(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 616 499**

(15) Folleto corregido: T3

Texto afectado: Descripción

(48) Fecha de publicación de la corrección: 19.09.2017

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA CORREGIDA T9

(86) Fecha de presentación y número de la solicitud internacional: **12.10.2004 PCT/IB2004/003313**

(87) Fecha y número de publicación internacional: **21.04.2005 WO05036852**

(96) Fecha de presentación y número de la solicitud europea: **12.10.2004 E 04769606 (7)**

(97) Fecha y número de publicación de la concesión europea: **23.11.2016 EP 1673916**

(54) Título: **Aparatos y método para autenticación en redes de IP heterogéneas**

(30) Prioridad:

13.10.2003 US 510787
08.10.2004 US 960641

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.06.2017

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

MALINEN, JARI T.;
KNIVETON, TIMOTHY J. y
SAHASRABUDHE, MEGHANA

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Aparatos y método para autenticación en redes de IP heterogéneas

Antecedentes de la invención:

Campo de la invención:

La presente invención se refiere a un sistema y a un método para autenticar y autorizar servicios de red.

Descripción de la técnica relacionada:

En las arquitecturas de sistema de 3G (tercera generación) futuras, los servicios de red se pueden proporcionar a través de muchos métodos de acceso de red diferentes, por ejemplo CDMA2000 (*Code Division Multiple Access, version 2000*, Acceso Múltiple por División de Código, versión 2000), red basada en IP no celular, LAN (*Local Area Network*, Red de Área Local) Inalámbrica 802.11, Bluetooth o Ethernet. No obstante, en 3GPP2, en la actualidad los dispositivos móviles solo son capaces de acceder a servicios de red usando métodos de acceso de CDMA2000. Por lo tanto, con el fin de proporcionar servicios de red de forma más fiable y eficiente, existe una necesidad de permitir a los dispositivos móviles la capacidad de autenticarse a través de diferentes tipos de redes de acceso de tal modo que diferentes redes de acceso puedan autorizar servicios.

No existe proceso de autenticación universal alguno para autenticar a un usuario (terminal) en ningún tipo de tecnología de acceso de red. Y esto hace que sea difícil obtener acceso y movilidad de sesiones en un escenario de acceso múltiple. Es necesario un intercambio de mensajes entre la red y la estación móvil, para permitir una provisión de servicio en una red de IP genérica, celular o no celular, para usar la misma autoridad. No obstante, existe el problema de que es necesario que el terminal use algún otro método para autenticarse a sí mismo con la red del operador y recibir servicio si este no está usando la red celular de CDMA2000.

Problemas similares tienen lugar cuando se usa una microplaca de R-UIM que contiene la identidad de un usuario para el uso de teléfonos celulares móviles en redes de CDMA, similar a cómo las tarjetas de SIM (*Subscriber Identity Module*, Módulo de Identidad de Abonado) contienen la identidad de un usuario en las redes de GSM (*Global System for Mobile communication*, Sistema Global para comunicaciones Móviles). El R-UIM se describe en el documento de 3GPP2 C.S0023-0.

Por ejemplo, si el terminal está usando una radio de Bluetooth o WLAN (*Wireless LAN*, LAN Inalámbrica) para sus conexiones, por ejemplo, con Internet, y está usando la misma identidad de registro a partir del módulo R-UIM, el mismo necesita un protocolo no celular separado para lograr esto, que es el problema que aborda la presente solicitud.

El documento "*Dynamic Network Interface Selection in Multi Homed Mobile Host*", XP010626772 describe un mecanismo de selección de interfaz para anfitriones móviles de bases múltiples. Este mecanismo permite una toma dinámica de decisiones durante la operación de un dispositivo móvil.

El documento US 2003/119481 A1 divulga un método de cómo un equipo de terminal puede seleccionar una red móvil terrestre pública particular. Con detalle, el equipo de terminal selecciona una red móvil pública por medio de una comparación de un identificador de red móvil terrestre pública recibido e identificadores móviles terrestres públicos que se almacenan en el equipo de terminal.

Sumario de la invención:

El objetivo que subyace a la presente invención radica en proporcionar una posibilidad para que un dispositivo móvil se autentique a través de diferentes tipos de redes de acceso.

El presente objetivo se consigue por medio de un sistema tal como se expone en la reivindicación 1, un método tal como se expone en la reivindicación 14, un dispositivo de control de acceso tal como se expone en la reivindicación 22, o mediante un dispositivo de abonado tal como se expone en la reivindicación 29.

Por lo tanto, de acuerdo con la invención, el dispositivo móvil recibe información en lo que respecta a un tipo de acceso de red (este mensaje de información puede ser un mensaje explícito que se envía al dispositivo móvil o puede ser una información que se encuentra generalmente disponible en la red). El dispositivo móvil crea un mensaje de inicio que contiene la identidad de usuario y envía este en un mensaje de autenticación a un controlador de acceso. El controlador de acceso evalúa el mensaje de inicio y lo reenvía al servidor de autenticación correcto.

Por lo tanto, es necesario que el dispositivo móvil aborde solo un controlador de acceso, que reenvía el mensaje de autenticación al servidor de autenticación correcto. Es decir, no es necesario que el dispositivo móvil halle cómo se va a alcanzar el servidor de autenticación.

Además, también se puede proporcionar una pluralidad de servidores de autenticación para diferentes servicios. De acuerdo con la técnica anterior tal como se ha descrito en lo que antecede, el dispositivo móvil tendría que enviar una pluralidad de mensajes de autenticación a todos los diferentes servidores de autenticación cuyos servicios se van a usar. En contraste con lo anterior, de acuerdo con la presente invención, el dispositivo móvil solo ha de enviar un mensaje de inicio en el que están encapsulados una pluralidad de mensajes de autenticación que se corresponden con los servidores de autenticación.

Por lo tanto, se simplifica el procedimiento de autenticación. Además, también la carga de tráfico en la red se reduce debido a que solo se requiere un único mensaje de inicio a pesar de que se vaya a usar una pluralidad de servicios.

Algunos desarrollos ventajosos se definen en las reivindicaciones dependientes.

Por ejemplo, el mensaje de información puede indicar un soporte de protocolo de autenticación extensible (EAP).

El mensaje de información se puede expedir cuando el dispositivo móvil entra en una red.

El mensaje de inicio puede contener un mensaje de opción de identificador de cliente y un mensaje de opción de identidad de soporte de protocolo de autenticación extensible, en el que dichos mensajes contienen información en lo que respecta a al menos uno de tipo de cliente, identidad de usuario e información acerca de cómo abordar al cliente en el interior de la red de IP medular (a la que se hace referencia en lo siguiente también como información de dirección medular).

Un protocolo entre el dispositivo móvil y la red de acceso puede comprender al menos uno de protocolos de capa de red como UDP, ICMP, ICMPv6 o protocolos de capa de enlace como IEEE 802.1x, IEEE 802.11i y un perfil de Bluetooth.

Un mecanismo de autenticación que se aplica puede comprender un protocolo de autenticación extensible (EAP).

Un mecanismo de autenticación que se aplica puede ser un mecanismo de autenticación que usa un módulo de identidad de usuario extraíble (R-UIM, *Removable User Identity Module*) que aplica un algoritmo de Autenticación Celular y Cifrado de Voz (CAVE, *Cellular Authentication and Voice Encryption*), o un USIM que aplica que aplica el algoritmo de AKA

Breve descripción de los dibujos:

La figura 1 muestra un modelo de referencia de red de acceso múltiple de CDMA2000 de acuerdo con las realizaciones de la invención;

la figura 2A y 2B un flujo de señales de acuerdo con un primer ejemplo de una primera realización de la invención;

la figura 3A y 3B un flujo de señales de acuerdo con un segundo ejemplo de la primera realización de la invención;

la figura 4A y 4B un flujo de señales de acuerdo con un primer ejemplo de una segunda realización de la invención;

la figura 5A y 5B un flujo de señales de acuerdo con un segundo ejemplo de la segunda realización de la invención, y

las figuras 6A, 6B y 6C un controlador de acceso, una estación móvil y un encaminador utilizable de acuerdo con las realizaciones de la invención.

Descripción detallada de las realizaciones preferidas:

Tal como se ha descrito en lo que antecede, de acuerdo con la invención, se proporciona un sistema para autenticar y autorizar servicios de red, que comprende: un encaminador para expedir un anuncio de encaminador que contiene que indica un tipo de acceso de red y un soporte de protocolo de autenticación extensible; un dispositivo móvil que tras la recepción del anuncio de encaminador determina el tipo de acceso de red y crea un mensaje de inicio que contiene un mensaje de opción de identificador de cliente y un mensaje de opción de identidad de EAP (*Extensible Authentication Protocol*, Protocolo de Autenticación Extensible), que contienen tipo de cliente, identidad de usuario e información de dirección medular, encapsula adicionalmente el mensaje de inicio en un protocolo IPv4 o IPv6 compatible con una red de acceso que se identifica en el anuncio de encaminador, por ejemplo UDP, ICMPv6 (*Internet Control Message Protocol version 6*, Protocolo de Mensajes de Control de Internet versión 6 (para IPv6)), o un protocolo de capa de enlace como IEEE 802.1x, IEEE 802.11i o un perfil de Bluetooth adecuado, y un controlador de acceso para leer el mensaje encapsulado a partir del móvil y reenviar el mensaje encapsulado a un servidor de

autenticación que se identifica en el mensaje encapsulado.

Se pueden usar varios mecanismos de autenticación. En la siguiente descripción de las realizaciones preferidas, se toman como ejemplos el mecanismo de autenticación de EAP-AKA (*Authentication and Key Agreement*, Autenticación y Acuerdo de Claves) que usa un USIM (*Universal Subscriber Identity Module*, Módulo de Identidad de Abonado Universal) (la primera realización) y un mecanismo de autenticación que usa R-UIM (*Removable User Identity Module*, Módulo de Identidad de Usuario Extraíble) que aplica un algoritmo de CAVE (*Cellular Authentication and Voice Encryption*, Autenticación Celular y Cifrado de Voz) (la segunda realización).

Una primera realización se refiere a un uso combinado de redes de datos por paquetes celulares y no celulares de CDMA2000 y, en concreto, se refiere a la autenticación de usuario y la autorización de servicios usando un Módulo de Identidad de Abonado Universal (USIM, *Universal Subscriber Identity Module*) al comunicarse a través de múltiples tipos de redes de acceso usando la especificación de EAP-AKA. Esta capacidad es útil para automatizar la gestión de claves aprovechando la infraestructura de claves existente para autenticaciones no de datos, tal como se ha mostrado con métodos similares en otros entornos celulares. La autenticación del usuario y la autorización del servicio permite que el operador celular proporcione al usuario diversos tipos de red de acceso, al tiempo que se mantiene una provisión de servicio unificada, una gestión de acceso de red basada en usuario y una autenticación de itinerancia, al tiempo que se aprovecha todo esto de la infraestructura de autenticación / contabilidad / facturación existente. El beneficio se puede resumir como una unificación de autenticación de CDMA2000 basada en tarjeta inteligente para múltiples métodos de acceso.

La realización describe una forma de acceso de red, señalización de movilidad, y otra autenticación de servicios para los usuarios de WLAN / CDMA2000. En particular, de acuerdo con la primera realización, se proporciona un esquema de acceso múltiple en el que la autenticación de red a partir de la WLAN, así como protección de señalización de gestión de movilidad, usa la combinación especial de protocolos de AAAv6 (*Authentication, Authorization and Accounting for Ipv6*, Autenticación, Autorización y Contabilidad para Ipv6), EAP-AKA (*Extensible Authentication Protocol Authentication and Key Agreement*, Protocolo de Autenticación Extensible - Autenticación y Acuerdo de Claves) y de Radius, así como la arquitectura de acceso múltiple específica de CDMA2000 para el método presentado.

Tal como se ha descrito en lo que antecede, de acuerdo con la primera realización, se ha de solucionar el problema de que es necesario que el terminal use algún otro método para autenticarse a sí mismo con la red del operador y recibir servicio si este no está usando la red celular de CDMA2000. De acuerdo con la presente realización, el problema se supera mediante la definición de un método para autenticar a un usuario usando la especificación de EAP-AKA para ejecutarse a través de cualquier tecnología de acceso y medular siempre que el usuario tenga un USIM que contenga la identidad del usuario, tal como se describirá en lo siguiente con detalle.

De acuerdo con la primera realización, el mecanismo de autenticación de EAP-AKA (tal como se define en J. Arkko, H. Haverinen. *EAP AKA Authentication (work in progress)*, Borrador de Internet (draft-arkko-pppext-eap-aka-10.txt), Grupo de Tareas Especiales de Ingeniería en Internet, junio de 2003, por ejemplo) se aplica para autenticar a un usuario en la red que esté usando cualquier tecnología de acceso de red. Por lo tanto, se logra una autenticación mutua, una autorización de red y una provisión de servicio mediante una interacción entre múltiples partes (pero sin limitarse a) las siguientes entidades: terminal, USIM (*Universal Subscriber Identity Module*, Módulo de Identidad de Abonado Universal), Controlador de Acceso, Pasarela de Autenticación y el Centro de Autenticación (AuC, *Authentication Center* / HLR (*Home Location Register*, Registro de Posiciones Propio, el AuC está ubicado en el HLR)) de la red de CDMA2000. En lo siguiente, este se describe con detalle cómo se puede lograr esto.

La figura 1 muestra un modelo de referencia de red de acceso múltiple de CDMA2000, en el que también se proporcionan, en particular, el controlador de acceso (AC, *Access controller*) y el Servidor de Autenticación (AS, *Authentication Server*).

En la parte superior izquierda de la figura 1, se muestra una red de proveedor de acceso visitada (en particular, la red de servicio). Una red de radio (RN, *radio network*) de origen está conectada con una PDSN de servicio por medio de una interfaz de RAN-PDSN (interfaz de R-P). A10 y A11 son unas interfaces para mensajes de control que se definen en CDMA2000. La PDSN (*Packet Data Serving Network*, Red de Servicio de Datos por Paquetes) actúa como un agente extraño, y proporciona acceso a Internet, intranets y servidores de Protocolo de Aplicación Inalámbrica (WAP, *Wireless Application Protocol*) para estaciones móviles y similares. La RN de origen también está conectada con un Centro de Conmutación de Servicios Móviles (MSC, *Mobile Services Switching Center*) por medio de una interfaz A1.

El MSC está conectado con la red de proveedor de acceso propia de la estación móvil por medio de una red de SS7. La red de proveedor de acceso propia comprende un Registro de Posiciones Propio (HLR, *Home Location Register*) y un Centro de Autenticación (AuC, *Authentication Center*), que es necesario de acuerdo con las realizaciones que se describen en lo siguiente.

En la parte central izquierda de la figura 1, se muestra una red de proveedor de acceso visitada objetivo, con la que

se puede conectar una estación móvil. La red de proveedor de acceso objetivo comprende una RN objetivo y una PDSN objetivo, que están conectadas por medio de una interfaz de R-P similar a como es en la red de proveedor de acceso visitada de servicio. Ambas PDSN también están conectadas con una red de IP (Protocolo de Internet versión 4 (Ipv4, *Internet Protocol version 4*) y / o Protocolo de Internet versión 6 (Ipv6, *Internet Protocol versión 6*)). Para esta conexión, en CDMA2000 se define una interfaz Pi. La PDSN de servicio también está conectada con un servidor de AAAL (*Local AAA*, (*Authentication, Authorization and Accounting*), AAA (Autenticación, Autorización y Contabilidad) Local), que también tiene acceso a la red de IP.

En el lado derecho de la figura 1, se muestra la red de proveedor de acceso propia que se ha descrito en lo que antecede, una red de IP propia que está conectada con la red de IP y que comprende una AAAH (*Home AAA*, AAA Propia), y una red de intermediario que comprende un servidor de AAA. Además, se ilustra el Agente Propio (HA, *Home Agent*), que se puede disponer en la red de IP propia, en una red privada o en la red de proveedor de acceso propia.

Una posibilidad de acceso adicional para la estación móvil se muestra en la parte inferior izquierda de la figura 1, en la que se ilustra una red de proveedor de acceso visitada objetivo adicional. Este es el escenario para las realizaciones que se describen en lo siguiente. En el presente caso, la estación móvil conecta con una WLAN (*Wireless Local Area Network*, Red de Área Local Inalámbrica) objetivo. La WLAN está conectada por medio de una interfaz de IP con un Controlador de Acceso (AC, *Access Controller*) que se describirá con más detalle más adelante. El AC está conectado con un Servidor de Acceso (AS, *Access Server*), que proporciona una conexión con la red de IP y también con la red de proveedor de acceso propia, en particular con el AuC de la red de proveedor de acceso propia.

