(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 447 546**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04W 76/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.11.2008 E 08873855 (4)**

(97) Fecha y número de publicación de la concesión europea: **15.01.2014 EP 2263396**

(54) Título: **Acceso a través de redes de acceso no-3GPP**

(30) Prioridad:

11.04.2008 US 44242 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.03.2014

(73) Titular/es:

TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

NÄSLUND, MATS;
ARKKO, JARI;
BLOM, ROLF;
LEHTOVIRTA, VESA;
NORRMAN, KARL;
ROMMER, STEFAN y
SAHLIN, BENGT

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Acceso a través de redes de acceso no-3GPP

Campo técnico

La presente invención se refiere a un método de establecimiento de comunicación entre un UE (User Equipment, equipo de usuario), denominado a asimismo un terminal, un terminal de usuario o una estación de usuario, y un nodo de red, y se refiere además a un sistema que comprende por lo menos un UE y un nodo de red.

Antecedentes

El 3GPP (3rd Generation Partnership Project, proyecto de asociación de tercera generación) está en el proceso de definición de un estándar extendido para la transmisión de paquetes de datos, denominado EPS (Evolved Packet System, sistema evolucionado de paquetes). En el EPS, además de tecnologías de acceso-3GPP nativas tales como WCDMA (Wideband Code Division Multiple Access, acceso múltiple por división de código de banda ancha), LTE (Long Term Evolution, evolución a largo plazo), estará soportado asimismo el acceso a servicios de comunicación de datos y/o servicios de Internet a través de acceso no-3GPP, incluyendo en particular el acceso a través de una red local tal como una HPLMN (Home Public Land Mobile Network, red móvil terrestre pública local) por medio de métodos/tecnologías/redes/estándares de acceso no-3GPP, por ejemplo WiMAX acorde con el estándar IEEE 802.16, una WLAN (Wireless Local Area Network, red de área local inalámbrica), por ejemplo acorde con el estándar IEEE 802.11g/n, xDSL (Digital Subscriber Line, línea de abonado digital), etc. Para el objetivo de la invención descrita en la presente memoria, "red local" debe entenderse como la entidad con la que un usuario tiene un acuerdo comercial, a menudo en forma de abono, para el acceso de red o acceso de servicios y por lo tanto comprende tanto redes convencionales de operador de telecomunicaciones, como operadores virtuales, etc. El documento US-2008/0026734-A1 da a conocer un sistema de este tipo, que involucra un UE que conecta a una red-3GPP a través de una red de acceso WLAN. Una red de acceso puede ser gestionada y/o administrada por otra entidad diferente a la red local, en cuyo caso existe normalmente un acuerdo comercial entre las dos redes.

Los métodos de acceso no-3GPP pueden agruparse en una de estas dos categorías:

- Acceso no-3GPP de confianza, y

- Acceso no-3GPP no de confianza, denominado así mismo acceso no-3GPP no fiable.

Las dos categorías de acceso no-3GPP se muestran en la figura 1a, que es una vista general de un "sistema de paquetes evolucionado" tal como se define en el documento estándar 3GPP TS23.402, "Architecture enhancement for non-3GPP accesses".

La definición exacta de los términos "de confianza" y "no de confianza" para un acceso EPS está actualmente bajo discusión. La discusión se complica debido al hecho de que aplican tanto aspectos técnicos -considérese, por ejemplo, la siguiente cuestión: ¿el acceso es seguro/de confianza debido a unos medios técnicos de protección suficiente? - como aspectos comerciales -considérese, por ejemplo la siguiente cuestión: ¿tiene el operador local, es decir el operador de la red local, un "acuerdo" lo suficientemente fuerte con el operador de la red de acceso como para considerar la red de acceso como de confianza desde el punto de vista del operador local? Por lo tanto, existe tanto un interés de los abonados (por ejemplo, privacidad) como un interés de los operadores (por ejemplo, comercial) para determinar si cierto acceso es o no de confianza.

Lo que sí está claro es que las redes de acceso no-3GPP de confianza y no de confianza son generalmente redes de acceso IP (protocolo de Internet) que utilizan tecnología de acceso, cuya especificación está fuera del alcance de 3GPP. Una "hipótesis" de trabajo adoptada recientemente por el 3GPP SA2 a este respecto es que si una red de acceso IP no-3GPP es o no de confianza, no es una característica de la propia red de acceso. En un escenario no itinerante, es una decisión del operador de la HPLMN, es decir el operador local, si una red de acceso IP no-3GPP se utiliza como una red acceso no-3GPP de confianza o no de confianza, y compete al operador implementar medidas de seguridad adecuadas en el caso respectivo, por ejemplo según la discusión siguiente de la descripción de antecedentes.

