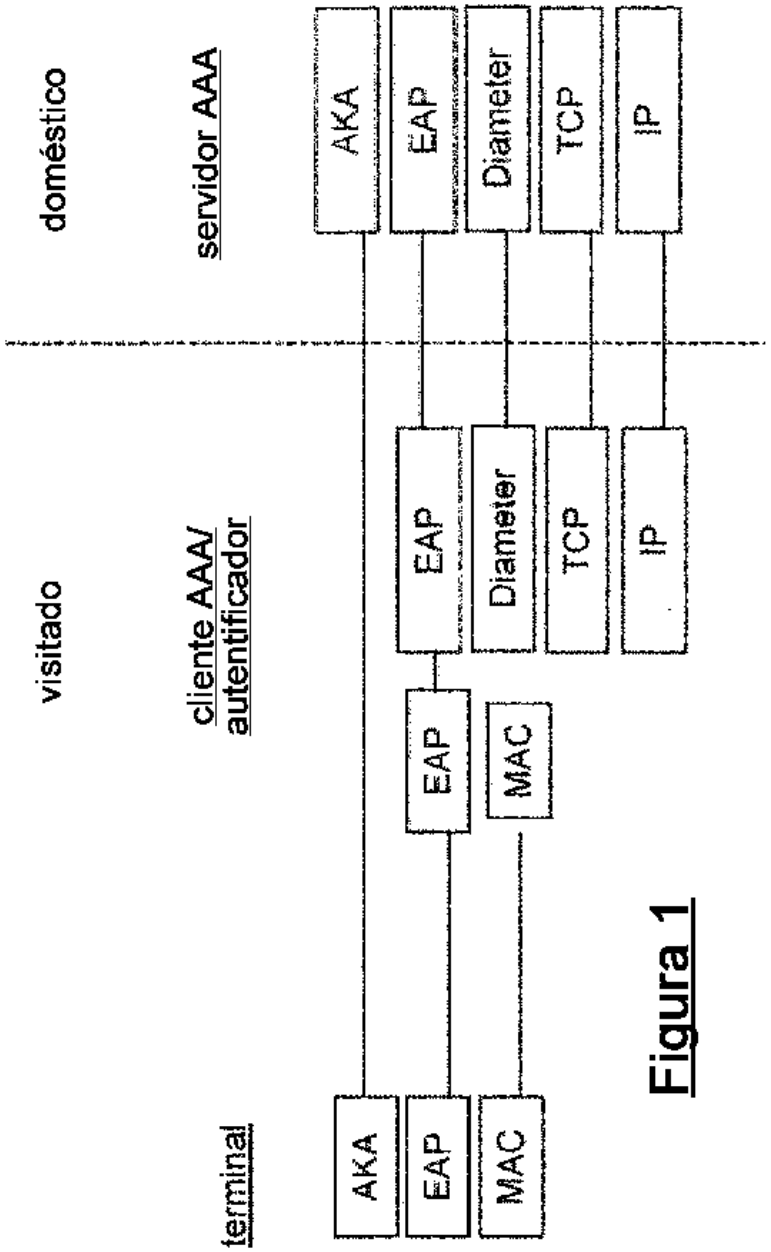
doméstico
visitado
servidor AAA
cliente AAA/
autentificador
terminal
AKA
EAP
Diameter
TCP
IP
EAP
Diameter
TCP
IP
EAP
MAC
AKA
EAP
MAC