Las nuevas funcionalidades (es decir, los dispositivos que comprenden las nuevas funcionalidades) de acuerdo con las realizaciones que se describen en lo siguiente se indican mediante recuadros a rayas. Es decir, estas nuevas funcionalidades se encuentran en el AC y el AS. Además, de forma opcional, el AS se puede proporcionar en el AAAH de la red de IP propia.

El terminal es un dispositivo que necesita ser capaz de obtener acceso a todos los tipos de redes de IP, incluyendo la red de IP que es parte de la red celular y también la red de acceso OWLAN (*Operator Wireless LAN*, LAN de Operador Inalámbrica). También es necesario que el terminal sea capaz de ejecutar los algoritmos de AKA al tener un USIM. Y también es necesario que este ejecute el protocolo IPv6. Si se usa MIPv6, este proceso también se puede utilizar para crear, de forma dinámica, Asociaciones de Seguridad entre el Agente Propio y el terminal. La especificación de EAP-AKA muestra cómo se puede llevar a cabo la autenticación de AKA usando mensajes de EAP. De acuerdo con la presente realización, se describe cómo se puede usar esta especificación para la autenticación con independencia de la tecnología de acceso.

En el momento en el que el terminal entra en una red capaz de esta funcionalidad, este recibe un Anuncio de Encaminador (RA, *Router Advertisement*), que incluye una indicación de soporte, por ejemplo, una opción de anuncio de encaminador o de agente a partir del AC local (*Access controller*, controlador de Acceso) que indica este tipo de soporte de AAA (*Authentication, Authorization and Accounting*, Autenticación, Autorización y Contabilidad). Esto inicia la autenticación, la generación de claves y la provisión de servicio de acuerdo con la presente realización.

Los mensajes de EAP están encapsulados o bien en mensajes de AAAv6 o bien en la capa de enlace de WLAN (tal como en IEEE 802.1x, IEEE 802.11i o en un mensaje de perfil de Bluetooth adecuado, en encapsulación de EAP de PPP, o en cualquier mensaje de protocolo de PANA de último salto adecuado, según se normalice en el futuro) cuando se intercambian estos entre el terminal y el controlador de acceso, que es el elemento de red responsable de controlar el acceso de los usuarios a la red de IP. Si se usa AAAv6, el mensaje de identidad de EAP / AKA inicial va en el mensaje de Identidad de EAP en el mensaje de AAAv6.

Entre el controlador de acceso y el Servidor de Autenticación, los mensajes de EAP se portan en un protocolo de red medular como Diameter o Radius. El AC determina la dirección de IP del Servidor de Autenticación mediante la asignación del mismo a partir de la IMSI (*International Mobile Subscriber Identity*, Identidad de Abonado Móvil Internacional) y el dominio. El Servidor de Autenticación tiene una interfaz lógica con el HLR / Centro de Autenticación (AuC, *Authentication Center*) a través del MSC. Este actúa como una pasarela entre el protocolo MAP (red de SS7) y los protocolos de autenticación que se usan en IP.

Un escenario para autenticar al usuario en una red de OWLAN de acuerdo con la presente realización se describe en lo siguiente con flujos de mensaje.

1. El terminal envía un mensaje de solicitud de acceso (que podría ser un mensaje de Solicitud de AAAv6 o cualquier otro mensaje para solicitar un acceso de red) al controlador de acceso. El mensaje de Respuesta de EAP / Identidad de AKA está insertado en este mensaje. Asimismo, es necesario que exista una provisión de pasar el NAI de usuario en este mensaje.
2. El controlador de acceso capta el mensaje de EAP y lo coloca en un mensaje de solicitud (que podría ser un mensaje de Solicitud de AA de Diameter o un mensaje de Solicitud de Acceso de Radius) que se envía en la red

medular al Servidor de Autenticación (AS, *Authentication Server*). Por ejemplo, en Diameter, el mensaje de EAP se encontraría en el AVP de cabida útil de EAP. El controlador de acceso resuelve a qué AS debería ir la solicitud, basándose en la parte de dominio del NAI de usuario.

3. Con la recepción del mensaje, el AS identifica en primer lugar el AuC que contiene la información de autenticación para el usuario. Esto podría estar basado en la parte de usuario del NAI de usuario. Por ejemplo, si el NAI de usuario que se usa es de la forma IMSI@dominio, entonces la IMSI se puede usar para identificar el HLR / AuC de usuario. Este solicita el quintete de autenticación de UMTS a partir del AuC. Este quintete consiste en cinco valores, en concreto, a) una puesta a prueba de red RAND, b) una respuesta esperada por el usuario XRES, c) una clave de cifrado CK, d) una clave de integridad IK y e) un testigo de autenticación de red AUTN. Con la obtención de estos valores, este crea los atributos AT_RAND (un número aleatorio), AT_AUTN (un vector de autorización) y AT_MAC (*message authentication code*, código de autenticación de mensaje). Este calcula y almacena el valor AT_RES para su uso posterior. Este crea el mensaje de Solicitud de EAP / AKA / Puesta a Prueba que contiene el valor de AT_RAND, el valor de AT_AUTN y el valor de AT_MAC. Por último, este envía un mensaje, que contiene el mensaje de Solicitud de EAP / AKA / Puesta a Prueba en el mismo y el NAI que identifica al usuario (en el atributo de Nombre de Usuario), al AC. El mensaje podría ser un mensaje de Respuesta de AA de Diameter o un mensaje de Puesta a Prueba de Acceso de Radius. Si este es un mensaje de Diameter, el mensaje de EAP se porta en el AVP de cabida útil de EAP.

4. El AC envía un mensaje al terminal que contiene la Solicitud de EAP / AKA / Puesta a Prueba. Este puede ser un mensaje de AAAv6 o cualquier otro protocolo de acceso de red en uso entre el terminal y el controlador de acceso.

5. Cuando el terminal recibe este mensaje, este extrae en primer lugar el mensaje de Solicitud de EAP / AKA / Puesta a Prueba. Entonces, este usa el AKA para calcular los valores de AT_RES, dando los valores de AT_RAND y de AT_MAC que se reciben en el interior de la Solicitud de EAP / AKA / Puesta a Prueba como una entrada al AKA. Este también calcula el valor de AT_AUTN y lo compara con el AT_AUTN que se recibe en la Solicitud de EAP / AKA / Puesta a Prueba. Si estos valores coinciden, el mensaje de Solicitud de EAP / AKA / Puesta a Prueba se autentica con éxito, de lo contrario, el mensaje de autenticación falla. Si los valores han coincidido, este crea y envía un mensaje (AAAv6) al AC que contiene el mensaje de Respuesta de EAP / AKA / Puesta a Prueba. El mensaje de Respuesta de EAP / AKA / Puesta a Prueba contiene el valor de AT_RES calculado.

6. El AC envía de nuevo un mensaje de solicitud (Solicitud de AA de Diameter / Solicitud de Acceso de Radius). Esta vez, este contiene la Respuesta de EAP / AKA / Puesta a Prueba.

7. Cuando el AS recibe este mensaje, este compara el valor de AT_RES que el mismo había calculado anteriormente con el valor de AT_RES en el mensaje de EAP recibido. Si los valores coinciden, la autenticación de AKA tiene éxito; de lo contrario, la autenticación falla. Dependiendo del resultado, este envía o bien un mensaje de Aceptación de Acceso o bien uno de Rechazo de Acceso (en el caso de Radius). Para Diameter, este envía un mensaje de Respuesta de AA con el resultado en el AVP de Código de Resultado.

8. Con la recepción de este mensaje, el AC sabe si la autenticación tuvo éxito o no. El Ac envía el mensaje de respuesta apropiado al terminal. Cuando el terminal recibe este mensaje, la autenticación de red de acceso de OWLAN se ha completado. Si la autenticación tuvo éxito, el AC aplicará una regla de filtrado que permite que pasen los paquetes que se envían a partir del terminal autenticado.

A continuación, el procedimiento anterior se describe con algo de más detalle al hacer referencia al diagrama de flujo de señales que se muestra en las figuras 2A y 2B. El diagrama de flujo de señales ilustra las señales que se intercambian entre el terminal (term., es decir, el UE), el Centro de Autenticación (AC, *Authentication Center*) y el Servidor de Autenticación (AS, *Authentication Server*).

En la etapa 2-A, el terminal recibe un Anuncio de Encaminador (o bien no solicitado o bien solicitado) a partir del AC. El Anuncio de Encaminador (RA, *Router Advertisement*) incluye la Opción de Puesta a Prueba de AAA que contiene la Puesta a Prueba Local. Antes de enviar el siguiente mensaje, el terminal ha de haber adquirido una dirección de IP asignada (en el caso de una dirección de IPv4 a partir de, por ejemplo, un servidor de DHCP (*Dynamic Host Configuration Protocol*, Protocolo Dinámico de Configuración de Ordenador Principal). En el caso de una dirección de IPv6, esta podría ser una dirección autoconfigurada).

En la etapa 2-B, el terminal deduce a partir de la presencia de un indicador de AAA en el Anuncio de Encaminador que es necesario realizar una autenticación de acceso de AAA. El terminal comienza la secuencia de autenticación mediante el envío de un mensaje de Solicitud de AAA (que se indica mediante RQ1) al AC. La Solicitud de AAA contiene una Opción de Identificador de Cliente de AAA (que se indica en el diagrama de flujo de señales como cID) así como una opción que porta el mensaje de Identidad de EAP. Tanto la Opción de Identificador de Cliente de AAA como el mensaje de Identidad de EAP contienen el NAI del usuario (IMSI@dominio).

En la etapa 2-C, el AC obtiene la dirección del AS a partir del NAI que está contenido en la Opción de Identificador de Cliente de AAA (usando un DNS, si es necesario) y envía un mensaje de Solicitud de AAA (AR, *AAA Request*) al AS. La AR contiene el mensaje de Identidad de EAP (en el atributo de cabida útil de EAP) y el NAI (en el atributo de Nombre de Usuario) que se recibe en la Opción de Identificador de Cliente de AAA en la etapa B.

En la etapa 2-D, el AS realiza lo siguiente tras la recepción del mensaje de AR en la etapa 2-C:

- Basándose en la parte de IMSI del NAI, el AS identifica el AuC que contiene la información de autenticación para el usuario.
- Este pregunta y obtiene un quintete de autenticación de UMTS a partir del AuC. Este consiste en 5 valores:

  a) una puesta a prueba de red RAND, b) una respuesta esperada por el usuario XRES, c) una clave de cifrado CK, d) una clave de integridad IK y e) un testigo de autenticación de red AUTN.

- Este calcula los valores AT_RAND (un número aleatorio), AT_AUTN (un vector de autorización) y AT_MAC (*message authentication code*, código de autenticación de mensaje). Este calcula y almacena el valor AT_RES para su uso posterior (que se obtiene a partir de la XRES).
- Este crea el mensaje de Solicitud de EAP / AKA / Puesta a Prueba que contiene el valor de AT_RAND, el valor de AT_AUTN y el valor de AT_MAC.
- Este envía un mensaje de Puesta a Prueba de Acceso (AA, *AAA Answer*), que contiene la Solicitud de EAP / AKA / Puesta a Prueba (en el atributo específico del fabricante de 3GPP2) y el NAI que identifica al usuario (en el atributo de Nombre de Usuario), al AC.

En la etapa 2-E, el AC envía un mensaje de Respuesta de AAA (RP2), que contiene la Solicitud de EAP (ERq en el diagrama de flujo de señales) / AKA / Puesta a Prueba en la Opción de Datos Insertados de AAAv6, una Opción de Identificador de Cliente de AAA que contiene el NAI y una Opción de Puesta a Prueba de AAAv6, al terminal. La Opción de Puesta a Prueba de AAAv6 contiene un valor de Puesta a Prueba Local que es ajustado por el AC.

En la etapa 2-F, el terminal realiza lo siguiente tras la recepción de la Respuesta de AAA en la etapa 2-E:

- Este usa el AKA para calcular los valores de AT_RES, dando los valores de AT_RAND y de AT_MAC que se reciben en el interior de la Solicitud de EAP / AKA / Puesta a Prueba como una entrada al AKA.

- Este calcula el valor AT_AUTN tal como se especifica en AKA.

- Este compara el valor de AT_AUTN calculado con el valor que se recibe en la Solicitud de EAP / AKA / Puesta a Prueba. Si los valores coinciden, el mensaje de Solicitud de EAP / AKA / Puesta a Prueba se autentica con éxito, de lo contrario, el mensaje de autenticación falla.

- Este envía un mensaje de Solicitud de AAA (RQ3), que contiene la Puesta a Prueba Local en una Opción de Puesta a Prueba de AAAv6, una Opción de Identificador de Cliente de AAA (NAI de la forma IMSI@dominio) y un mensaje de Respuesta de EAP (ER, *EAP Response*) / AKA / Puesta a Prueba en la Opción de Datos Insertados de AAAv6, al AC. La Respuesta de EAP / AKA / Puesta a Prueba contiene el valor de AT_RES calculado.

En la etapa 2-G, el AC envía un mensaje de Solicitud de AAA (AR, *AAA Request*) al AS (que es identificado por el NAI). El mensaje de AR contiene la Respuesta de EAP / AKA / Puesta a Prueba (en el atributo específico del fabricante de 3GPP2) y el NAI (en el atributo de Nombre de Usuario) que se recibe en la Opción de Identificador de Cliente de AAA de la Solicitud de AAA.

En la etapa 2-H, el AS realiza lo siguiente tras la recepción del mensaje de AR en la etapa 2-G:

- Este compara el valor de AT_RES que el mismo ha calculado en la etapa D con el valor de AT_RES que está contenido en la Respuesta de EAP / AKA / Puesta a Prueba. Si los valores coinciden, la autenticación de AKA tiene éxito; de lo contrario, la autenticación falla.
- Si la autenticación tiene éxito, este envía un mensaje de AA, que contiene el NAI que identifica al usuario (en el atributo de Nombre de Usuario) al AC. Si la autenticación ha fallado, entonces este envía el mensaje de Rechazo de Acceso al AC.

En la etapa 2-I, el AC sabe, tras la recepción del mensaje de AA en la etapa 2-H, que la autenticación de AKA tuvo éxito. El AC envía un mensaje de Respuesta de AAA (que se indica mediante RP3 en la figura 2A) con el campo de Código ajustado para indicar ÉXITO (el valor 0), al terminal. Cuando el terminal recibe este mensaje, la autenticación de red de acceso de OWLAN se ha logrado. Si la autenticación tuvo éxito, el AC aplicará una regla de filtrado que permite que pasen los paquetes que se envían a partir del terminal autenticado.

A continuación, se describe cómo se realiza el establecimiento de autenticación generalizado para vinculaciones de movilidad de acuerdo con la primera realización.

1. La secuencia comienza con el terminal enviando un mensaje de solicitud (AAAv6, capa de enlace de WLAN o cualquier otro protocolo de acceso de red) al Agente Propio (HA, *Home Agent*). La solicitud contiene el NAI del usuario (IMSI@dominio) así como un mensaje de Respuesta de EAP / AKA / Identidad insertado.

2. El HA capta el mensaje de EAP y lo coloca en un mensaje de solicitud (que podría ser un mensaje de Solicitud

de AA de Diameter o un mensaje de Solicitud de Acceso de Radius) que se envía en la red medular al Servidor de Autenticación (AS, *Authentication Server*). Por ejemplo, en Diameter, el mensaje de EAP se encontraría en el AVP de cabida útil de EAP. El HA resuelve a qué AS debería ir la solicitud basándose en la parte de dominio del NAI de usuario, debido a que la parte de dominio del NAI indica el dominio en el que reside el AS.

3. Con la recepción del mensaje, el AS identifica en primer lugar el AuC que contiene la información de autenticación para el usuario. Esto podría estar basado en la parte de usuario del NAI de usuario. Por ejemplo, si el NAI de usuario que se usa es de la forma IMSI@dominio, entonces la IMSI se puede usar para identificar el HLR / AuC de usuario. Este solicita el quintete de autenticación de UMTS a partir del AuC. Este quintete consiste en cinco valores, en concreto, a) una puesta a prueba de red RAND, b) una respuesta esperada por el usuario XRES, c) una clave de cifrado CK, d) una clave de integridad IK y e) un testigo de autenticación de red AUTN. Con la obtención de estos valores, este crea los atributos AT_RAND (un número aleatorio), AT_AUTN (un vector de autorización) y AT_MAC (*message authentication code*, código de autenticación de mensaje). Este calcula y almacena los valores AT_RES y la clave de sesión K para su uso posterior. Este crea el mensaje de Solicitud de EAP / AKA / Puesta a Prueba que contiene el valor de AT_RAND, el valor de AT_AUTN y el valor de AT_MAC. Por último, este envía un mensaje, que contiene el mensaje de Solicitud de EAP / AKA / Puesta a Prueba en el mismo y el NAI que identifica al usuario (en el atributo de Nombre de Usuario), al HA. El mensaje podría ser un mensaje de Respuesta de AA de Diameter o un mensaje de Puesta a Prueba de Acceso de Radius. Si este es un mensaje de Diameter, el mensaje de EAP se porta en el AVP de cabida útil de EAP.