Resulta obvio que los diferentes tipos de accesos no-3GPP utilizarán diferentes medios de protección entre la red local y el terminal/UE, por ejemplo:

- En el establecimiento de conectividad en un acceso no de confianza, se establecerá probablemente un túnel IPsec (Internet Protocol Security, protocolo de seguridad de internet) entre el terminal y un nodo de "pasarela" "sobre" el acceso, es decir, una ePDG (evolved Packet Data Gateway, pasarela de paquetes de datos evolucionada), tal como se muestra en la figura 1a. Se entiende que en la presente memoria "conectividad" significa "el estado o un estado de estar conectado". El establecimiento del túnel IPsec se realiza además mediante un procedimiento ejecutado según el protocolo IKE (Internet Key Exchange, intercambio de clave de Internet), específicamente la versión 2 del mismo. Esto hará la seguridad más o menos independiente de las características de seguridad de la red de acceso utilizada. No obstante, una red de confianza no tendrá o necesitará esta característica.

- En el establecimiento de conectividad en un acceso de confianza es probable que se utilice el EAP (Extensible Authentication Protocol, protocolo de autenticación extensible) y éste puede incluir, pero no necesariamente, el método EAP AKA (Authentication and Key Agreement, acuerdo de autenticación y gestión de claves) para la autenticación de acceso, mientras que un acceso no de confianza puede utilizar o no utilizar el EAP.

- Los accesos establecidos según diferentes métodos pueden utilizar diferentes soluciones de movilidad, por ejemplo MIP (IP móvil) o PMIP (Proxy MIP). Con respecto a movilidad y seguridad IP, MIP se da a conocer el documento US-2007/006295-A1, que da a conocer un método que proporciona movilidad segura para un terminal en un sistema móvil que comprende por lo menos dos subredes basadas en IP. De acuerdo con el método, un terminal detecta una nueva subred basada en IP y sus requisitos de seguridad.

Considérese un UE que está a punto de establecer conectividad, por ejemplo con la finalidad de unirse a algún servicio o servicios a través de una red de acceso no-3GPP. A priori, en general el UE no sabe si el acceso está o no considerado como "de confianza" por la red local. Entonces la cuestión consiste en si el UE debería o no establecer un túnel IPsec con una ePDG, siendo éste un procedimiento que requiere recursos/costes/tiempo relativamente elevados que deberían evitarse en la medida de lo posible. En particular, si el UE intenta utilizar el IKE/IPsec, pero éste no está de hecho soportado por la red, se derrocha señalización y/o pueden producirse casos de error.

Si bien el UE podría estar preconfigurado estáticamente con información adecuada, no existen métodos utilizados de forma general para señalizar dinámicamente al UE si el acceso está o no considerado de confianza. En general, el UE puede deducir algunos aspectos "técnicos" de la propia tecnología utilizada, por ejemplo WiMAX o WLAN, pero el UE no puede obtener información y comprender todos los aspectos técnicos, por ejemplo la presencia de una ePDG o qué protocolo de movilidad debe ser utilizado. A un nivel superior, el UE no puede conocer los aspectos de carácter "comercial". Por ejemplo, considérese una red de acceso no-3GPP dada, por ejemplo una red WIMAX proporcionada por una parte o un operador A. Dos diferentes operadores de red local, B y C, podrían tener opiniones diferentes sobre si la parte A y la red proporcionada por la misma es o no de confianza, debido a sus políticas de seguridad y acuerdos comerciales. Por lo tanto, un UE que utiliza un abono en el operador B debería considerar quizás de confianza la parte A y su red de acceso, mientras que un UE que utiliza un abono en el otro operador C debería considerar no de confianza la parte A y su red de acceso. La situación se complica más aún si se tienen en cuenta accesos "heredados" a través de redes 3GPP, por ejemplo una I-WLAN (Interworking Wireless Local Area Network, red de área local inalámbrica de interconexión) según el documento estándar 3GPP TS 33.234. En un acceso a través de una red de acceso I-WLAN, puede utilizarse una pasarela en forma de una PDG (Packet Data Gateway (pasarela de paquetes de datos), una pasarela acorde con el estándar 3GPP general o anterior, a diferenciar de la ePDG especial mencionada anteriormente) para determinar el túnel IPsec hacia/desde el UE y por lo tanto esta red WLAN se considerará como "no de confianza". Sin embargo, en el futuro el acceso a través de una WLAN conectada a un EPS podría, quizás, ser de confianza, por ejemplo debido a la utilización de mejoras de seguridad acordes con el estándar IEEE 802.11i, y por lo tanto no utilizaría o no tendría la IPsec/PDG. Esto muestra (de nuevo) que una tecnología de acceso dada puede o no ser considerada de confianza y utilizar diferentes medios de seguridad hacia el UE, dependiendo de la situación.