Figura 1

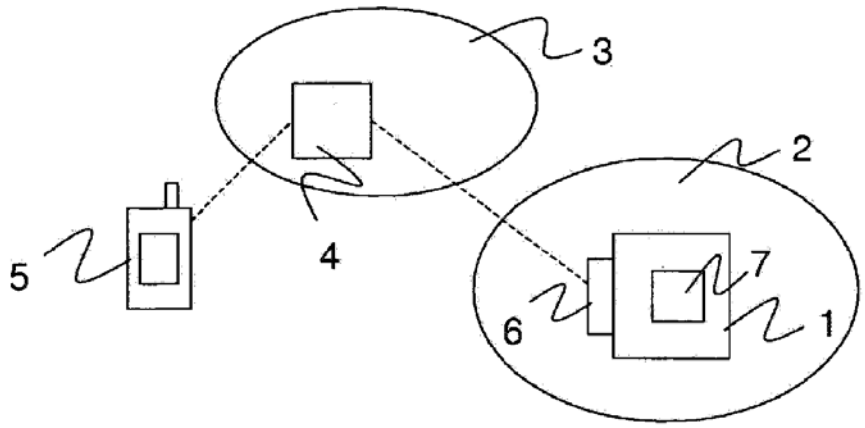

Figura 2

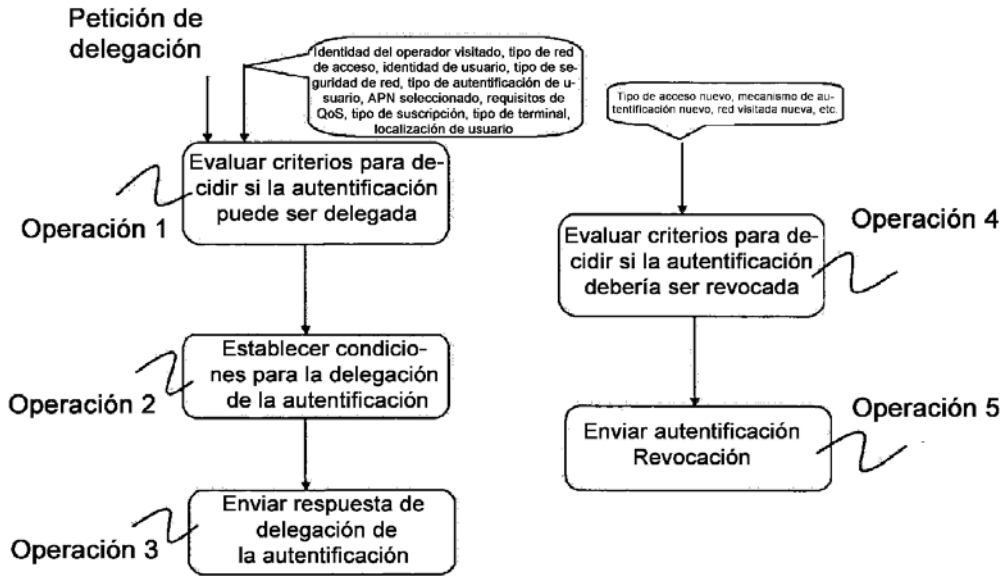

Figura 3a

Figura 3b

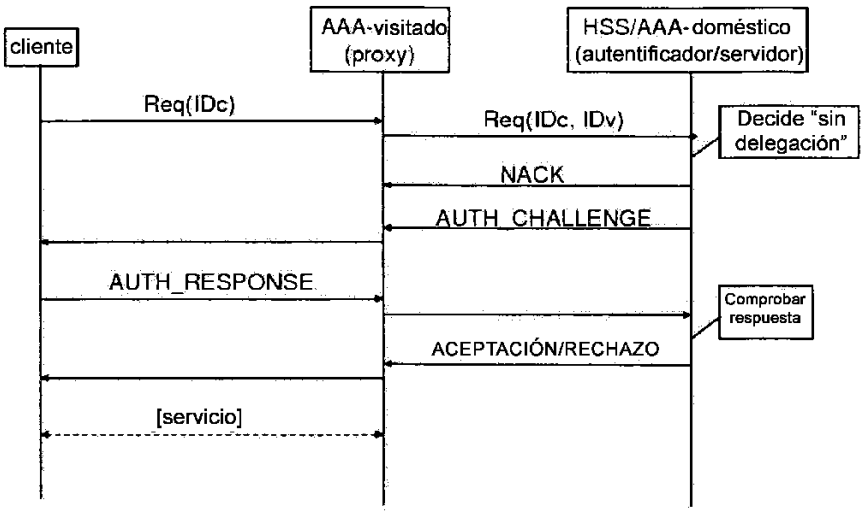

Figura 4