4. El HA envía un mensaje al terminal que contiene la Solicitud de EAP / AKA / Puesta a Prueba. Este puede ser un mensaje de AAAv6 o cualquier otro protocolo de acceso de red en uso entre el terminal y el controlador de acceso.

5. Cuando el terminal recibe este mensaje, este extrae en primer lugar el mensaje de Solicitud de EAP / AKA / Puesta a Prueba. Entonces, este usa el AKA para calcular los valores de AT_RES, dando los valores de AT_RAND y de AT_MAC que se reciben en el interior de la Solicitud de EAP / AKA / Puesta a Prueba como una entrada al AKA. Entonces, este calcula el valor K. Este también calcula el valor de AT_AUTN y lo compara con el AT_AUTN que se recibe en la Solicitud de EAP / AKA / Puesta a Prueba. Si estos valores coinciden, el mensaje de Solicitud de EAP / AKA / Puesta a Prueba se autentica con éxito, de lo contrario, el mensaje de autenticación falla. Si los valores han coincidido, este crea y envía un mensaje (AAAv6) al HA que contiene el mensaje de Respuesta de EAP / AKA / Puesta a Prueba. El mensaje de Respuesta de EAP / AKA / Puesta a Prueba contiene el valor de AT_RES calculado. El terminal almacena el valor K para usar este en el futuro para la Asociación de Seguridad (SA, *Security Association*) con el HA.

6. El HA envía de nuevo un mensaje de solicitud (Solicitud de AA de Diameter / Solicitud de Acceso de Radius). Esta vez, este contiene la Respuesta de EAP / AKA / Puesta a Prueba.

7. Cuando el AS recibe este mensaje, este compara el valor de AT_RES que el mismo había calculado anteriormente con el valor de AT_RES en el mensaje de EAP recibido. Si los valores coinciden, la autenticación de AKA tiene éxito; de lo contrario, la autenticación falla. Dependiendo del resultado, este envía o bien un mensaje de Aceptación de Acceso o bien uno de Rechazo de Acceso (en el caso de Radius). Para Diameter, este envía un mensaje de Respuesta de AA con el resultado en el AVP de Código de Resultado. Este también envía un AVP de Distribución de Claves debido a que es necesario que el mismo transporte la clave de autenticación de BU hasta el HA y el AVP de Tiempo de Vida de Autorización que tiene el tiempo de vida asociado de la clave de autenticación de BU.

8. Con la recepción de este mensaje, el HA sabe si la autenticación tuvo éxito o no. Este crea una Asociación de Seguridad con el terminal para el fin de autenticar las Actualizaciones de Vinculación. Este asocia la clave de autenticación K con esta SA e inicializa el tiempo de vida de la misma tal como se recibe en el mensaje. El HA envía el mensaje de respuesta apropiado al terminal. Cuando el terminal recibe este mensaje, el establecimiento de clave de autenticación de BU se ha completado.

En lo siguiente, el procedimiento anterior se describe con más detalle al hacer referencia al diagrama de flujo de señales que se muestra en las figuras 3A y 3B.

En la etapa 3-A, el terminal recibe de manera implícita un conocimiento de que su HA es capaz de realizar una autenticación de AKA. Antes de enviar el siguiente mensaje, el terminal ha de haber adquirido una dirección de IPv4 asignada, por ejemplo, con DHCP.

En la etapa 3-B, el terminal deduce a partir de su conocimiento estático con su red propia que es necesario realizar una autenticación de vinculación. El terminal comienza la secuencia de autenticación mediante el envío de un mensaje de Solicitud de AAA (que se indica mediante RQ1 en la figura 3A) al HA. La Solicitud de AAA contiene una Opción de Identificador de Cliente de AAA (cID) así como una opción que porta la Respuesta de EAP y el mensaje de Identidad de EAP (ERs / EAPIdentity). Tanto la Opción de Identificador de Cliente de AAA como el mensaje de Identidad de EAP contienen el NAI del usuario (IMSI@dominio).

En la etapa 3-C, el HA obtiene la dirección del AS a partir del NAI que está contenido en la Opción de Identificador de Cliente de AAA (usando un servidor dinámico de nombres (DNS, *dynamic name server*), si es necesario) y envía un mensaje de Solicitud de AAA (AR, *AAA Request*) al AS. La AR contiene el mensaje de Identidad de EAP (en el atributo de cabida útil de EAP) y el NAI (en el atributo de Nombre de Usuario) que se recibe en la Opción de Identificador de Cliente de AAA en la etapa B.

En la etapa 3-D, el AS realiza lo siguiente tras la recepción del mensaje de AR en la etapa 3-B:

- Este observa, a partir del campo de Razón de la Respuesta de EAP / Identidad que la clave de sesión que se establece con este procedimiento se usará para una autenticación Asistida por el Cliente (por lo tanto, este no tiene que enviar la clave más adelante a HA alguno que no sea el que actúa como la asistencia).

- Basándose en la parte de IMSI del NAI, el AS identifica el AuC que contiene la información de autenticación para el usuario.

- Este pregunta y obtiene un quintete de autenticación de UMTS a partir del AuC.

- Este calcula los valores AT_RAND (un número aleatorio) y AT_AUTN (un vector de autorización) y AT_MAC (*message authentication code*, código de autenticación de mensaje).

- Este calcula y almacena los valores AT_RES y K para su uso posterior.

- Este crea la Solicitud de EAP / AKA / Puesta a Prueba que contiene el valor de AT_RAND, el valor de AT_AUTN y el valor de AT_MAC.

- Este envía un mensaje de Puesta a Prueba de Acceso (AC, *Access Challenge*), que contiene la Solicitud de EAP / AKA / Puesta a Prueba (en el atributo específico del fabricante de 3GPP2) y el NAI que identifica al usuario (en el atributo de Nombre de Usuario), al HA.

En la etapa 3-E, el HA envía un mensaje de Respuesta de AAA (que se indica mediante RP2 en la figura), que contiene la Solicitud de EAP / AKA / Puesta a Prueba en la Opción de Datos Insertados de AAAv6, una Opción de Identificador de Cliente de AAA y una Opción de Puesta a Prueba de AAAv6, al terminal. La Opción de Identificador de Cliente de AAA contiene el NAI que identifica al usuario y la Opción de Puesta a Prueba de AAAv6 contiene un valor de Puesta a Prueba Local que es ajustado por el HA.

En la etapa 3-F, el terminal realiza lo siguiente tras la recepción de la Respuesta de AAA en la etapa 3-E:

- Este usa el AKA para calcular el valor de AT_RES y el valor de K, dando el valor de AT_RAND que se recibe en el interior de la Solicitud de EAP / AKA / Puesta a Prueba como una entrada al AKA.

- Este compara el valor de AT_AUTN calculado con el valor que se recibe en la Solicitud de EAP / AKA / Puesta a Prueba. Si los valores coinciden, el mensaje de Solicitud de EAP / AKA / Puesta a Prueba se autentica con éxito, de lo contrario, el mensaje de autenticación falla.

- Este almacena la clave K para el fin de usar la misma para la Asociación de Seguridad con el HA.

- Este almacena el tiempo de vida de la Asociación de Seguridad con el HA con el fin de ser capaz de deducir, cuándo se ha de renovar este.

- Este envía un mensaje de Solicitud de AAA (RQ3), que contiene la Puesta a Prueba Local en una Opción de Puesta a Prueba de AAAv6, una Opción de Identificador de Cliente de AAA (NAI de la forma IMSI@dominio) y un mensaje de Respuesta de EAP / AKA / Puesta a Prueba en la Opción de Datos Insertados de AAAv6, al HA. La Respuesta de EAP / AKA / Puesta a Prueba contiene el valor de SRES calculado.

En la etapa 3-G el HA envía un mensaje de AR al AS (que es identificado por el NAI). El mensaje de AR contiene la Respuesta de EAP / AKA / Puesta a Prueba (en el atributo específico del fabricante de 3GPP2) y el NAI (en el atributo de Nombre de Usuario) que se recibe en la Opción de Identificador de Cliente de AAA.

En la etapa 3-H, el AS realiza lo siguiente tras la recepción del mensaje de AR en la etapa 3-F:

- Este compara el valor de AT_RES que el mismo ha calculado en la etapa 3-C con el valor de AT_RES que está contenido en la Respuesta de EAP / AKA / Puesta a Prueba. Si los valores coinciden, la autenticación de AKA tiene éxito, de lo contrario, la autenticación falla.
- Este envía un mensaje de AA al HA. El mensaje de AA contiene la clave de autenticación de BU en un atributo específico del fabricante, el NAI que identifica al usuario en el atributo de Nombre de Usuario y el tiempo de vida

de clave de autenticación de BU en otro atributo específico del fabricante. El campo de tiempo de vida de clave es ajustado por el AS al valor 259200 (3 días), por ejemplo.

En la etapa 3-I: el HA crea o renueva la Asociación de Seguridad que se va a usar con el terminal para autenticar las Actualizaciones de Vinculación, asocia la clave K como la clave de autenticación con el mismo e inicializa el tiempo de vida para la SA de acuerdo con el valor que se recibe en el atributo de tiempo de vida de clave. Entonces, el HA envía un mensaje de Respuesta de AAA (RP3), que contiene una Opción de Respuesta de Clave Generalizada de AAA y el campo de Código ajustado para indicar ÉXITO (el valor 0), al terminal. La Opción de Respuesta de Clave Generalizada de AAA no contiene la clave K, sino que el campo de tiempo de vida se ajusta al valor que se recibe en el atributo de tiempo de vida de clave y el valor del campo de SPI de Clave está ajustado para indicar la Asociación de Seguridad entre el HA y el terminal. Cuando el terminal recibe este mensaje, el procedimiento de establecimiento de clave de autenticación de BU general se ha completado.

En la etapa 3-J, para la aplicación de IPv4 Móvil, el terminal formará la Extensión de Autenticación Propia - Móvil en la Solicitud de Registro (RREQ, *Registration Request*) de IPv4 Móvil, usando las BSA, tal como se crea a partir del material de claves. El HA aplicará, de forma automática, la BSA correspondiente a la Extensión de Autenticación de MN-HA cuando se realiza la autenticación de mensaje de la RREQ.

Para la aplicación de IPv6 Móvil, el terminal enviará unas actualizaciones de vinculación protegidas con IPSec al HA, de tal modo que las asociaciones de seguridad de IPSec manipuladas por R-UIM se aplicarán de forma automática al paquete enviado. Cuando el HA recibe el paquete, su módulo de IPSec conoce de forma automática la SA que el mismo puede aplicar a continuación al paquete de encabezamiento de movilidad entrante. Este paquete puede ser la HOTI de IPv6 Móvil o el mensaje de Actualización de Vinculación.

En la etapa 3-K, para la aplicación de IPv4 Móvil, el HA aplicará la Extensión de Autenticación Propia - Móvil en la Respuesta de Registro (RREP, *Registration Reply*) de IPv4 Móvil construida, usando las BSA, tal como se crea a partir del material de claves que se recibe a partir del AS. El terminal aplicará a continuación, de forma automática, la BSA correspondiente a la Extensión de Autenticación de MN-HA cuando se realiza la autenticación de mensaje de la RREP recibida.

Para la aplicación de IPv6 Móvil, el módulo de IPSec de HA protegerá de forma automática el mensaje de BAck enviado usando la o las SA manipuladas por R-UIM. Entonces, cuando se recibe un paquete de encabezamiento de movilidad asegurado por IPSec a partir del HA, el terminal aplica de forma automática la asociación de seguridad de IPSec manipulada por R-UIM para la dirección opuesta en comparación con la que se usa en la etapa N.

Esto completa un flujo de protocolo de aplicación de protección de señalización de movilidad con éxito. Con unas aplicaciones que no sean registros de base de IPv6 / IP Móvil, este tipo de procedimiento se puede usar para manipular cualquier SA de IPsec.

En lo siguiente, se describe una segunda realización de la presente invención.

Similar a la primera realización, la segunda realización se dirige al campo del uso combinado de redes de datos por paquetes celulares y no celulares de CDMA2000 y, en concreto, se refiere a la autenticación de usuario y la autorización de servicios usando un Módulo de Identidad de Usuario Extraíble (R-UIM, *Removable User Identity Module*) al comunicarse a través de múltiples tipos de redes de acceso. A pesar de que en la actualidad no existe protocolo alguno para realizar la autenticación de R-UIM a través de redes de IP no celulares, esta capacidad es útil para automatizar la gestión de claves aprovechando la infraestructura de claves existente para autenticaciones no de datos, tal como se ha mostrado con métodos similares en otros entornos celulares. La autenticación del usuario y la autorización del servicio permite que el operador celular proporcione al usuario diversos tipos de red de acceso, al tiempo que se mantiene una provisión de servicio unificada, una gestión de acceso de red basada en usuario y una autenticación de itinerancia, al tiempo que se aprovecha todo esto de la infraestructura de autenticación / contabilidad / facturación existente. El beneficio se puede resumir como una unificación de autenticación de CDMA2000 basada en tarjeta inteligente para múltiples métodos de acceso.

De acuerdo con la segunda realización, diversos protocolos se combinan para dar un mecanismo de distribución de claves y de autenticación de acceso múltiple basada en R-UIM, que se puede ejecutar a través de IP en diferentes capas de enlace. El sistema, que usa diversos mensajes de encapsulación en diferentes fases, permite que los elementos de red intercambien datos de tal modo que tanto el equipo de terminal como la red de operador pueden ejecutar el algoritmo de CAVE (*Cellular Authentication and Voice Encryption*, Autenticación Celular y Cifrado de Voz) de CDMA2000 para servicios de datos por paquetes no celulares y celulares basados en IP. Mediante el uso de los datos intercambiados y los resultados del algoritmo de CAVE, el terminal y la red de acceso se pueden autenticar mutuamente entre sí, y obtener claves seguras que se pueden usar para aplicaciones de un tiempo limitado, tal como autorización de acceso de red o protección de mensajes de autenticación de señalización de itinerancia. Se hace notar que el algoritmo de CAVE se describe adicionalmente en ANSI-TIA / EIA-41, "*Cellular Radio Telecommunications Intersystem Operations*", 1997, por ejemplo.
El terminal puede realizar unas sesiones autenticadas basadas en IP a través de tipos de red heterogéneos,

incluyendo CDMA2000, LAN Inalámbrica 802.11, Bluetooth o Ethernet. La red de acceso puede ser de punto a punto, o de punto a multipunto. El terminal puede combinar la ejecución de este método con IPv6 Móvil, o este puede ejecutar el mismo a través de un acceso de IPv6 simple, uno sin soporte de movilidad.

En los casos no celulares, de acuerdo con la presente segunda realización, se proporciona un método uniforme para que el equipo móvil y la red de operador se comuniquen entre sí a través de cualquier red capaz de IP, e intercambien de forma segura credenciales y establezcan una provisión de servicio, con independencia de las características de la red subyacente que se usa. El método, tal como se describe, está vinculado con el método de CDMA2000 existente mediante la compartición de solo la identidad de registro, de tal modo que usando este método, no se requiere que los operadores reorganicen cada tecnología, sino que pueden aprovechar este método más genérico cuando no se usa un mecanismo específico de capa de enlace. Mediante la adición de unos pocos elementos de red, tal como se describe en la presente invención, el operador puede aprovechar su infraestructura de servicio de CDMA2000 existente con poco o ningún cambio en los elementos de red existentes.

En lo siguiente, se describe con más detalle el procedimiento de acuerdo con la segunda realización.