En resumen, puede existir una necesidad de un modo de notificar al UE sobre por lo menos alguna "propiedad" de la red de acceso, tal como una propiedad que implique si el acceso es o no de confianza, qué tipo de funciones de movilidad y seguridad deberían utilizarse, etc. Además, un método para realizar dicha notificación debería ser lo suficientemente seguro como para evitar ataques y por supuesto debería proporcionar asimismo robustez en general.

Compendio

Un objetivo de la invención es permitir a un UE establecer conectividad con, o a través de una red, de tal modo que por lo menos en uno o varios aspectos ésta sea eficiente y/o segura.

Dichos aspectos pueden incluir, por ejemplo, sobrecarga de ancho de banda/señalización/computacional y resistencia frente a ataques maliciosos.

De este modo, puede permitirse al UE, por ejemplo, elegir un modo de comunicación en función de si una red a través de la cual deberá conectarse es o no de confianza.

Se da a conocer un método realizado por un equipo de usuario para la comunicación a través de una red de acceso. El método comprende las etapas de:

- recuperar información especial a partir de, o para interpretar una condición especial indicada en un mensaje enviado al equipo de usuario desde un servidor AAA en una red local del equipo de usuario, en un procedimiento de autenticación que forma parte del establecimiento de una conexión desde el equipo de usuario a través de la red de acceso, la condición especial haciendo referencia a si la red de acceso es o no de confianza, y

- utilizar, en una etapa siguiente del procedimiento de establecimiento de la conexión, la información recuperada o el resultado de la interpretación de la condición especial, para seleccionar un modo apropiado de establecer la conectividad a través de la red de acceso.

La red de acceso puede ser, por ejemplo, una WLAN, que comprende una parte de acceso radioeléctrico WLAN y la conexión de línea fija con el punto de acceso, y posiblemente asimismo una red central o partes seleccionadas de la misma detrás de una red de acceso.

La información acerca de si la red de acceso es o no de confianza, o una indicación al respecto, puede enviarse en o dentro de mensajes transmitidos al UE en una etapa preliminar de establecimiento de la comunicación, en particular dentro de un mensaje enviado en un procedimiento de autenticación, por ejemplo en una primera etapa del mismo. De este modo, puede posibilitarse que el UE esté en conocimiento por lo menos de una "propiedad" del acceso relacionada con la confianza, de manera segura, sin añadir nuevos protocolos o rondas de señalización.

La propiedad puede ser enviada, en particular, dentro de un mensaje de Solicitud EAP/Desafío AKA, dentro de un mensaje de Solicitud EAP/Notificación AKA o dentro de un mensaje de Éxito EAP.

De manera habitual, una representación del método de acceso que se describe en la presente memoria puede comprender uno o varios programas informáticos o rutinas informáticas, es decir, partes de código de programa en general que son legibles por un ordenador, denominado asimismo en la presente memoria un procesador o un procesador electrónico, para llevar a cabo las etapas del procedimiento correspondiente. Las partes de código de programa pueden haber sido escritas, y ser o haber sido leídas desde uno o varios productos de programa informático, es decir, soportes de código de programa, tales como un disco duro, un disco compacto (CD, compact disc), una tarjeta de memoria o un disco flexible. Las partes de código de programa pueden estar almacenadas, por ejemplo, en una memoria de un UE y/o de un servidor o nodo de red, tal como una memoria que sea por ejemplo una memoria flash, una EEPROM (Electrically Erasable Programmable ROM, ROM programable borrable eléctricamente), un disco duro o una ROM (Read-Only Memory, memoria de sólo lectura).