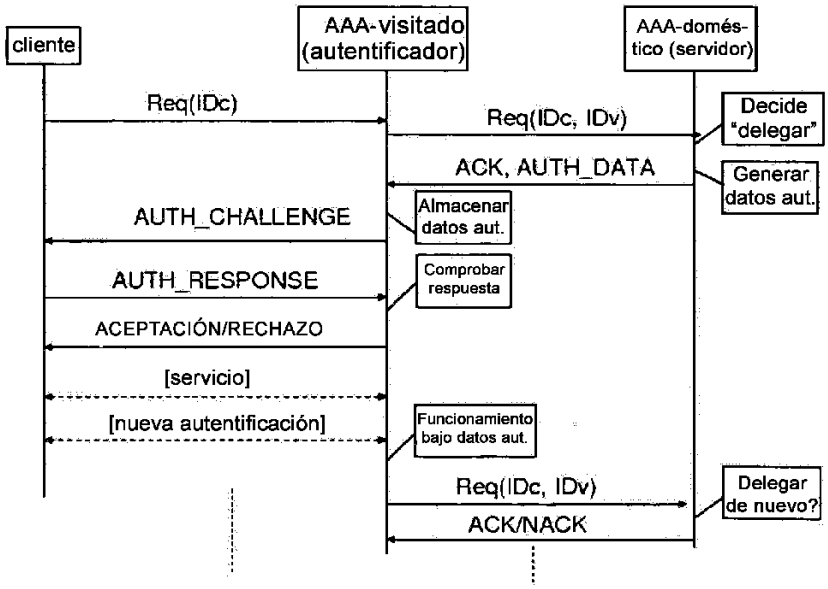

Figura 5

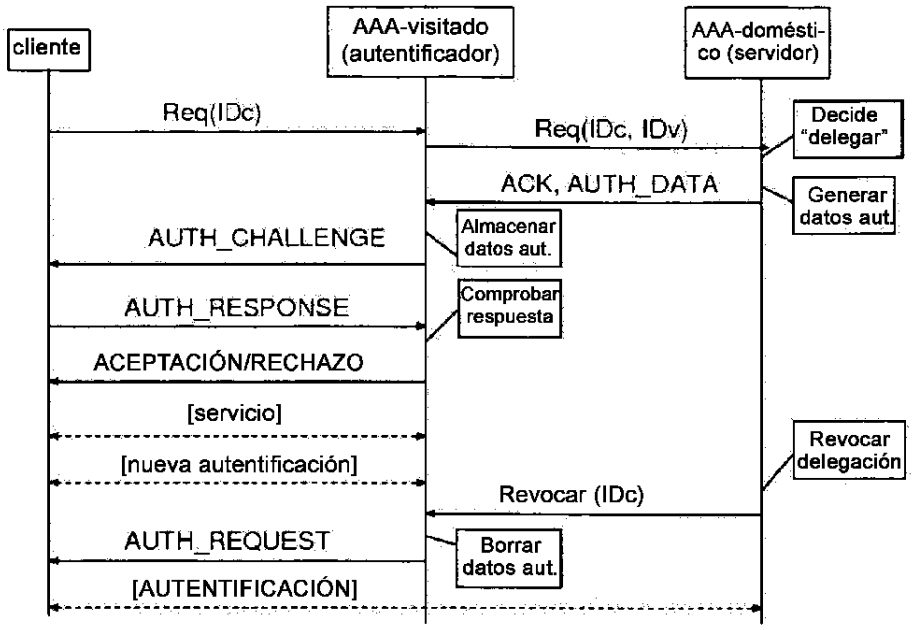

Figura 6

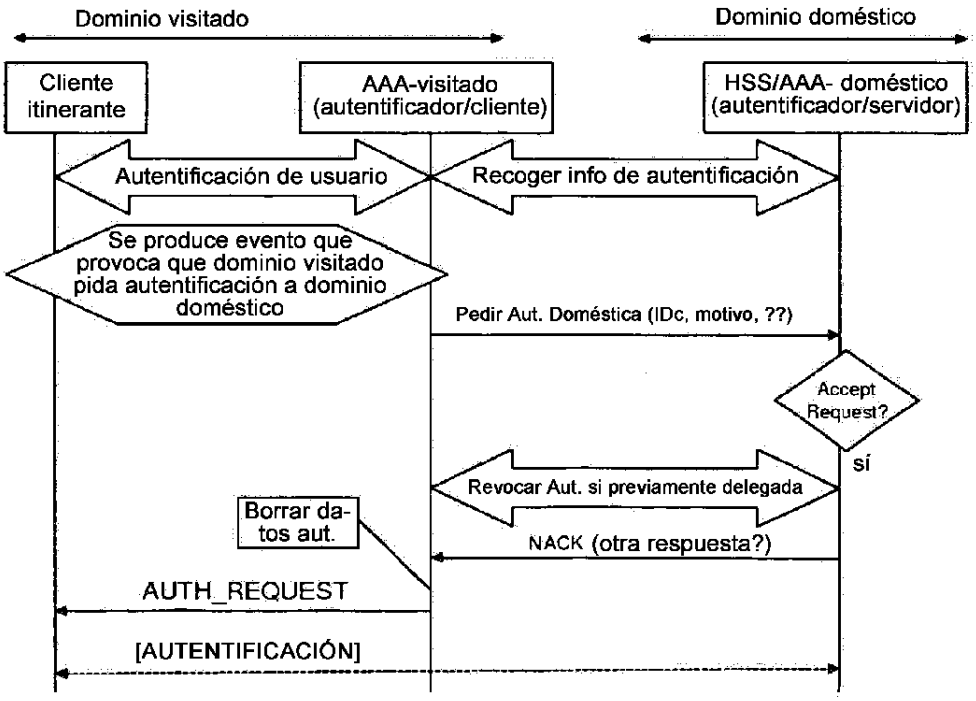

Figura 7

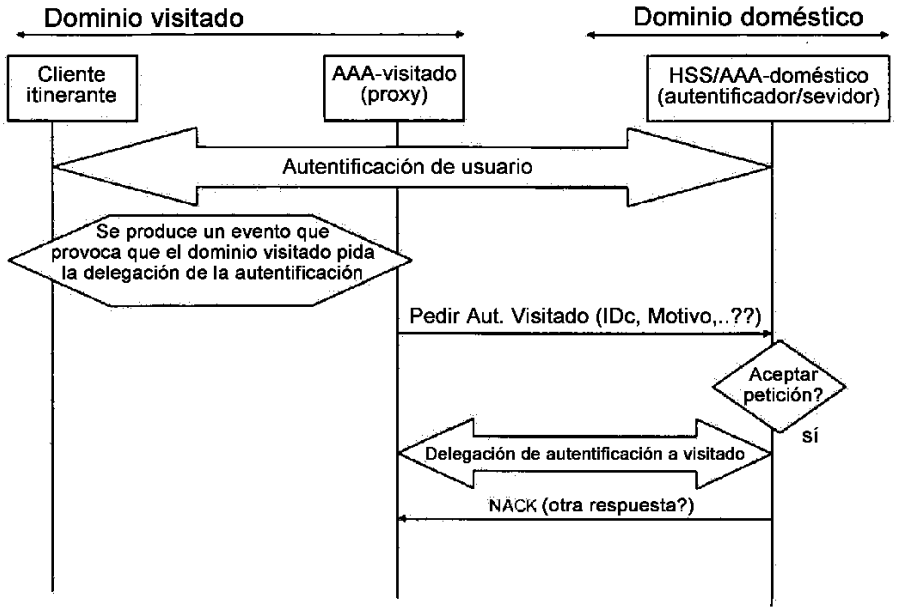

Figura 8