La realización se dirige a teléfonos móviles u otros dispositivos móviles (a los que se hace referencia en lo que antecede en el presente documento como ME o equipo móvil), que tienen capacidades de comunicación basadas en IP, por lo general a través de enlaces inalámbricos, y que tiene el módulo R-UIM. La realización también se puede usar con dispositivos fijos en su arranque pero es de lo más útil con dispositivos móviles. La realización permite una autenticación mutua, una autorización de red y una provisión de servicio mediante una interacción entre múltiples partes que implican (pero sin limitarse a) las siguientes entidades: ME, R-UIM (que se considera una entidad separada en virtud de su procesador interno, memoria no volátil, y algoritmos y datos privados), Controlador de Acceso, Pasarela de Autenticación, y el Centro de Autenticación (AuC, *Authentication Center* / HLR (*Home Location Register*, Registro de Posiciones Propio)) de la red de CDMA2000, similar a como es en la primera realización.

En el momento en el que el ME entra en una red capaz de una funcionalidad de GRASP (*General R-UIM Authentication and Service Provisioning*, Autenticación de R-UIM General y Provisión de Servicio, el ejemplo de protocolo que se describe en la presente segunda realización), el ME recibe un Anuncio de Encaminador, que incluye una indicación de soporte de GRASP, por ejemplo, una opción de anuncio de encaminador o de agente a partir del AC local que indica este tipo de soporte de AAA. Esto inicia la autenticación, la generación de claves y la provisión de servicio tal como se describe en la presente invención. A continuación, el ME responde al AC con el mensaje de EAP / R-UIM / Inicio que contiene una opción de Identificador de Cliente y un mensaje de Identidad de EAP. Ambas opciones contienen la identidad de usuario (IMSI@dominio), que se construye a partir de la IMSI del usuario en el R-UIM, en el tiempo de arranque de ME y el dominio en un archivo adicional en el R-UIM o en la memoria no volátil del ME. Este mensaje de EAP de identidad está encapsulado en IP / IPv6 como un mensaje de AAA de enlace de acceso. El mensaje de AAA de enlace de acceso se puede encontrar, por ejemplo, en mensajes de UDP o de ICMPv6, tal como se describe en un caso de mejor implementación en el Apéndice A para IPv4 e IPv6, respectivamente, en una encapsulación de capa de enlace, tal como en IEEE 802.1x, IEEE 802.11i o en un mensaje de perfil de Bluetooth adecuado, en encapsulación de EAP de PPP, o en cualquier mensaje de protocolo de PANA de último salto adecuado, según se normalice en el futuro).

El AC determina la dirección de IP del Servidor de Autenticación mediante la asignación del mismo a partir de la IMSI y el dominio, y reenvía el mensaje de AAA al núcleo de IP usando, por ejemplo, RADIUS, o cualquier otro protocolo de AAA medular tal como DIAMETER, para su transporte de encapsulación. Entonces, el mensaje es recibido por el AS que, entonces, entra en contacto con el AuC / HLR.

El AS puede ser un servidor de AAA que se comunica directamente o por medio del MSC de servicio con el AuC / HLR que usa mensajería de SS7 o de A1 que emula autenticaciones de circuito de voz. Dicho de otra forma, el AS tendría una funcionalidad para comunicarse con el AuC / HLR. Con esta elección de arquitectura, la red de CDMA existente puede permanecer sin modificaciones, solo se ha de añadir un AS. Este es el enfoque de superposición no intrusiva.

Como alternativa, un enfoque con una integración más compacta daría lugar a cambios en la red de CDMA2000. El AS puede ser un cliente / intermediario de AAA (RADIUS) en la PDSN, que reenvía las autenticaciones a un servidor de AAA Propio (AAAH, *Home AAA*) modificado respecto del convencional en la red medular por paquetes de CDMA2000. Esto último requiere que el AAAH tenga la funcionalidad de comunicarse con el AuC / HLR, una modificación al núcleo de paquetes de CDMA2000. La última elección de arquitectura daría la posibilidad de usar autenticaciones de R-UIM para las sesiones de datos por paquetes de CDMA2000 nativas por medio de una PDSN, tal como se realiza en la actualidad con EAP-CHAP, o EAP-PAP, debido a que esas autenticaciones terminan al final de la sesión de PPP en la PDSN, y dan lugar a un intercambio de mensajes de RADIUS con el servidor de AAAH. Dicho de otra forma, esta última alternativa haría de intermediario en las autenticaciones de R-UIM no celulares por medio de la PDSN o directamente con el servidor de AAA propio, o transferiría autenticaciones de PPP-R-UIM celulares al mismo punto de extremo, usando capacidades de cliente de RADIUS de PDSN ampliadas. La extensión sería la capacidad de EAP-R-UIM y su asignación a mensajes de RADIUS, volviendo a usar en potencia la mensajería de RADIUS no celular para el método que se describe.

Cuando el AS recibe un registro, este procede a recuperar un material de manipulación aleatorizado a partir del AuC, en la forma de un RAND o RANDU (dependiendo de la naturaleza global o única de la autenticación que se está realizando), y devuelve esta información aleatoria como una puesta a prueba al ME, en la forma de un mensaje de EAP / R-UIM / Puesta a Prueba que contiene una opción de ID de cliente, en el interior de una Respuesta de AAA (que se transporta a través de RADIUS).

Ahora, el ME ha recibido la puesta a prueba aleatoria (RAND) a partir del AS, y está listo para ejecutar el algoritmo de CAVE con el fin de autenticarse a sí mismo y generar claves de cifrado para la sesión. El ME envía una instrucción al R-UIM para comenzar el algoritmo de CAVE de Ejecución, y proporciona el ESN (*electronic serial number*, número de serie electrónico del teléfono, determinado y tiempo de arranque de ME), RAND / RANDU, tipo de rand (único o global, dependiendo de qué se suministró), y el número PIN, si es necesario, para este R-UIM. Entonces, el ME ejecuta Obtener Respuesta, para conseguir que el R-UIM pase la AUTHR o AUTHU (respuesta de la puesta a prueba global o única) de salida al ME.

Después de que el ME haya recibido la respuesta de la puesta a prueba, este envía la misma al AC en un paquete similar tal como se ha descrito en lo que antecede, pero este es un mensaje de EAP / R-UIM / Inicio con la Puesta a Prueba Local, ID de Cliente, y una opción de datos insertados que contiene el material de respuesta de la puesta a prueba. Entonces, el AC consulta la dirección del AS al igual que en la etapa previa, y reenvía el mensaje por medio de RADIUS. El AS obtiene el mensaje, y determina con qué AuC / HLR ponerse en contacto mediante la realización de una consulta de asignación basándose en la IMSI y el Dominio que se reciben en la opción secundaria de identidad, y también recupera su estado de sesión almacenado basándose en la IMSI@dominio. El AS procede a verificar la autenticidad del cliente mediante la recuperación de credenciales de CAVE a partir del AuC / HLR, la ejecución del algoritmo de CAVE y la comparación de la respuesta que se recibe a partir del ME con la respuesta que se recibe a partir del AuC / HLR.

Si las respuestas que se reciben a partir del ME y el AuC son iguales, el AS reenvía la clave de sesión y el código de éxito de vuelta al AC en otro mensaje de EAP. Tras la recepción de este mensaje de EAP, el AC concede acceso al ME y guarda la clave de sesión para su uso durante la sesión. Esto ocurre, por ejemplo, mediante la funcionalidad de cliente de AAA medular en el AC. Este manipula una asociación o asociaciones de seguridad de IPSec con ME en el AC, o crea una regla de cortafuegos para conceder acceso a la red para el ME.

Entonces, el AC transmite el mensaje de vuelta al ME, que está insertado en el protocolo de AAA de último salto tal como se ha descrito previamente (por ejemplo, en ICMPv6), con la opción secundaria de clave eliminada. Por lo tanto, la clave no se transmite a través del último salto, lo que puede ser poco seguro, y el ME usa la clave que este obtuvo en el R-UIM, y el AC usa la clave que se transmite de vuelta a partir del AS a través de RADIUS.

A continuación, el procedimiento anterior se describe con más detalle al hacer referencia al diagrama de flujo de señales que se muestra en las figuras 4A y 4B. Se hace notar que este flujo de señales es similar al que se muestra en las figuras 2A y 2B, de tal modo que no se explican de nuevo abreviaturas y similares que se describen en conexión con las figuras 2A y 2B.

En la etapa 4-A, el terminal recibe un Anuncio de Encaminador (o bien no solicitado o bien solicitado) a partir del AC. El Anuncio de Encaminador (RA, *Router Advertisement*) incluye un indicador que indica un soporte de AAA. Antes de enviar el siguiente mensaje, el terminal ha de haber adquirido una dirección de IPv4 asignada, por ejemplo, con DHCP.

En la etapa 4-B, el terminal deduce a partir de la presencia de un indicador de AAA en el Anuncio de Encaminador que es necesario realizar una autenticación de acceso de AAA. El terminal comienza la secuencia de autenticación mediante el envío de un mensaje de Solicitud de AAA (RQ1) al AC. La Solicitud de AAA contiene una Opción de Identificador de Cliente de AAA así como una opción que porta el mensaje de Identidad de EAP. Tanto la Opción de Identificador de Cliente de AAA como el mensaje de Identidad de EAP contienen el NAI del usuario (IMSI@dominio).

En la etapa 4-C, el AC obtiene la dirección del AS a partir del NAI que está contenido en la Opción de Identificador de Cliente de AAA (usando un DNS, si es necesario) y envía un mensaje de Solicitud de AAA (AR, *AAA Request*) al AS. La AR contiene el mensaje de Identidad de EAP (en el atributo de cabida útil de EAP) y el NAI (en el atributo de Nombre de Usuario) que se recibe en la Opción de Identificador de Cliente de AAA en la etapa B.

En la etapa 4-D, el AS realiza lo siguiente tras la recepción del mensaje de AR en la etapa 4-C:

- Este crea un mensaje de Solicitud de EAP / R-UIM / Solicitud de Inicio que indica el inicio del procedimiento de autenticación de R-UIM.
- Este envía un mensaje de Respuesta de AAA (AA, *AAA Answer*), que contiene la Solicitud de EAP / R-UIM / Inicio (en el atributo de cabida útil de EAP) y el NAI que identifica al usuario (en el atributo de Nombre de Usuario), al AC.

En la etapa 4-E, el AC envía un mensaje de Respuesta de AAA (RP1), que contiene la Solicitud de EAP / R-

UIM / Inicio en la una Opción de Datos Insertados y una Opción de Identificador de Cliente de AAA al terminal. La Opción de Identificador de Cliente de AAA contiene el NAI que identifica al usuario.

En la etapa 4-F, el terminal envía un mensaje de Solicitud de AAA (RQ1), que contiene una Opción de Identificador de Cliente de AAA que contiene el NAI (IMSI@dominio) y una Opción de Datos Insertados de AAA que porta un mensaje de Respuesta de EAP / R-UIM / Inicio. El campo de Razón de la Respuesta de EAP / R-UIM / Inicio se ajusta a 0 (cero), que indica que no se usará la clave de sesión para cosa alguna (solo se realiza la autenticación de CAVE).

En la etapa 4-G, el AC obtiene la dirección del AS a partir del NAI que está contenido en la Opción de Identificador de Cliente de AAA (usando un DNS, si es necesario) y envía un mensaje de Solicitud de AAA (AR, *AAA Request*) al AS. La AR contiene el mensaje de Respuesta de EAP / R-UIM / Inicio y el NAI (en los campos de atributo de Radius específicos del fabricante), tal como se recibe en la Opción de Identificador de Cliente de AAA en la etapa 4-F.

En la etapa 4-H, el AS realiza lo siguiente tras la recepción del mensaje de AR en la etapa G:

- Basándose en la parte de IMSI del NAI, el AS identifica el AuC que contiene la información de autenticación para el usuario.
- Este pregunta y obtiene dos tripletes de autenticación de Cave a partir del AuC.
- Este calcula los valores MAC_RAND y MAC_AUTHR como el AT_RAND y el AT_MAC, que se especifican en H. Haverinen "*EAP SIM Authentication (work in progress)*" Borrador de Internet (draft-haverinen-pppext-eap-sim-10.txt), Grupo de Tareas Especiales de Ingeniería en Internet, febrero de 2003, por ejemplo, para este EAP-R-UIM.
- Este almacena el valor MAC_AUTHR para su uso posterior.
- Este crea el mensaje de Solicitud de EAP / R-UIM / Puesta a Prueba que contiene el valor de MAC_RAND y dos valores de RAND (que se obtienen a partir de los tripletes de autenticación).
- Este envía un mensaje de Respuesta de AAA (AA, *AAA Answer*), que contiene la Solicitud de EAP / R-UIM / Puesta a Prueba y el NAI que identifica al usuario (en los campos de atributo de Radius específicos del fabricante), al AC.

En la etapa 4-I, el AC envía un mensaje de Respuesta de AAA (RP2), que contiene la Solicitud de EAP / R-UIM / Puesta a Prueba en la Opción de Datos Insertados de AAA, una Opción de Identificador de Cliente de AAA que contiene el NAI.

En la etapa 4-J, el terminal realiza lo siguiente tras la recepción de la Respuesta de AAA en la etapa 4-I:

- Este usa el R-UIM para calcular dos valores de AUTHR / AUTHU, dando los dos valores de RAND que se reciben en el interior de la Solicitud de EAP / R-UIM / Puesta a Prueba como una entrada al módulo R-UIM.
- Este calcula los valores MAC_RAND y MAC_AUTHR como el AT_RAND y el AT_MAC que se especifican en el documento al que se ha hecho referencia en lo que antecede de H. Haverinen "*EAP SIM Authentication (work in progress)*" Borrador de Internet (draft-haverinen-pppexteap-sim-10.txt), Grupo de Tareas Especiales de Ingeniería en Internet, febrero de 2003, por ejemplo.
- Este compara el valor de MAC_RAND calculado con el valor que se recibe en la Solicitud de EAP / R-UIM / Puesta a Prueba. Si los valores coinciden, el mensaje de Solicitud de EAP / R-UIM / Puesta a Prueba se autentica con éxito, de lo contrario, el mensaje de autenticación falla.
- Este envía un mensaje de Solicitud de AAA (RQ3) que contiene una Opción de Identificador de Cliente de AAA (NAI de la forma IMSI@dominio) y un mensaje de Respuesta de EAP / R-UIM / Puesta a Prueba en la Opción de Datos Insertados de AAA, al AC. La Respuesta de EAP / R-UIM / Puesta a Prueba contiene el valor de MAC_AUTHR calculado.

En la etapa 4-K, el AC envía un mensaje de AR al AS (que es identificado por el NAI). El mensaje de AR contiene la Respuesta de EAP / R-UIM / Puesta a Prueba y el NAI (en un campo de atributo de Radius específico del fabricante) tal como se recibe en la Opción de Identificador de Cliente de AAA de la Solicitud de AAA.

En la etapa 4-L, el AS realiza lo siguiente tras la recepción del mensaje de AR en la etapa K:

- Este compara el valor de MAC_AUTHR que el mismo ha calculado en la etapa 4-D con el valor de MAC_AUTHR que está contenido en la Respuesta de EAP / R-UIM / Puesta a Prueba. Si los valores coinciden, la autenticación de CAVE tiene éxito; de lo contrario, la autenticación falla.

- Este envía un mensaje de AA, que contiene el NAI que identifica al usuario (en un campo de atributo de Radius), al AC y el Código de Resultado que indica el éxito (Atributo de Mensaje de Respuesta en AA) o el fallo (Atributo de Mensaje de Respuesta en un mensaje de Rechazo de Acceso) de la autenticación, al AC.

En la etapa 4-M, el AC sabe, tras la recepción del mensaje de AA en la etapa 4-L, si la autenticación de CAVE tuvo éxito o no. Si la autenticación tuvo éxito, el AC envía un mensaje de Respuesta de AAA con el campo de Código

ajustado para indicar ÉXITO (el valor 0), al terminal. Cuando el terminal recibe este mensaje, la autenticación de red de acceso de OWLAN se ha logrado.

Si la autenticación tuvo éxito, el AC aplicará una regla de filtrado que permite que pasen los paquetes que se envían a partir del terminal autenticado. Como alternativa, puede haber una entrada, o un par de entradas, de IPsec de acceso de red que se crea entre el terminal y el AC con esta aplicación (u otro código de aplicación), usando el mismo tipo de un mecanismo de manipulación tal como se explica para la aplicación de IPv6 / IP Móvil en lo sucesivo.

En un segundo caso de acuerdo con la segunda realización, se describe un flujo de señalización entre el MS, el HA y el AS, que usa señalización de enlace de acceso (NAAP, PPP-LCP o similar) y señalización de enlace medular (Radius o DIAMETER) y EAP-R-UIM como la señalización de extremo a extremo. La señalización combinada se muestra en las figuras 5A y 5B.