Breve descripción de los dibujos

Los objetivos, ventajas y efectos así como las características de la invención se comprenderán más fácilmente a partir de la siguiente descripción detallada de realizaciones a modo de ejemplo de la invención, cuando se lean junto con los dibujos adjuntos, en los cuales:

- la figura 1a es una vista esquemática de un EPS acorde con la técnica anterior,

- la figura 1b es otra vista esquemática de un EPS que incluye una VPLMN (Visited Public Land Mobile Network, red móvil terrestre publica visitada),

- la figura 2 es un diagrama de señales transmitidas entre nodos involucrados en un procedimiento de autenticación de acuerdo con el EAP,

- la figura 3 es un diagrama de señales transmitidas entre nodos involucrados en un procedimiento de acceso para equipo de usuario,

- la figura 4a es un diagrama de bloques de un equipo de usuario, que muestra unidades o módulos requeridos para recuperar o interpretar información especial en un mensaje recibido y para utilizar la información especial,

- la figura 4b es un diagrama de bloques de equipo de usuario que muestra componentes internos habituales del mismo,

- la figura 4c es un esquema de una unidad de memoria que contiene o lleva código de programas para su utilización por un equipo de usuario,

- la figura 5a es un diagrama de bloques similar a la figura 4a, de un nodo o servidor, que muestra unidades requeridas para recuperar e introducir información especial en un mensaje,

- la figura 5b es un diagrama de bloques similar a la figura 5a, en la que el mensaje es un mensaje incluido en un procedimiento de autenticación,

- la figura 5c es un diagrama de bloques similar a la figura 4b, de un nodo o servidor, que muestra componentes internos habituales del mismo, y

- la figura 5d es un esquema de una unidad de memoria que contiene o lleva código de programa para su utilización por un servidor.

Descripción detallada

Aunque la invención abarca diversas modificaciones y construcciones alternativas, en los dibujos se muestran realizaciones de la invención y en adelante se describirán en detalle. Sin embargo, debe entenderse que la descripción específica y los dibujos no están previstos para limitar la invención a las formas específicas dadas a conocer.

A continuación se describirá un procedimiento que involucra un UE que accederá a una red local. En particular, se describirá cómo un UE establece conectividad de red. El objetivo puede ser, por ejemplo, que el UE desea una conexión a través de una red local, a una parte tal como un cliente o un servidor, no mostrado, conectado a la red local o a un servicio accesible a través de la red local. Sin embargo, el procedimiento que se describe en la presente memoria trata sólo del establecimiento de conectividad de red, y cómo o con qué propósito se vaya a utilizar la conectividad no forma parte del procedimiento. En la figura 1b se muestran esquemáticamente los componentes más importantes involucrados. Un UE 1, en general un terminal, por ejemplo un teléfono móvil o una estación móvil, establecerá una conexión a través de una red de acceso no-3GPP que es, considerada por una red local HPLMN 5, una red de confianza tal como la que se muestra en 3 o bien una red no de confianza tal como la que se muestra en 3'. Además, en el caso mostrado el UE 1 está asimismo itinerando, es decir, accederá a través de la red de acceso respectiva a su HPLMN a través de una VPLMN 7. Se asume que la HPLMN y la VPLMN funcional de acuerdo con el estándar EPS. Asimismo, se asume que el UE 1 tiene medios para funcionar de acuerdo con el mismo estándar.

Puede asumirse que el UE 1, asociado con la red local 5, que está estableciendo conectividad utilizando el estándar EPS mediante una red de acceso no-3GPP tiene un USIM (Universal Subscriber Identity Module, módulo de identidad de abonado universal), no mostrado. Incluso si no se requiere el USIM para la autenticación de acceso, habitualmente éste es necesario para establecer una conexión IPsec segura a una ePDG 9 en la VPLMN 7 y/o para establecer señalización de movilidad segura, por ejemplo, MIP.