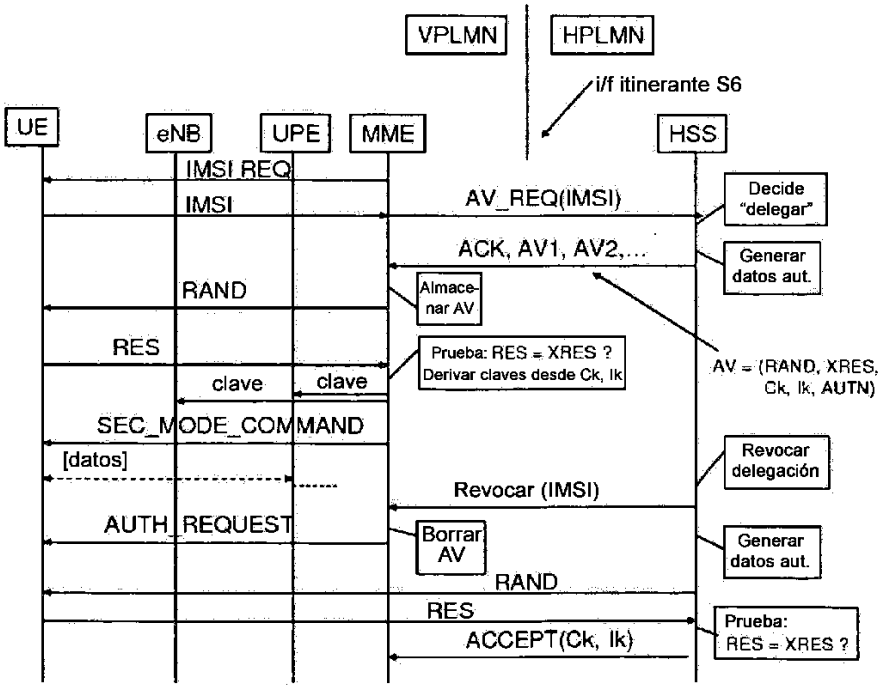

Figura 9

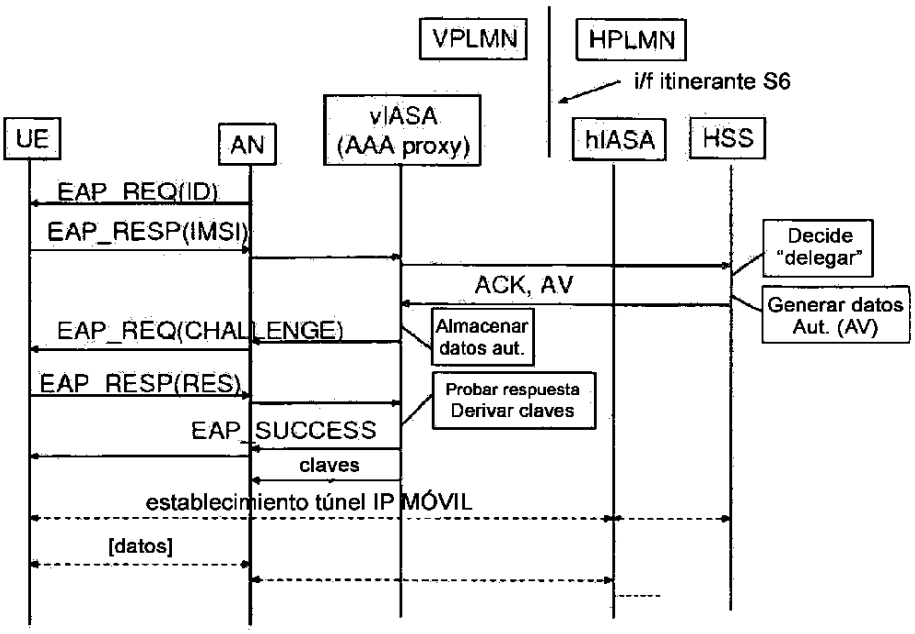
VPLMN
HPLMN
i/f itinerante S6
UE
AN
vIASA
(AAA proxy)
hIASA
HSS
EAP_REQ(ID)
EAP_RESP(IMSI)
Decide
"delegar"
ACK, AV
Generar datos
Aut. (AV)
EAP_REQ(CHALLENGE)
Almacenar
datos aut.
EAP_RESP(RES)
Probar respuesta
Derivar claves
EAP_SUCCESS
claves
establecimiento túnel IP MÓVIL
[datos]

Figura 10