En la etapa 5-A, el terminal recibe de manera implícita un conocimiento de que su HA es capaz de realizar una autenticación de R-UIM. Antes de enviar el siguiente mensaje, el terminal ha de haber adquirido una dirección de IPv4 asignada, por ejemplo, con DHCP.

En la etapa 5-B, el terminal deduce a partir de su conocimiento estático con su red propia que es necesario realizar una autenticación de vinculación. El terminal comienza la secuencia de autenticación mediante el envío de un mensaje de Solicitud de AAA (RQ1) al HA. La Solicitud de AAA contiene una Opción de Identificador de Cliente de AAA así como una opción que porta el mensaje de Identidad de EAP. Tanto la Opción de Identificador de Cliente de AAA como el mensaje de Identidad de EAP contienen el NAI del usuario (IMSI@dominio).

En la etapa 5-C, el HA obtiene la dirección del AS a partir del NAI que está contenido en la Opción de Identificador de Cliente de AAA (usando un DNS, si es necesario) y envía un mensaje de Solicitud de AAA (AR, *AAA Request*) al AS. La AR contiene el mensaje de Identidad de EAP (en el atributo de cabida útil de EAP) y el NAI (en el atributo de Nombre de Usuario) que se recibe en la Opción de Identificador de Cliente de AAA en la etapa 5-B.

En la etapa 5-D, el AS realiza lo siguiente tras la recepción del mensaje de AR en la etapa C:

- Este crea un mensaje de Solicitud de EAP / R-UIM / Solicitud de Inicio que indica el inicio del procedimiento de autenticación de R-UIM. Con el fin de realizar esto, el AS también entra en contacto con el AuC (*Authentication Center*, Centro de Autenticación).

- Este envía un mensaje de Respuesta de AAA (AA, *AAA Answer*), que contiene la Solicitud de EAP / R-UIM / Inicio (en el atributo de cabida útil de EAP) y el NAI que identifica al usuario (en el atributo de Nombre de Usuario), al HA.

En la etapa 5-E, el HA envía un mensaje de Respuesta de AAA (RP1), que contiene la Solicitud de EAP / R-UIM / Solicitud de Inicio en la Opción de Datos Insertados y una Opción de Identificador de Cliente de AAA al terminal. La Opción de Identificador de Cliente de AAA contiene el NAI que identifica al usuario.

En la etapa 5-F, el terminal envía un mensaje de Solicitud de AAA (RQ2), que contiene una Opción de Identificador de Cliente de AAA que contiene el NAI (IMSI@dominio) y una Opción de Datos Insertados de AAA que porta un mensaje de Respuesta de EAP / R-UIM / Inicio. El campo de Razón de la Respuesta de EAP / R-UIM / Inicio se ajusta a 2 (10 en binario), que indica que la clave de sesión se usará para la protección de registro propio (la autenticación de CAVE se realizará después de la etapa I y se crean unas asociaciones de seguridad de IPSec para proteger los encabezamientos de movilidad con HA después de la etapa M).

En la etapa 5-G, el HA obtiene la dirección del AS a partir del NAI que está contenido en la Opción de Identificador de Cliente de AAA (usando un DNS, si es necesario) y envía un mensaje de Solicitud de AAA (AR, *AAA Request*) al AS. La AR contiene el mensaje de Respuesta de EAP / R-UIM / Inicio y el NAI (en los campos de atributo de Radius específicos del fabricante), tal como se recibe en la Opción de Identificador de Cliente de AAA en la etapa F.

En la etapa 5-H, el AS realiza lo siguiente tras la recepción del mensaje de AR en la etapa G:

- Basándose en la parte de IMSI del NAI, el AS identifica el AuC que contiene la información de autenticación para el usuario.
- Este pregunta y obtiene tantos tripletes de autenticación de Cave a partir del AuC como sea necesario. Esto se determina por medio de la longitud de clave del algoritmo de CAVE y la Id de Perfil de Cifrado de IPSec que se usa (una a partir del conjunto tal como se define en IKE (*Internet Key Exchange*, Intercambio de Claves de Internet) v2). Esta Id de perfil se comunica en el paquete de EAP.
- Este calcula los valores MAC_RAND y MAC_AUTHR como el AT_RAND y el AT_MAC, que se especifican en el documento al que se ha hecho referencia en lo que antecede de H. Haverinen "*EAP SIM Authentication (work in progress)*" Borrador de Internet (draft-haverinen-pppexteap-sim-10.txt), Grupo de Tareas Especiales de

Ingeniería en Internet, febrero de 2003, por ejemplo, para este EAP-R-UIM.

- Este almacena el valor MAC_AUTHR para su uso posterior.
- Este crea el mensaje de Solicitud de EAP / R-UIM / Puesta a Prueba que contiene el valor de MAC_RAND y dos valores de RAND (que se obtienen a partir de los tripletes de autenticación).
- Este envía un mensaje de Respuesta de AAA (AA, *AAA Answer*), que contiene la Solicitud de EAP / R-UIM / Puesta a Prueba y el NAI que identifica al usuario (en los campos de atributo de Radius específicos del fabricante), al HA.

En la etapa 5-I, el HA envía un mensaje de Respuesta de AAA (RP2), que contiene la Solicitud de EAP / R-UIM / Puesta a Prueba en la Opción de Datos Insertados de AAA, una Opción de Identificador de Cliente de AAA que contiene el NAI.

En la etapa 5-J, el terminal realiza lo siguiente tras la recepción de la Respuesta de AAA en la etapa 5-1:

- Este usa el R-UIM para calcular dos valores de AUTHR / AUTHU, dando los dos valores de RAND que se reciben en el interior de la Solicitud de EAP / R-UIM / Puesta a Prueba como una entrada al algoritmo de Run_CAVE en el módulo R-UIM.
- Este calcula los valores MAC_RAND y MAC_AUTHR como el AT_RAND y el AT_MAC, que se especifican en el documento al que se ha hecho referencia en lo que antecede de H. Haverinen "*EAP SIM Authentication (work in progress)*" Borrador de Internet (draft-haverinen-pppexteap-sim-10.txt), Grupo de Tareas Especiales de Ingeniería en Internet, febrero de 2003, por ejemplo.
- Este compara el valor de MAC_RAND calculado con el valor que se recibe en la Solicitud de EAP / R-UIM / Puesta a Prueba. Si los valores coinciden, el mensaje de Solicitud de EAP / R-UIM / Puesta a Prueba se autentica con éxito, de lo contrario, el mensaje de autenticación falla.
- Este envía un mensaje de Solicitud de AAA (RQ3), que contiene una Opción de Identificador de Cliente de AAA (NAI de la forma IMSI@dominio) y un mensaje de Respuesta de EAP / R-UIM / Puesta a Prueba en la Opción de Datos Insertados de AAA, al HA. La Respuesta de EAP / R-UIM / Puesta a Prueba contiene el valor de MAC_AUTHR calculado.

En la etapa 5-K, el HA envía un mensaje de AR al AS (que es identificado por el NAI). El mensaje de AR contiene la Respuesta de EAP / R-UIM / Puesta a Prueba y el NAI (en un campo de atributo de Radius específico del fabricante) tal como se recibe en la Opción de Identificador de Cliente de AAA de la Solicitud de AAA.

En la etapa 5-L, el AS realiza lo siguiente tras la recepción del mensaje de AR en la etapa K:

- Este compara el valor de MAC_AUTHR que el mismo ha calculado en la etapa 5-D con el valor de MAC_AUTHR que está contenido en la Respuesta de EAP / R-UIM / Puesta a Prueba. Si los valores coinciden, entonces la autenticación de CAVE tiene éxito; de lo contrario, la autenticación falla.
- Este envía un mensaje de AA, que contiene el NAI que identifica al usuario (en un campo de atributo de Radius) al HA y el Código de Resultado que indica el éxito (Atributo de Mensaje de Respuesta en AA) o el fallo (Atributo de Mensaje de Respuesta en AA) de la autenticación, y una respuesta de clave (Id de Perfil de Cifrado, clave o claves, tiempo de vida) al HA.

En la etapa 5-M, el HA sabe tras la recepción del mensaje de AA en la etapa 5-L, si la autenticación de CAVE tuvo éxito o no. Si la autenticación tuvo éxito, el HA envía un mensaje de Respuesta de AAA (RP3) con el campo de Código ajustado para indicar ÉXITO (el valor 0) al terminal. Cuando el terminal recibe este mensaje, se realiza la manipulación y la autorización de registro propio de OWLAN. Si la autenticación de R-UIM tuvo éxito, el HA manipulará

- para la aplicación de IPv4 Móvil, una Asociación de Seguridad de Vinculación (BSA, *Binding Security Association*) que se va a usar con la Extensión de Autenticación de MN-HA para el estado de IPv4 Móvil apropiado a partir del material de claves que se obtiene cuando se ejecuta el algoritmo de Run_CAVE en el R-UIM.
- para la aplicación de IPv6 Móvil, dos asociaciones de seguridad de IPSec con la SADB a partir del material de claves que se obtiene cuando se ejecuta el algoritmo de Run_CAVE en el R-UIM. Estas SA (*Security Associations*, Asociaciones de Seguridad) son set up para paquetes de encabezamiento de movilidad (MIPv6) o de registro (MIPv4) entrantes y salientes con el terminal, y con los otros parámetros según son identificados por la Id de Perfil de Cifrado de IPSec usada. Posiblemente, esta acción usa la interfaz de Pfkey del módulo de IPSec, no requiriendo por lo tanto interfaz especial alguna entre el demonio de manipulación de R-UIM y el módulo de IPSec.

En la etapa 5-N, para la aplicación de IPv4 Móvil, el terminal formará la Extensión de Autenticación Propia - Móvil en la Solicitud de Registro (RREQ, *Registration Request*) de IPv4 Móvil, usando las BSA, tal como se crea a partir del material de claves. El HA aplicará, de forma automática, la BSA correspondiente a la Extensión de Autenticación de MN-HA cuando se realiza la autenticación de mensaje de la RREQ.
Además, en la etapa 5-N, para la aplicación de IPv6 Móvil, el terminal enviará unas actualizaciones de vinculación

protegidas con IPSec al HA, de tal modo que las asociaciones de seguridad de IPSec manipuladas por R-UIM se aplicarán de forma automática al paquete enviado. Cuando el HA recibe el paquete, su módulo de IPSec conoce de forma automática la SA que el mismo puede aplicar a continuación al paquete de encabezamiento de movilidad entrante. Este paquete puede ser la HOTI de IPv6 Móvil (*Home Test Init*, Inicialización de Prueba Propia) o el mensaje de Actualización de Vinculación (BU, *Binding Update*).

En la etapa 5-O, para la aplicación de IPv4 Móvil, el HA aplicará la Extensión de Autenticación Propia - Móvil en la Respuesta de Registro (RREP, *Registration Reply*) de IPv4 Móvil construida, usando las BSA, tal como se crea a partir del material de claves que se recibe a partir del AS. El terminal aplicará a continuación, de forma automática, la BSA correspondiente a la Extensión de Autenticación de MN-HA cuando se realiza la autenticación de mensaje de la RREP recibida.

Además, para la aplicación de IPv6 Móvil, el módulo de IPSec de HA, en la etapa 5-O, protegerá de forma automática el mensaje de BAck (*Binding Acknowledgement*, Acuse de Recibo de Vinculación) enviado usando la o las SA manipuladas por R-UIM. Entonces, cuando se recibe un paquete de encabezamiento de movilidad asegurado por IPSec a partir del HA, el terminal aplica de forma automática la asociación de seguridad de IPSec manipulada por R-UIM para la dirección opuesta en comparación con la que se usa en la etapa N.

Esto completa un flujo de protocolo de aplicación de protección de señalización de movilidad con éxito. Con unas aplicaciones que no sean registros de base de IPv6 / IP Móvil, este tipo de procedimiento se puede usar para manipular cualquier SA de IPsec.

La invención tal como se describe en las realizaciones anteriores, se puede implementar en un soporte lógico o sistema de soporte físico insertado o elementos de microplaca, que se ejecutan en diversas entidades de red que están implicadas en el intercambio. Algunas funcionalidades importantes de la implementación en un terminal son: acceso a una API para las funciones de R-UIM convencional, y la capacidad de construir paquetes de IP arbitrarios que incluyen direcciones encapsuladas. En el controlador de Acceso, algunas funciones importantes son la encapsulación y la desencapsulación de paquetes en mensajes de AAA de acceso, tales como mensajes de UDP o de ICMPv6 y de AAA medular, tales como mensajes de RADIUS o de DIAMETER, por ejemplo, adaptando a partir de la aplicación de NASREQ (tal como se describe en P. Calhoun, W. Bulley, A. Rubens, J. Haag, G. Zorn. *Diameter NASREQ Application (work en progress)*. Borrador de Internet (draft-ietf-aaa-diameter-nasreq-08.txt), Grupo de Tareas Especiales de Ingeniería en Internet, noviembre de 2001, por ejemplo). Asimismo, este reutilizaría las capacidades de filtrado de paquetes genéricas de un encaminador de acceso, Servidor de Acceso de Red o PDSN, dependiendo de en dónde está ubicado el punto de servicio de autenticación de acceso para el método.

El mejor modo de implementación de la segunda realización se bosqueja en la figura 1. Este sería implementar la funcionalidad del terminal en un dispositivo móvil, que interconecta con el soporte físico de R-UIM (en el caso de la segunda realización) así como con la red. La funcionalidad enviaría y recibiría mensajes de protocolo de GRASP con el encaminador de acceso de IP, servidor de acceso o estación de base con la que se conecta el dispositivo móvil a través de la red de radio. Cuando el dispositivo móvil ha recibido mensajes a partir de los elementos de red que suministran información de entrada (una puesta a prueba, o RAND) al algoritmo de autenticación, este accederá al R-UIM para ejecutar el algoritmo de CAVE. Esto genera, a nivel local, una respuesta y un secreto compartido con la red.

En la red, la invención se puede implementar mediante un soporte lógico adicional en el encaminador de acceso / estación de base de WLAN, para aceptar mensajes encapsulados a partir del equipo móvil, y los vuelve a encapsular en el protocolo de RADIUS basado en servidor, para el tránsito de vuelta a la red del operador. Un Agente Propio de IP Móvil opcional con un soporte lógico adicional se añade a la red del operador, y adicionalmente se usa una pasarela (AS o AAAH) para traducir mensajes entre RADIUS y los mensajes de SS7 de CDMA2000. De esta forma, la seguridad del protocolo de CAVE está limitada a los límites del ME y el AuC / HLR, y la infraestructura existente en la red de CDMA2000 se reutiliza para la autenticación y la autorización, posiblemente incluso para facturación y contabilidad. Por lo tanto, en las redes de IP o de CDMA2000 no se necesitan cambios, o se necesitan unos cambios mínimos.

La implementación funcional puede tener lugar en diversos lugares de los sistemas operativos, por ejemplo en los núcleos de OS (*Operating System*, Sistema Operativo), o en un soporte lógico de nivel de usuario, dependiendo de los detalles específicos de la implementación.

En lo siguiente, los elementos de red que están implicados se describen de forma concisa al hacer referencia a las figuras 6A a 6C. Se hace notar que solo se describen aquellos miembros que son necesarios para la descripción de las realizaciones anteriores, la figura 6A muestra un controlador de acceso (AC, *access controller*) de acuerdo con las realizaciones anteriores. El controlador de acceso 1 comprende unos medios de recepción 1a, que reciben un mensaje de autenticación en el que está encapsulado un mensaje de inicio que se ha descrito en lo que antecede. Además, el controlador de acceso comprende unos medios de procesamiento 1b. Los medios de procesamiento 1b leen el mensaje de inicio encapsulado (por ejemplo, un mensaje de opción de identificador de cliente y un mensaje de opción de identidad de EAP (*Extensible Authentication Protocol*, Protocolo de Autenticación Extensible), que

contienen tipo de cliente, identidad de usuario e información de dirección medular, tal como se ha descrito en lo que antecede). Entonces, el mensaje encapsulado es reenviado por unos medios de reenvío 1c a un servidor de autenticación que se identifica en el mensaje encapsulado.

La figura 6B muestra un terminal móvil 2. Se hace notar que el terminal móvil es solo un ejemplo para un dispositivo de abonado. El terminal móvil 2 comprende unos medios de determinación 2a que determinan un tipo de acceso de red tras la recepción de un mensaje de información (es decir, un anuncio de encaminador RA que se ha descrito en lo que antecede) que indica al menos un tipo de acceso de red. Además, el terminal móvil 3 comprende unos medios de creación 2b que crean el mensaje de inicio tal como se ha descrito en lo que antecede. Unos medios de encapsulación 2c de la estación móvil 2 encapsulan el mensaje de inicio en un mensaje de autenticación compatible con una red de acceso que se identifica en el mensaje de información, y unos medios de envío 2d de la estación móvil 2 envían el mensaje de inicio a un controlador de acceso.