El UE 1 inicia el establecimiento de conectividad mediante poner en marcha un procedimiento de establecimiento. En primer lugar envía un mensaje o señal de solicitud, solicitando una conectividad a una red de acceso no-3GPP 3, 3', ver asimismo el diagrama de señal de la figura 3 donde se muestran etapas del procedimiento de establecimiento para el acceso. La solicitud puede contener uno o varios identificadores específicos de acceso básico/físico para el UE 1, por ejemplo una dirección MAC (control de acceso al medio), etc. Un nodo de acceso (AN, access node) 11 en la red de acceso respectiva recibe el mensaje o señal de solicitud, lo analiza y responde, por ejemplo, iniciando un proceso de intercambio de identidad de UE, siendo ésta, por ejemplo, la primera etapa de un procedimiento de autenticación acorde, por ejemplo, con el EAP. La identidad es habitualmente una identidad lógica que puede incluir información acerca de la red local del UE 1, y normalmente no está vinculada a una tecnología de acceso específica. En dicho procedimiento de intercambio de identidad del UE, el AN 11 en la red de acceso 3, 3' respectiva envía en primer lugar un mensaje Solicitar identidad EAP al UE 1, ver el diagrama de señales más detallado de la figura 2. El UE 1 recibe el mensaje Solicitar identidad EAP y envía en respuesta mismo un mensaje Responder identidad EAP, que contiene información sobre la identidad del UE y es recibido por el AN 11 en la red de acceso respectiva. El AN identifica el mensaje Responder identidad EAP y lo transfiere a un servidor 13 respectivo en la HPLMN 5 para el UE 1 o en asociación con el mismo, teniendo lugar la transferencia a través de la VPLMN 7 para el caso mostrado la figura 1b. Si bien la autenticación/señalización EAP entre el UE 1 y el AN 11 se lleva a cabo sobre un protocolo específico de acceso, por ejemplo 802.1x, la autenticación/transferencia EAP al servidor 13 se lleva a cabo habitualmente sobre un protocolo AAA basado en IP, tal como Diameter o Radius. El AN 11 puede por lo tanto añadir elementos de información adicionales cuando transmite el mensaje EAP sobre el protocolo AAA, por ejemplo un identificador de la red de acceso 3, 3' y/o del AN 11. A partir de este mensaje Responder identidad EAP, cuando es recibido por el servidor en la HPLMN, el servidor puede obtener o deducir la identidad de la red de acceso 3, 3' a través de la cual fue transmitido el mensaje, por ejemplo mediante identificadores de red contenidos en el protocolo AAA. El servidor 13 en la HPLMN 5 puede ser un servidor AAA o un HSS.

A continuación comienza el propio procedimiento de autenticación, y éste puede llevarse a cabo asimismo, por ejemplo, de acuerdo con el EAP. En el procedimiento de autenticación se envían mensajes apropiados entre el servidor 13 y el UE 1, siendo estos mensajes transmitidos sustancialmente sin cambios a través de la red de acceso 3, 3' respectiva, atravesando el AN 11 y la VPLMN 7. Por lo tanto, excepto en la realización de conversión entre el protocolo AAA y el protocolo de señalización específico de acceso, habitualmente el AN 11 solamente transmite todos estos mensajes entre el UE y el servidor.

Tal como se ve en la figura 2, estos mensajes asociados con el procedimiento de autenticación pueden incluir, secuencialmente en el tiempo, un mensaje de Solicitar EAP Desafío AKA enviado desde el servidor, un mensaje Responder EAP Desafío AKA enviado desde el UE, un mensaje Solicitar EAP Notificación AKA enviado desde el servidor, un mensaje Solicitar EAP Notificación AKA enviado desde el UE y un mensaje Éxito EAP enviado desde el servidor, asumiendo que la autenticación es satisfactoria.

En este punto, puede asignarse al UE en una dirección IP local mediante la red de acceso. Sin embargo, el UE puede seguir siendo inaccesible y puede tener que adoptar etapas adicionales para establecer conectividad con otras partes. Específicamente, el UE puede tener que establecer conectividad con un nodo pasarela, por ejemplo la mencionada ePDG 9 utilizada en los accesos no fiables. El nodo en cuestión podría ser adicional/alternativamente

un nodo que proporcione soporte de movilidad, por ejemplo un agente local (HA, Home Agent) MIP. Esto proporciona la seguridad y/o la accesibilidad "global" necesarias para el UE.

Por lo tanto, después de que se ha completado satisfactoriamente un procedimiento de autenticación puede llevarse a cabo un cuarto procedimiento, que incluye etapas específicas para la red de acceso y el establecimiento de una conexión IP general para el UE 1. Esto completa el establecimiento de la conectividad. En adelante, el UE estará capacitado para recibir/enviar datos, por ejemplo iniciar sesiones de comunicación con otras partes. La comunicación de datos entre el UE y alguna otra parte puede tener lugar por lo tanto en un quinto procedimiento que está fuera del procedimiento que se describe en la presente memoria.

Uno de los mensajes enviados desde el servidor 13 en el procedimiento de autenticación puede modificarse para contener información especial o para indicar una condición especial. La información especial o la condición especial pueden referirse a una propiedad o a características de la red de acceso 3, 3' utilizada. En particular, puede indicar si la red de acceso es de confianza o no de confianza, considerada desde la HPLMN 5.

El UE 1 está adaptado para recuperar la información especial desde, o interpretar la condición especial indicada en el mensaje, y utilizarla, o su interpretación, respectivamente, en el establecimiento de una conexión a través de la red de acceso 3, 3' respectiva.

Para llevar a cabo el procedimiento descrito anteriormente, el servidor 13 se modifica de manera que pueda reunir e introducir la información especial en un mensaje escogido o modificar el mensaje escogido haciendo que indique la condición especial, recuperando información pertinente, por ejemplo a partir de una lista o una base de datos en el servidor o conectada al mismo. La lista o base de datos puede incluir, por ejemplo, por lo menos todas las redes de acceso de confianza. Por supuesto, si es necesario a lista o base de datos puede incluir asimismo redes no de confianza. La búsqueda en esta lista o base de datos puede basarse en el identificador de red de acceso recibido como parte del procedimiento realizado de acuerdo con el protocolo AAA que se ha descrito anteriormente. La lista o base de datos puede ser actualizada continuamente. Debido, por ejemplo, a un nuevo acuerdo comercial, una red anteriormente no de confianza puede "actualizarse" para pasar a ser de confianza y viceversa.

Por lo tanto, en general, siempre que se utilice el EAP (AKA) en el procedimiento de acceso, puede incluirse en la señalización EAP una indicación procedente, por ejemplo del servidor 13 en la forma de un servidor AAA en la red local 5, al UE 1 sobre las "propiedades" de la red de acceso 3, 3' respectiva. Una característica útil del EAP (AKA) es que puede ser segura extremo a extremo (e2e) entre el servidor y el UE, protegiendo de este modo la propiedad/propiedades de red incluidas, por ejemplo frente a un fraude de terceras partes. Sin embargo, la indicación podría incluirse asimismo en la señalización de otros protocolos de autenticación cuando no se utiliza el EAP (AKA).

Para poder llevar a cabo estas tareas, es necesario modificar el UE 1 para incluir funciones realizadas por unidades o módulos, tal como se muestra en la figura 4a. Por lo tanto, es necesario disponer de una unidad o módulo 15 para recuperar información especial a partir de uno o varios mensajes o para interpretar una condición especial indicada en uno o varios mensajes. Podría existir una unidad o módulo 16 para almacenar la información especial o información acerca de la condición especial, respectivamente, en una celda de memoria 17 en el UE 1. Finalmente, el UE puede incluir una unidad o módulo 19 para utilizar la información especial recibida y/o almacenada o la información acerca de la condición especial, respectivamente, tal como para seleccionar un modo apropiado o adecuado de establecer una conexión a través de una red de acceso. Tal como es usual, puede considerarse que cada una de estas unidades o módulos comprende un procesador y uno o varios segmentos correspondientes de código del programa.

En general, el UE 1 puede tener una estructura sustancialmente convencional e incluir componentes internos organizados, por ejemplo, tal como se muestra esquemáticamente en el diagrama de bloques de la figura 4b. Puede incluir por lo tanto un procesador 21, una memoria 23, circuitos de comunicación radioeléctrica 25, circuitos 27 para controlar la pantalla, no mostrada, circuitos 29 para teclado, no mostrado, circuitos de salida de audio 31 y circuitos de entrada de audio 32. La memoria 23 puede ser una memoria electrónica tal como una memoria flash, una EEPROM (memoria de sólo lectura programable borrable eléctricamente), un disco duro o una ROM (memoria de solo lectura) y puede comprender una o varias unidades físicas independientes. El procesador controla el funcionamiento del UE 1 mediante la ejecución de código de programa almacenado en la parte de memoria del programa 33 de la memoria. El procesador 21 puede utilizar datos almacenados, por ejemplo, en la parte de memoria de datos 35 de la memoria 23.