La figura 6c muestra un encaminador 3 tal como se usa en las realizaciones anteriores. El encaminador 3 comprende unos medios de creación 3a que crean el mensaje de información que se ha descrito en lo que antecede, es decir, un Anuncio de Encaminador. Unos medios de envío 3b del encaminador 3 envían el mensaje de información a un dispositivo de abonado. Se hace notar que el encaminador 3 y el controlador de acceso 1 se pueden disponer en una unidad (como de acuerdo con las realizaciones que se han descrito en lo que antecede).

La invención no se limita a las realizaciones que se han descrito en lo que antecede sino que puede variar dentro del alcance de las reivindicaciones.

Por ejemplo, las realizaciones anteriores se pueden combinar con libertad, de tal modo que se usan tanto el mecanismo de autenticación de EAP-AKA que usa un USIM y una autenticación que usa R-UIM basándose en el algoritmo de CAVE.

Un protocolo entre el dispositivo móvil y la red de acceso puede comprender al menos uno de protocolos de capa de red como UDP, ICMP, ICMPv6 y protocolos de capa de enlace como IEEE 802.1x, IEEE 802.1 li y un perfil de Bluetooth.

Además, existen las siguientes variaciones de las realizaciones que se han descrito en lo que antecede:

1. Reutilización del método de EAP-SIM

El método, en el que un mecanismo de autenticación es un mecanismo que usa R-UIM (tal como se ha descrito en lo que antecede con respecto a la segunda realización, por ejemplo), está insertado en la misma encapsulación de protocolo que en el método para SIM, que se denomina EAP-SIM. Este uso es la reutilización del protocolo de EAP-SIM para portar la autenticación basada en R-UIM con el algoritmo de CAVE.

Una indicación del uso alterno de EAP-SIM se puede indicar usando un campo reservado en el protocolo de EAP-SIM, o como alternativa, un atributo adicional, llámese este AT-R-UIM.

2. Ubicación de la terminación de lado de red para los algoritmos de tarjeta inteligente

El punto de terminación de lado de red del algoritmo que se corresponde con el que se ejecuta en la tarjeta inteligente (algoritmo de secreto de AKA o de CAVE), se podría encontrar, en principio, o bien en el HLR / AuC, o bien ubicado junto con el servidor de AAA Propio AAAH (la figura 1). En el caso anterior, existe una interfaz, llámese esta G_h, a través de la cual el servidor de AAA propio propaga diálogos para el triplete / quintuplete con el algoritmo de tarjeta inteligente en cuestión, que usa un protocolo de red celular a través de G_h.

Además, se hace notar que el dispositivo o terminal móvil es solo un ejemplo para un terminal de abonado. Se hace notar que la expresión “móvil” no solo quiere decir que el terminal móvil está conectado con una red por medio de un enlace de radio, sino también un terminal que se puede conectar con diferentes medios de red de acceso por medio de cables fijos, por ejemplo. Por ejemplo, este puede incluir un ordenador que se puede conectar con terminales de red fijos tales como un ordenador que se puede conectar con una red fija en habitaciones de hotel, trenes y similares.

REIVINDICACIONES

1. Un sistema para autenticar y autorizar servicios de red que comprende:

un dispositivo móvil, estando configurado dicho dispositivo móvil
para determinar un tipo de acceso de red tras la recepción de un mensaje de información que indica al menos un tipo de acceso de red;
crear un mensaje de inicio que contiene al menos una identidad de usuario; y
encapsular el mensaje de inicio en un mensaje de autenticación compatible con una red de acceso que se identifica en el mensaje de información, comprendiendo adicionalmente dicho sistema:

un controlador de acceso para leer el mensaje encapsulado a partir del dispositivo móvil y reenviar el mensaje encapsulado a un servidor de autenticación que se identifica en el mensaje encapsulado.

2. El sistema de acuerdo con la reivindicación 1, que comprende adicionalmente:

un encaminador para expedir el mensaje de información, en donde el mensaje de información incluye un anuncio de encaminador.

3. El sistema de acuerdo con la reivindicación 1, en el que el mensaje de información indica un soporte de protocolo de autenticación extensible (EAP).

4. El sistema de acuerdo con la reivindicación 1, en el que el controlador de acceso está adaptado para expedir el mensaje de información al entrar el dispositivo móvil en la red.

5. El sistema de acuerdo con la reivindicación 1, en el que el mensaje de inicio contiene un mensaje de opción de identificador de cliente y un mensaje de opción de identidad de soporte de protocolo de autenticación extensible, en donde dichos mensajes contienen información relativa a al menos uno de tipo de cliente, identidad de usuario e información de dirección medular.

6. El sistema de acuerdo con la reivindicación 1, en el que un protocolo entre el dispositivo móvil y la red de acceso comprende al menos uno de UDP, ICMPv6, IEEE 802.1x, IEEE 802.11i y un perfil de Bluetooth.

7. El sistema de acuerdo con la reivindicación 1, en el que un mecanismo de autenticación que se aplica comprende un protocolo de autenticación extensible (EAP).

8. El sistema de acuerdo con la reivindicación 1, en el que un mecanismo de autenticación que se aplica es un mecanismo de autenticación que usa un módulo de identidad de usuario extraíble (R-UIM) que aplica un algoritmo de Autenticación Celular y Cifrado de Voz (CAVE).

9. El sistema de acuerdo con la reivindicación 1, en el que el controlador de acceso se proporciona en un Agente Propio del dispositivo móvil.

10. El sistema de acuerdo con la reivindicación 2, en el que el encaminador comprende
unos medios de creación para crear el mensaje de información que indica el al menos un tipo de acceso de red, y
unos medios de envío para enviar el mensaje de información a un dispositivo de abonado.

11. El sistema de acuerdo con la reivindicación 10, en el que el mensaje de información incluye un anuncio de encaminador.

12. El sistema de acuerdo con la reivindicación 2, en el que el mensaje de información indica un soporte de protocolo de autenticación extensible (EAP).

13. El sistema de acuerdo con la reivindicación 2, en el que el encaminador es parte del dispositivo de control de acceso.

14. Un método para autenticar y autorizar servicios de red, en el que la red comprende un dispositivo móvil y una función de control de autenticación, comprendiendo el método
determinar un tipo de acceso de red mediante el dispositivo móvil, tras la recepción de un mensaje de información que indica al menos un tipo de acceso de red;
crear un mensaje de inicio que contiene al menos una identidad de usuario,
encapsular el mensaje de inicio en un mensaje de autenticación compatible con una red de acceso identificada en el mensaje de información, y
leer, mediante un controlador de acceso, el mensaje encapsulado a partir del dispositivo móvil y reenviar el mensaje encapsulado a un servidor de autenticación identificado en el mensaje encapsulado.

15. El método de acuerdo con la reivindicación 14, en el que la red comprende adicionalmente un encaminador, que expide el mensaje de información, en donde el mensaje de información comprende un anuncio de encaminador.

16. El método de acuerdo con la reivindicación 14, en el que el mensaje de información indica un soporte de protocolo de autenticación extensible (EAP).

17. El método de acuerdo con la reivindicación 14, en el que el mensaje de información se expide cuando el dispositivo móvil entra en la red.

18. El método de acuerdo con la reivindicación 14, en el que el mensaje de inicio contiene un mensaje de opción de identificador de cliente y un mensaje de opción de identidad de soporte de protocolo de autenticación extensible, que contienen al menos uno de tipo de cliente, identidad de usuario e información de dirección medular.

19. El método de acuerdo con la reivindicación 14, en el que un protocolo entre el dispositivo móvil y la red de acceso es al menos uno de UDP, ICMPv6, IEEE 802.1x, IEEE 802.11 i y un perfil de Bluetooth.

20. El método de acuerdo con la reivindicación 14, en el que un mecanismo de autenticación que se aplica comprende un protocolo de autenticación extensible (EAP).

21. El método de acuerdo con la reivindicación 14, en el que un mecanismo de autenticación que se aplica comprende un mecanismo de autenticación que usa un módulo de identidad de usuario extraíble (R-UIM) que aplica un algoritmo de Autenticación Celular y Cifrado de Voz (CAVE).

22. El método de acuerdo con la reivindicación 14, en el que la función de controlador de acceso se proporciona en un Agente Propio (HA) del dispositivo móvil.

23. Un dispositivo de control de acceso que comprende:

unos medios de recepción para recibir un mensaje de inicio que está encapsulado en un mensaje de autenticación, siendo el mensaje de autenticación compatible con una red de acceso identificada en un mensaje de información,
unos medios de procesamiento para leer el mensaje encapsulado, y
unos medios de reenvío para reenviar el mensaje encapsulado a un servidor de autenticación identificado en el mensaje encapsulado.

24. El dispositivo de control de acceso de acuerdo con la reivindicación 23, en el que el mensaje de inicio contiene un mensaje de opción de identificador de cliente y un mensaje de opción de identidad de soporte de protocolo de autenticación extensible, en donde dichos mensajes contienen información relativa a al menos uno de tipo de cliente, identidad de usuario e información de dirección medular.

25. El dispositivo de control de acceso de acuerdo con la reivindicación 23, en donde el dispositivo de control de acceso se proporciona en un Agente Propio de un dispositivo móvil que ha enviado el mensaje de inicio.

26. El dispositivo de control de acceso de acuerdo con la reivindicación 23, que comprende adicionalmente unos medios de envío para enviar el mensaje de información a un dispositivo de abonado que indica al menos un tipo de acceso de red.

27. El dispositivo de control de acceso de acuerdo con la reivindicación 26, en el que el mensaje de información incluye un anuncio de encaminador.

28. El dispositivo de control de acceso de acuerdo con la reivindicación 26, en el que el mensaje de información indica un soporte de protocolo de autenticación extensible (EAP).

29. El dispositivo de control de acceso de acuerdo con la reivindicación 26, en el que el mensaje de información se expide cuando el dispositivo móvil entra en una red.

30. Un dispositivo de abonado que comprende:

unos medios de determinación para determinar un tipo de acceso de red tras la recepción de un mensaje de información que indica al menos un tipo de acceso de red;
unos medios de creación para crear un mensaje de inicio que contiene al menos una identidad de usuario;
unos medios de encapsulación para encapsular el mensaje de inicio en un mensaje de autenticación compatible con una red de acceso identificada en el mensaje de información; y
unos medios de envío para enviar el mensaje de inicio a un dispositivo de control de acceso.

31. El dispositivo de abonado de acuerdo con la reivindicación 30, en donde el dispositivo de abonado es un dispositivo móvil.

32. El dispositivo de abonado de acuerdo con la reivindicación 30, en el que el mensaje de información indica un soporte de protocolo de autenticación extensible (EAP).

33. El dispositivo de abonado de acuerdo con la reivindicación 30, en el que el mensaje de información se expide cuando el dispositivo de abonado entra en una red.

34. El dispositivo de abonado de acuerdo con la reivindicación 30, en el que el mensaje de inicio contiene un mensaje de opción de identificador de cliente y un mensaje de opción de identidad de soporte de protocolo de autenticación extensible, en donde dichos mensajes contienen información relativa a al menos uno de tipo de cliente, identidad de usuario e información de dirección medular.

35. El dispositivo de abonado de acuerdo con la reivindicación 30, en el que un mecanismo de autenticación que se aplica es un mecanismo de autenticación que usa un módulo de identidad de usuario extraíble (R-UIM) que aplica un algoritmo de Autenticación Celular y Cifrado de Voz (CAVE).

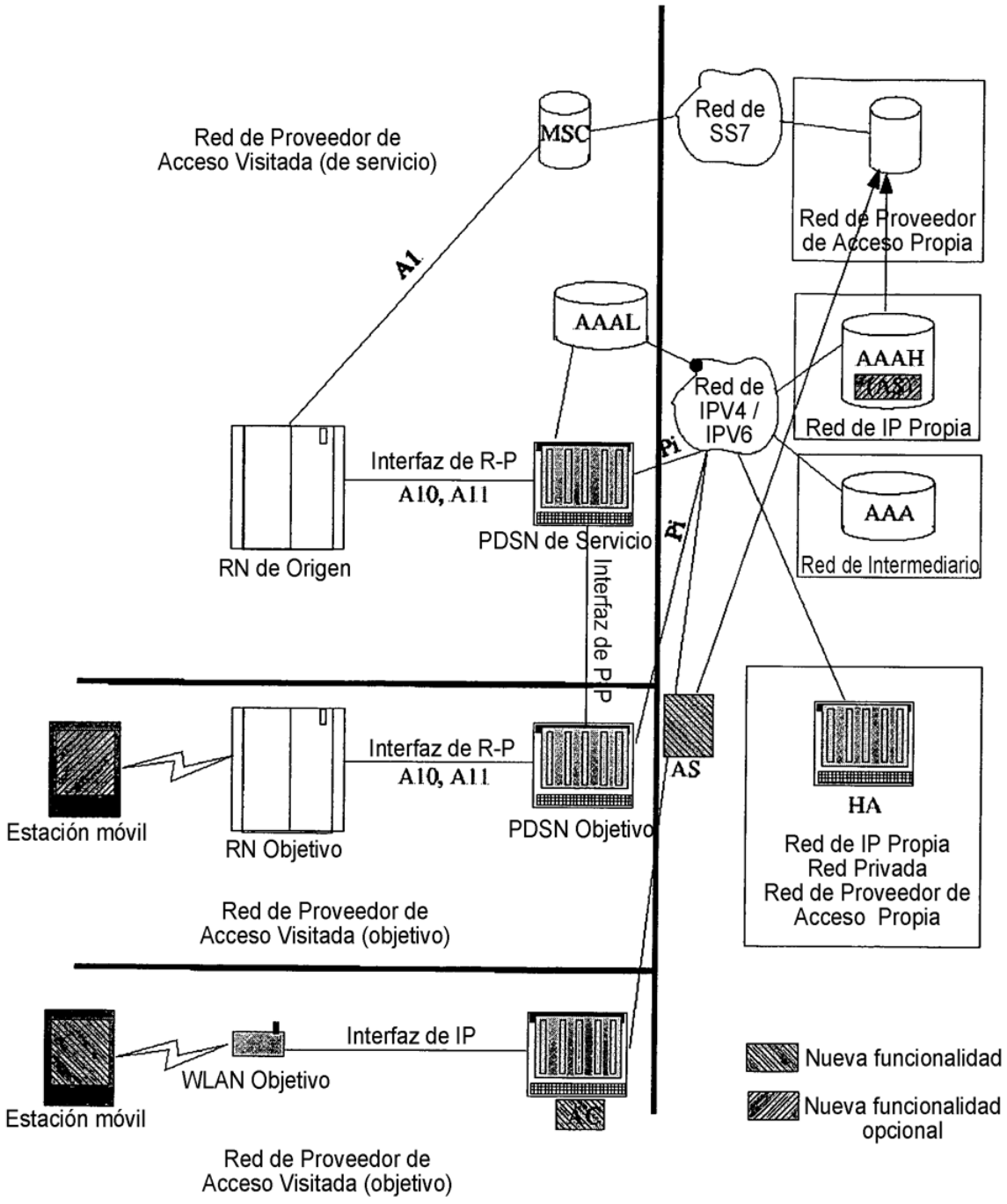
Red de Proveedor de Acceso Visitada (de servicio)
MSC
Red de SS7
Red de Proveedor de Acceso Propia
A1
AAAL
AAAH
Red de IP Propia
Red de IPV4 / IPV6
Pi
Interfaz de R-P
A10, A11
PDSN de Servicio
RN de Origen
AAA
Red de Intermediario
Interfaz de PP
AS
HA
Estación móvil
RN Objetivo
PDSN Objetivo
Red de IP Propia
Red Privada
Red de Proveedor de Acceso Propia
Red de Proveedor de Acceso Visitada (objetivo)
Interfaz de IP
WLAN Objetivo
AC
Estación móvil
Nueva funcionalidad
Nueva funcionalidad opcional
Red de Proveedor de Acceso Visitada (objetivo)

Fig. 1

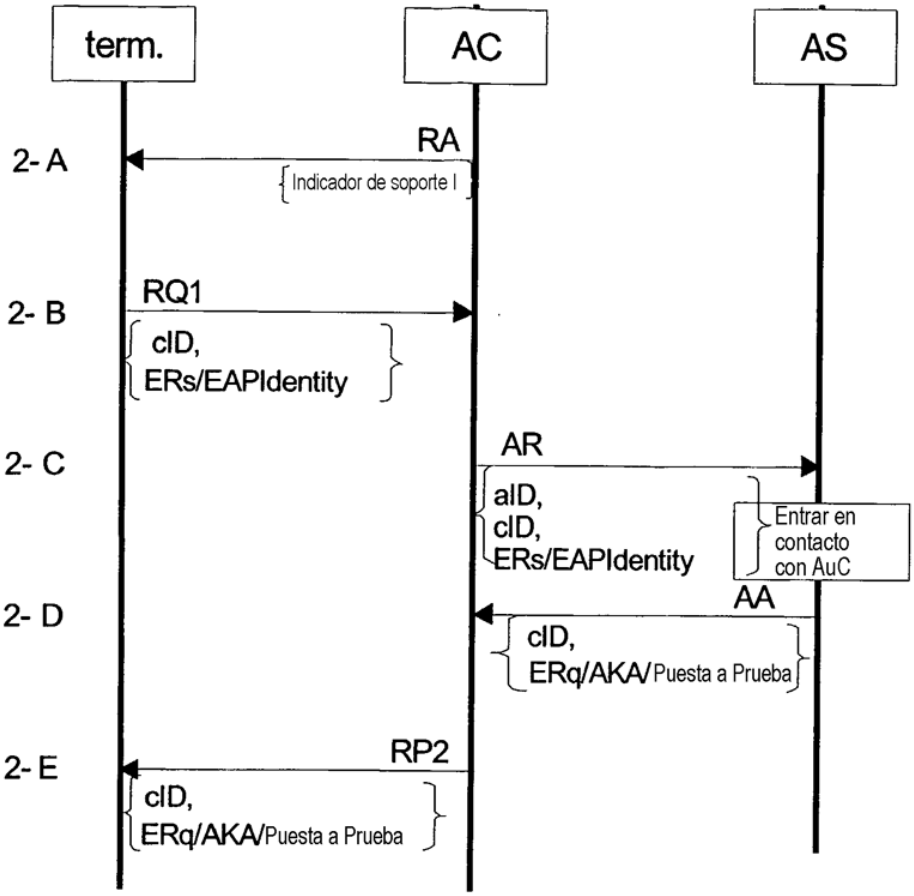
term.
AC
AS
2- A
RA
Indicador de soporte I
2- B
RQ1
cID,
ERs/EAPIdentity
2- C
AR
aID,
cID,
ERs/EAPIdentity
Entrar en contacto con AuC
AA
2- D
cID,
ERq/AKA/Puesta a Prueba
2- E
RP2
cID,
ERq/AKA/Puesta a Prueba

Fig. 2A

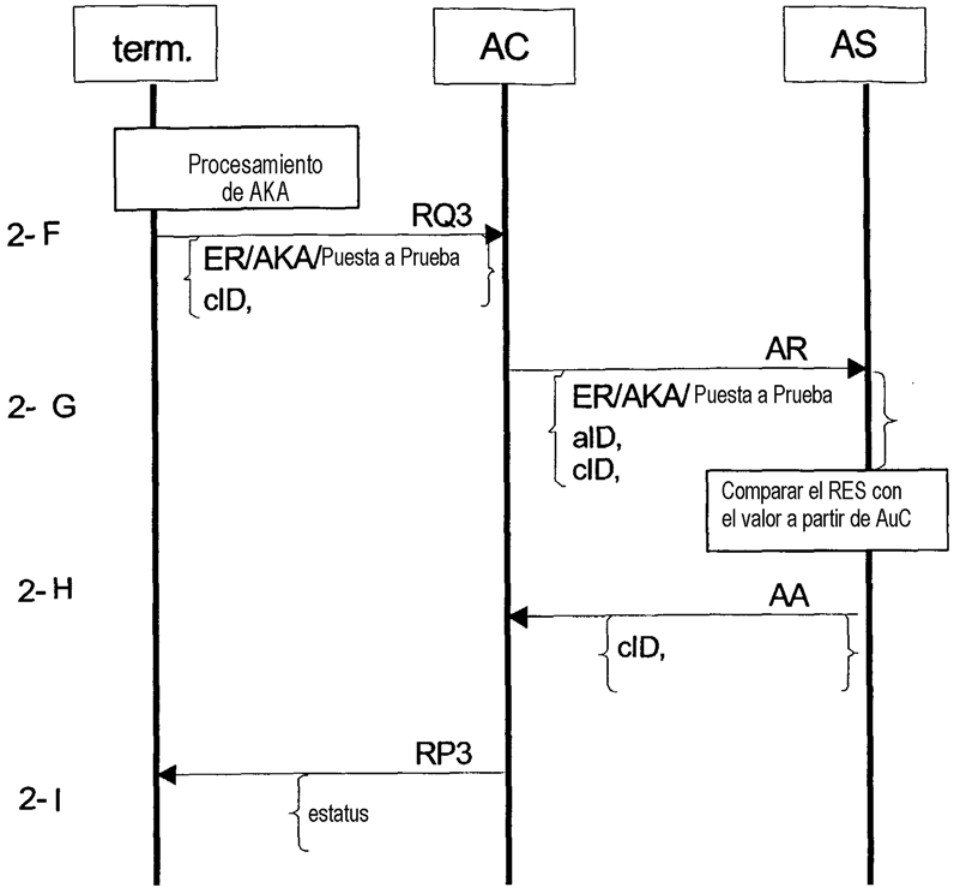
term.
AC
AS
Procesamiento de AKA
2- F
RQ3
ER/AKA/Puesta a Prueba
cID,
AR
2- G
ER/AKA/ Puesta a Prueba
aID,
cID,
Comparar el RES con el valor a partir de AuC
2- H
AA
cID,
RP3
2- I
estatus

Fig. 2B

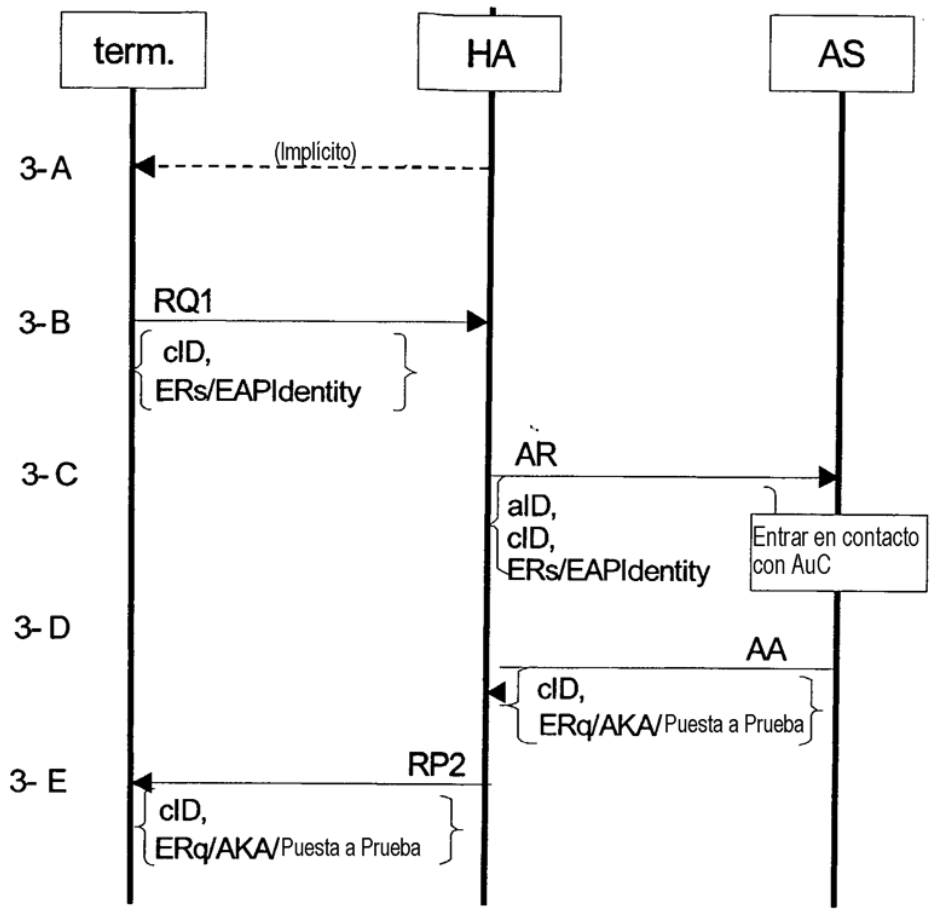
term.
HA
AS
3-A
(Implícito)
3-B
RQ1
cID,
ERs/EAPIdentity
3-C
AR
aID,
cID,
ERs/EAPIdentity
Entrar en contacto con AuC
3-D
AA
cID,
ERq/AKA/Puesta a Prueba
3-E
RP2
cID,
ERq/AKA/Puesta a Prueba

Fig. 3A

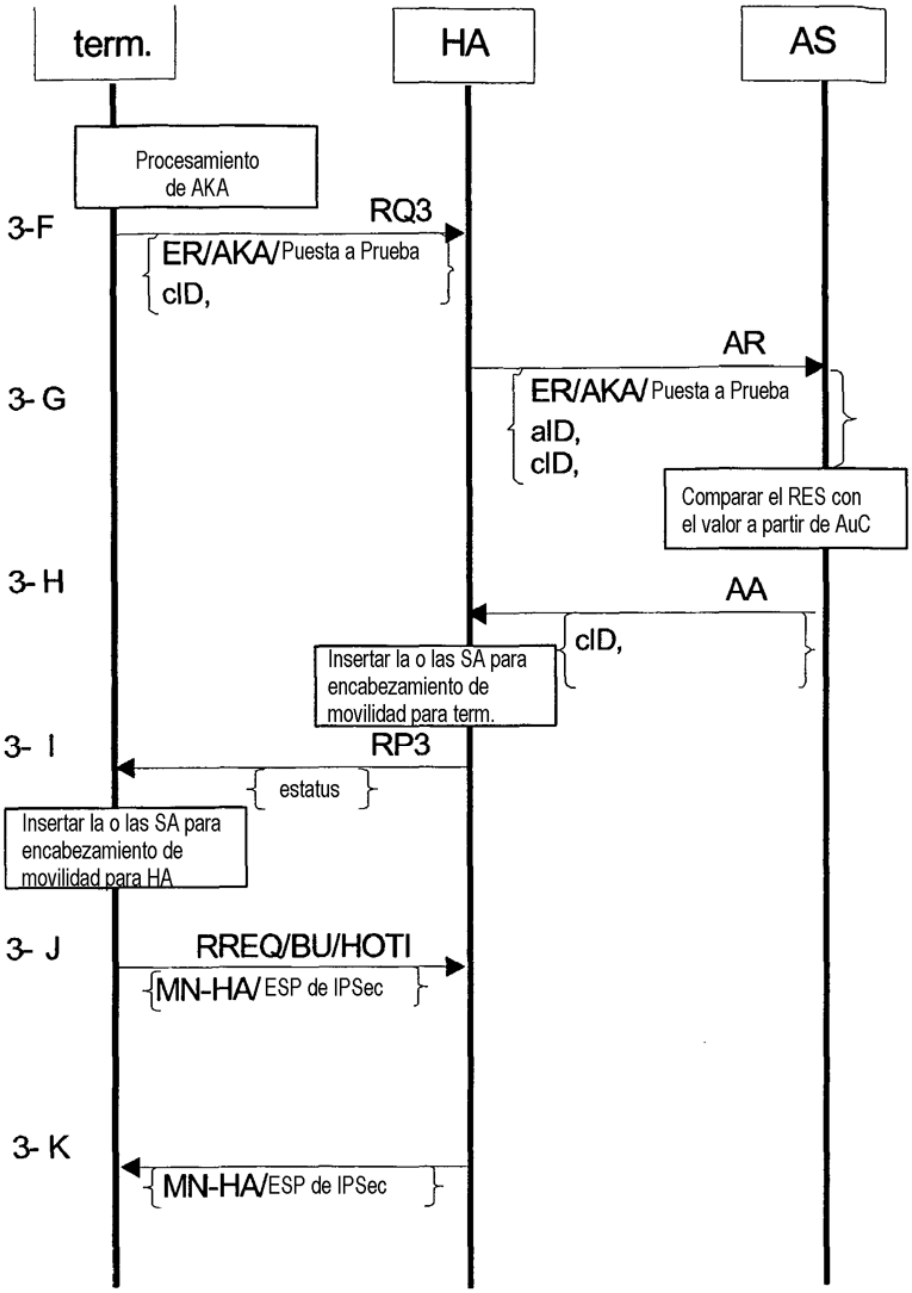
term.
HA
AS
Procesamiento de AKA
3-F
RQ3
ER/AKA/ Puesta a Prueba
cID,
AR
3- G
ER/AKA/ Puesta a Prueba
aID,
cID,
Comparar el RES con el valor a partir de AuC
3- H
AA
cID,
Insertar la o las SA para encabezamiento de movilidad para term.
3- I
RP3
estatus
Insertar la o las SA para encabezamiento de movilidad para HA
3- J
RREQ/BU/HOTI
MN-HA/ ESP de IPSec
3- K
MN-HA/ESP de IPSec

Fig. 3B

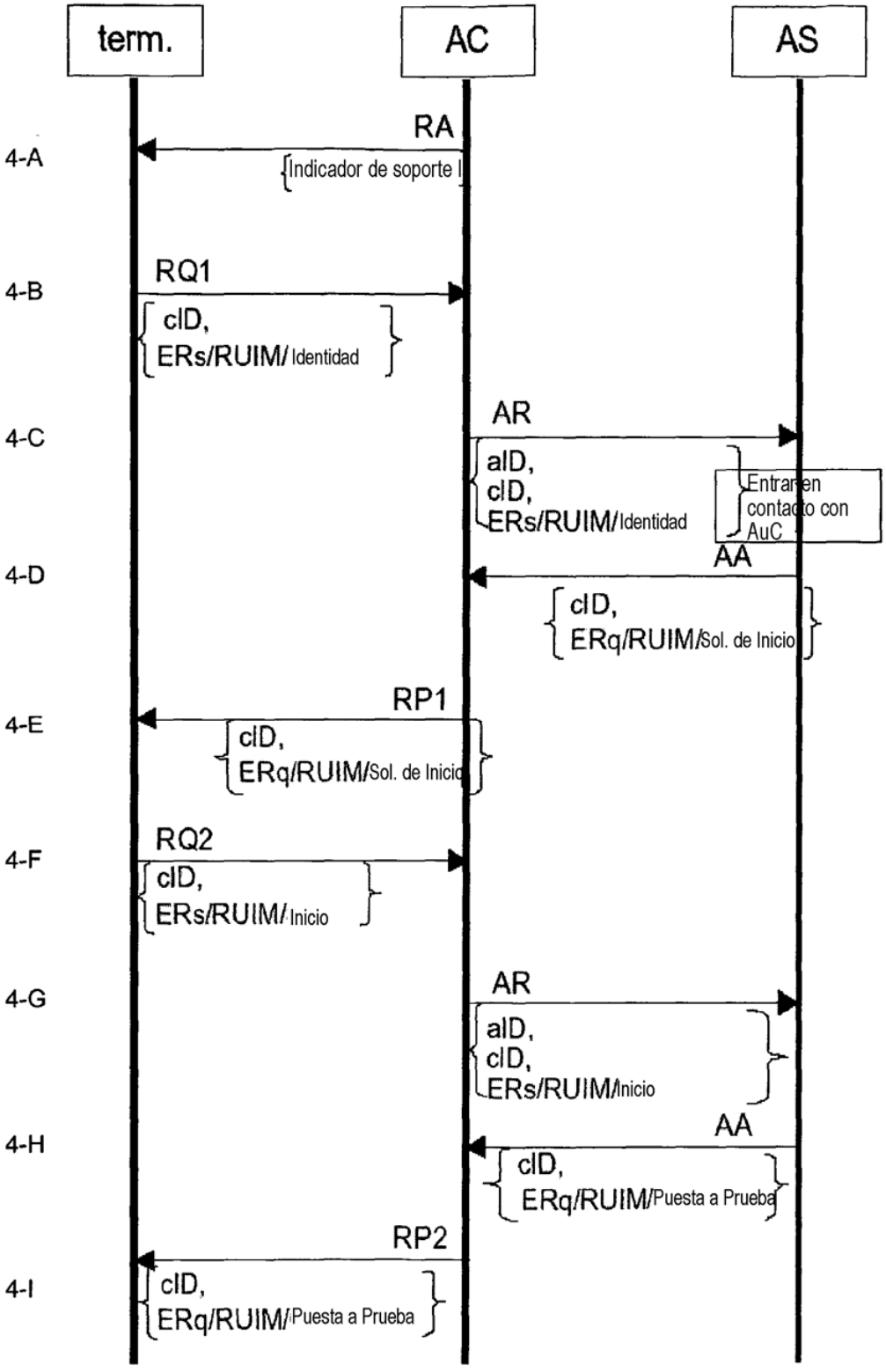
term.
AC
AS
RA
4-A
Indicador de soporte I
RQ1
4-B
clD,
ERs/RUIM/ Identidad
AR
4-C
alD,
clD,
ERs/RUIM/Identidad
Entran en contacto con AuC
AA
4-D
clD,
ERq/RUIM/Sol. de Inicio
RP1
4-E
clD,
ERq/RUIM/Sol. de Inicio
RQ2
4-F
clD,
ERs/RUIM/ Inicio
AR
4-G
alD,
clD,
ERs/RUIM/Inicio
AA
4-H
clD,
ERq/RUIM/Puesta a Prueba
RP2
4-I
clD,
ERq/RUIM/Puesta a Prueba