En la memoria de programa 33 está almacenado el código de programa que tiene diferentes rutinas o partes para los diversos procedimientos ejecutados por el procesador 21. Por lo tanto, la parte del código de programa para los servicios de telefonía básica está almacenada en un segmento de memoria 37, incluyendo dichos servicios el establecimiento y la utilización de conexiones de audio con otros UE. Existe asimismo código de programa almacenado en un segmento de memoria 39 para procedimientos que involucran el intercambio de datos, tal como para el establecimiento de una conexión IP. Este segmento de memoria de programa puede incluir por lo tanto partes de memoria en las que están almacenadas partes de código de programa para los procedimientos mostrados en las figuras 2 y 3. Estas partes de memoria comprenden por lo tanto código de programa que puede ser leído por

el procesador 21 y que, cuando es leído por el procesador, hace que el UE lleve a cabo los procedimientos correspondientes. Puede existir una parte de memoria 41 para almacenar código de programa para una conexión básica establecida, una parte de memoria 43 para almacenar código de programa para intercambio de identidad del UE, una parte de memoria 45 para almacenar código de programa para un procedimiento de autenticación, y una parte de memoria 47 para almacenar código de programa para establecimiento de conexión IP y específica de acceso. En la memoria de programa 33 puede existir además un segmento de memoria 49 para almacenar código de programa para conectividad IP/servicio, por ejemplo partes de código de programa para manejar movilidad IP (MIP), multiproveedor ("multihoming"), seguridad IP (IKE/IPsec), etc.

En la parte de memoria 45 para almacenar el código de programa para un procedimiento de autenticación puede estar dispuesto espacio de memoria 51 para almacenar código de programa para recuperar información especial a partir de, o interpretando una condición especial indicada en un mensaje recibido en el procedimiento de autenticación. Dicha condición o información especial puede estar relacionada, tal como se ha mencionado anteriormente, por ejemplo, por lo menos con una propiedad de la red asociada con el establecimiento de conectividad para una conexión para intercambio de datos, tal como una propiedad de una red de acceso 3, 3' utilizada. La información especial o información acerca de la condición especial puede estar almacenada en una celda de memoria 53 en la memoria 23 y puede utilizarse, por ejemplo, en el establecimiento de conexión IP y específica de acceso, para el que el código de programa está almacenado en la parte de memoria de programa 49. La parte de código de programa para esta utilización puede estar almacenada en un espacio de memoria 55 en el interior de dicha parte de memoria.

Las partes de código de programa pueden haber sido escritas y pueden ser o haber sido leídas desde uno o varios productos de programa informático, es decir soportes de código de programa, tales como un disco duro, un disco compacto (CD), una tarjeta de memoria o un disco flexible. Dicho producto de programa informático es, en general, una unidad de memoria 33' que puede ser portátil o estacionaria y se muestra en el esquema de la figura 4c. Puede tener segmentos de memoria, celdas de memoria y espacios de memoria dispuestos sustancialmente tal como en la memoria de programa 33 del UE 1, o el código de programa puede estar, por ejemplo, comprimido de cualquier modo adecuado. En general, la unidad de memoria 33' comprende por lo tanto código legible por ordenador, es decir código que puede ser leído por un procesador electrónico, el cual cuando es ejecutado por un UE 1 hace que el UE lleve a cabo etapas para ejecutar uno o varios de los procedimientos que realiza el UE de acuerdo con la descripción anterior. El código de programa contenido en la unidad de memoria 33' puede ser introducido en la memoria 23 del UE mediante cualquier método adecuado, tal como por descarga desde un servidor, no mostrado, que contiene la unidad de memoria o está conectado a la misma. En otra realización, la unidad de memoria 33' puede utilizarse directamente como parte de la memoria 33 del UE 1.

Del mismo modo que para el UE 1, para poder llevar a cabo el procedimiento descrito anteriormente, el servidor 13 debe ser modificado para incluir, tal como se muestra en la figura 5a, una unidad o módulo 61 para reunir o encontrar información especial o información relativa a una condición especial. Esta unidad o módulo pueden extraer, por ejemplo, dicha información desde una celda de memoria 63 en el servidor o conectada con el servidor 13. Otra unidad o módulo 65 puede introducir la información especial en uno o varios mensajes escogidos, o modificar uno o varios mensajes para indicar la condición especial. Tal como se ve en la figura 5b, el servidor 13 puede, por el ejemplo descrito anteriormente, ser modificado para incluir una unidad o un módulo 67 para obtener o deducir qué red de acceso se utiliza por un abonado para el que existe alguna comunicación en curso entre el UE 1 de abonado y el servidor. Entonces, el servidor puede incluir asimismo una unidad o módulo 69 para reunir o encontrar información relativa a una propiedad o características de la red de acceso utilizada. Esta unidad o módulo puede recuperar dicha información de una base de datos o listas de redes, incluyendo la base de datos o lista, por ejemplo, información especial para una serie de redes, y estando almacenada en una posición de memoria 71. Otra unidad o módulo 73 puede introducir información relativa a una propiedad o característica en un mensaje enviado a un abonado durante un procedimiento de autenticación.