Fig. 4A

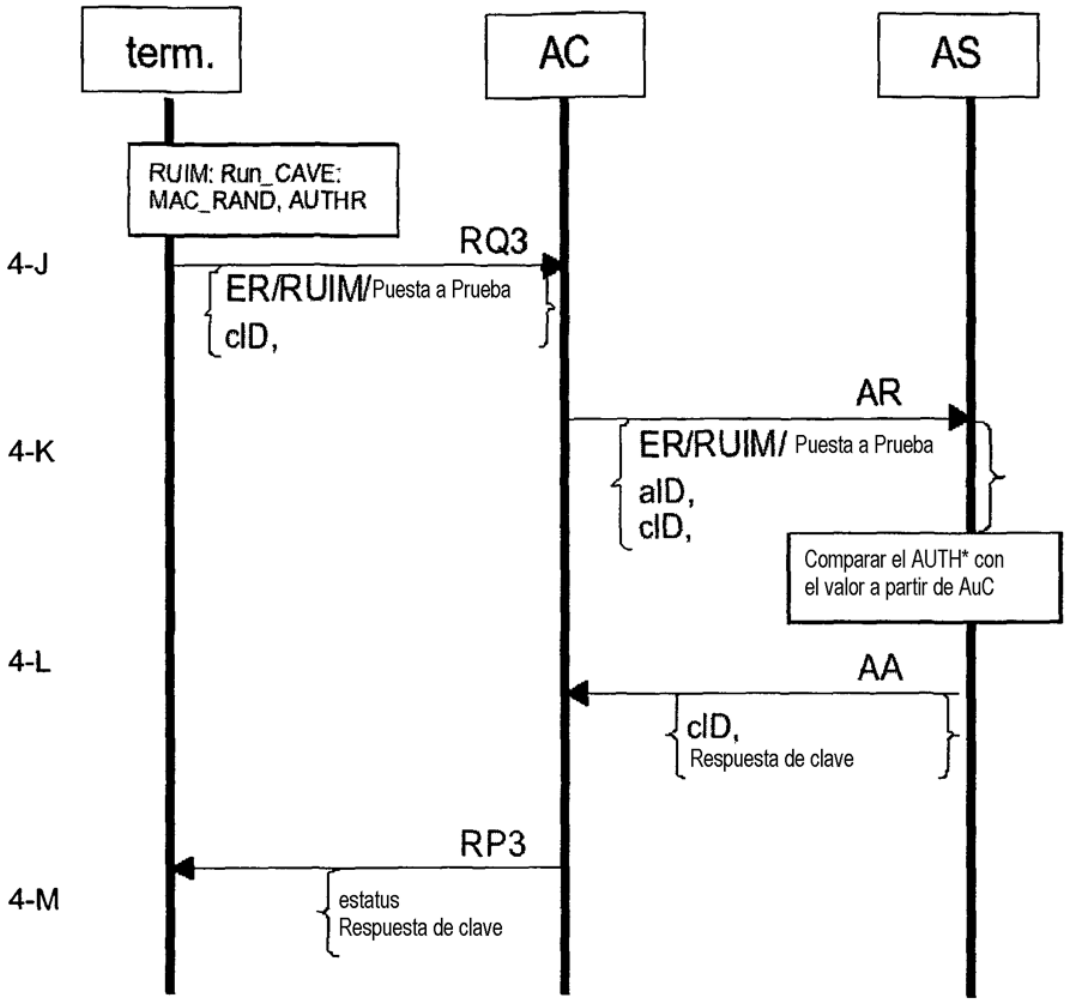
term.
AC
AS
RUIM: Run_CAVE:
MAC_RAND, AUTHR
4-J
RQ3
ER/RUIM/Puesta a Prueba
clD,
AR
4-K
ER/RUIM/ Puesta a Prueba
alD,
clD,
Comparar el AUTH* con
el valor a partir de AuC
4-L
AA
clD,
Respuesta de clave
RP3
4-M
estatus
Respuesta de clave

Fig. 4B

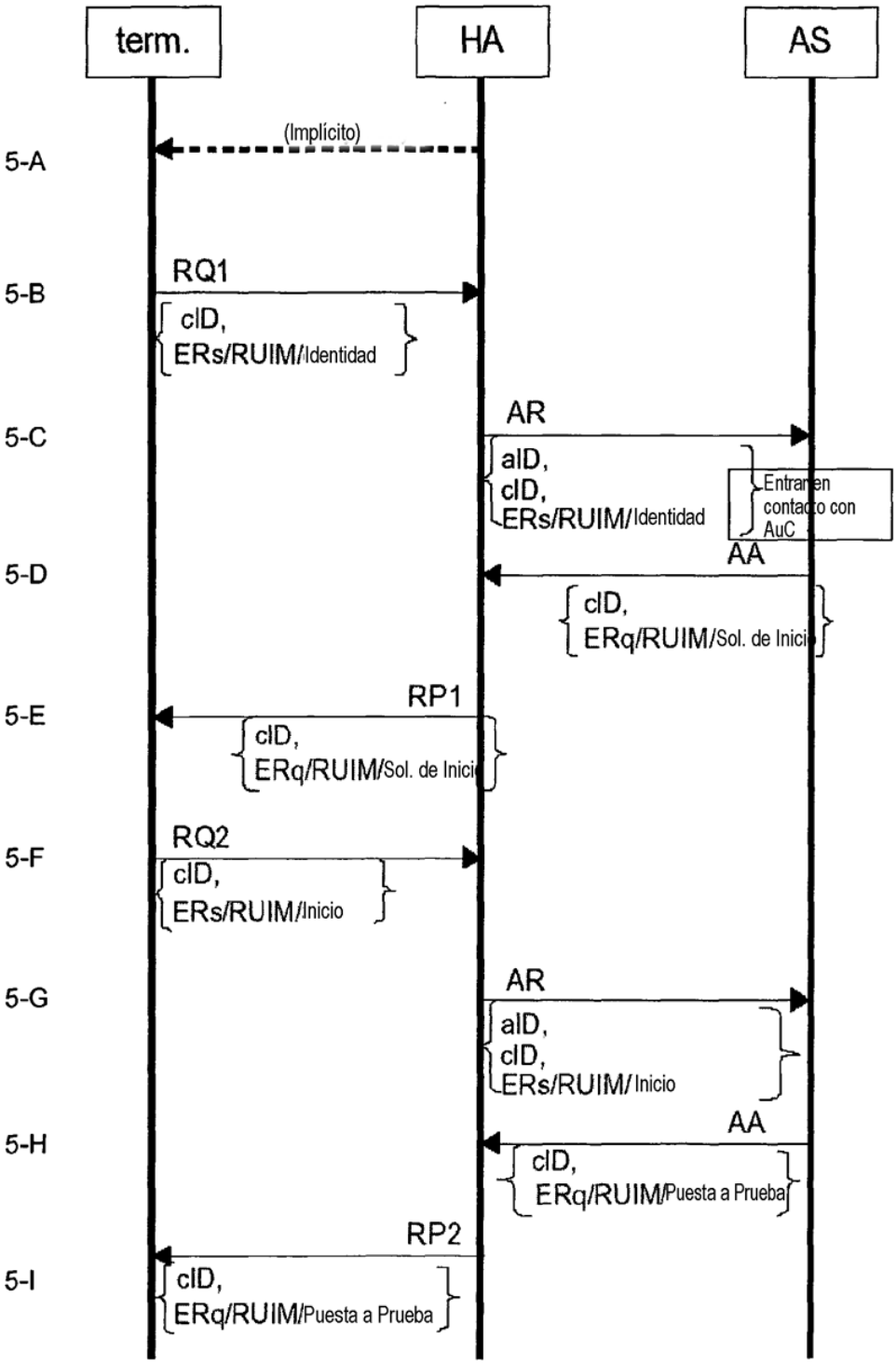
term.
HA
AS
5-A
(Implícito)
5-B
RQ1
clD,
ERs/RUIM/Identidad
5-C
AR
alD,
clD,
ERs/RUIM/Identidad
Entran en contacto con AuC
AA
5-D
clD,
ERq/RUIM/Sol. de Inici
5-E
RP1
clD,
ERq/RUIM/Sol. de Inici
5-F
RQ2
clD,
ERs/RUIM/Inicio
5-G
AR
alD,
clD,
ERs/RUIM/Inicio
AA
5-H
clD,
ERq/RUIM/Puesta a Prueba
RP2
5-I
clD,
ERq/RUIM/Puesta a Prueba

Fig. 5A

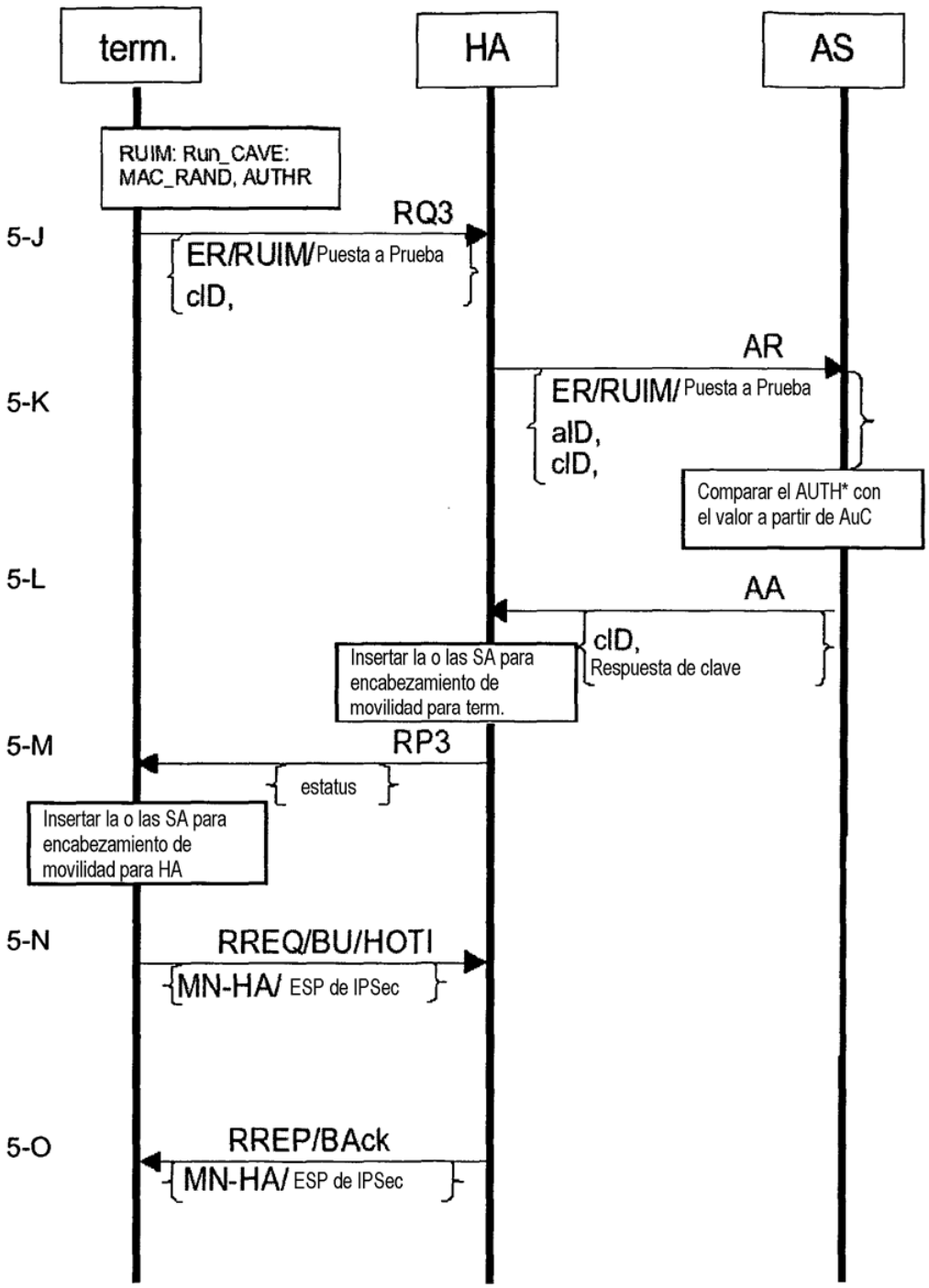
term.
HA
AS
RUIM: Run_CAVE: MAC_RAND, AUTHR
5-J
RQ3
ER/RUIM/ Puesta a Prueba
clD,
AR
5-K
ER/RUIM/ Puesta a Prueba
alD,
clD,
Comparar el AUTH* con el valor a partir de AuC
5-L
AA
clD,
Respuesta de clave
Insertar la o las SA para encabezamiento de movilidad para term.
5-M
RP3
estatus
Insertar la o las SA para encabezamiento de movilidad para HA
5-N
RREQ/BU/HOTI
MN-HA/ ESP de IPSec
5-O
RREP/BAck
MN-HA/ ESP de IPSec

Fig. 5B

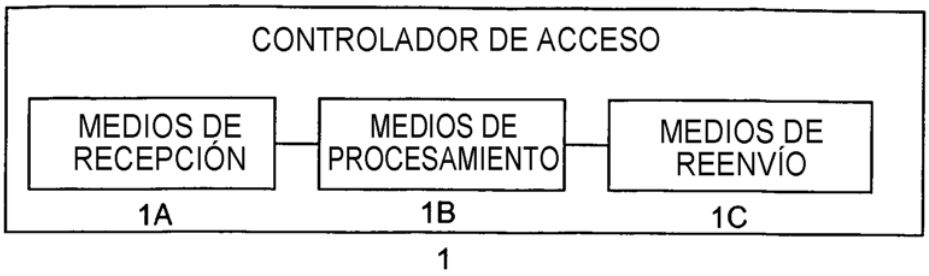

Fig. 6A

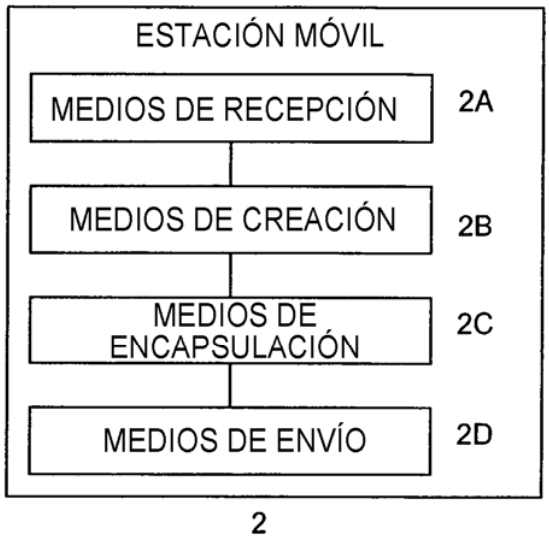

Fig. 6B

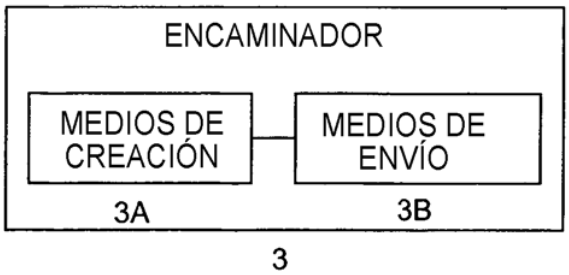

Fig. 6C