El servidor 13 puede implementarse como un ordenador, un grupo de ordenadores o una parte de un ordenador adecuada para conexión a una red. De este modo, tal como se ve en la figura 5c, éste puede comprender tal como es habitual un procesador 77, una memoria 79 y un puerto de red 81. La memoria 79 puede ser una memoria electrónica tal como una memoria flash, una memoria EEPROM, una EPROM (memoria de sólo lectura programable borrable), un disco duro o una ROM. La memoria puede tener espacios 83, 85 para código de programa y datos, respectivamente. En la memoria de programa está almacenado una parte de código de programa en un segmento de memoria 87 para llevar a cabo un procedimiento de autenticación, por ejemplo de acuerdo con el EAP que se ha descrito anteriormente. En el espacio de memoria de datos 85 están almacenados datos de abonado desde una posición de memoria 89 y están almacenados datos sobre redes de acceso en una posición de memoria 91. Los datos sobre redes de acceso pueden comprender un registro para cada red de acceso y en cada registro puede haber, en particular, un campo en el que hay almacenada información que indica si el acceso es de confianza o no de confianza. En el segmento de memoria 87 en el que está almacenada la parte del código de programa para el procedimiento de autenticación, existen partes de memoria 93, 95, 97 en las que están almacenadas partes de código de programa para obtener o deducir la identidad de la red de acceso utilizada, para reunir o encontrar información relativa a una característica o propiedad especial de la red de acceso y para introducir la información reunida o encontrada en un mensaje de autenticación, es decir en uno de los mensajes enviados al UE de abonado durante el procedimiento de autenticación, respectivamente.

Las partes del código de programa pueden haber sido escritas en, y pueden leerse o haber sido leídas desde uno o varios productos de programa informático, es decir soportes de código de programa, tales como un disco duro, un disco compacto (CD), una tarjeta de memoria o un disco flexible. Dicho producto de programa informático es generalmente una unidad de memoria 83' que puede ser portátil o estacionaria, tal como se muestra en el esquema de la figura 5d. Puede tener segmentos de memoria, celdas de memoria y espacios de memoria dispuestos sustancialmente tal como la memoria de programa 83 del servidor 13. El código de programa, por ejemplo, puede ser comprimido de manera adecuada. En general, la unidad de memoria 83' comprende de este modo código legible por ordenador, es decir código que puede ser leído por un procesador electrónico tal como 77, que cuando es ejecutado por un servidor 13 hace que el servidor lleve a cabo etapas para ejecutar uno o varios procedimientos o etapas procedimentales que lleva a cabo el servidor de acuerdo con la descripción anterior. El código de programa contenido en la unidad de memoria 83' puede ser introducido en la memoria 23 del UE mediante cualquier método adecuado, tal como por descarga desde un servidor, no mostrado, que comprende la unidad de memoria o está conectado a la misma. Si es adecuado, la unidad de memoria 83' puede utilizarse directamente como parte de la memoria 83 de servidor 13.

Se ha mencionado anteriormente que, por ejemplo, se utiliza el EAP en el establecimiento de la conexión. Tal como se ha mencionado, en el caso de un acceso no de confianza, esto no puede darse por hecho y por lo tanto es necesario tratar un caso general. El siguiente procedimiento más general puede utilizarse para un acceso en un sistema que incluye una red local 3GPP 5 y una red acceso no-3GPP 3, 3' y en el que el EAP puede o no ser utilizado:

1. El UE 1 solicita acceso.

2. Tiene lugar un intercambio de identidad básica.

3. Si la red de acceso 3, 3' respectiva no inicia la autenticación de acceso de acuerdo con el EAP, en la mayor parte de los casos el UE 1 puede asumir que la red de acceso no es de confianza. Será necesario un túnel a una ePDG 9, por ejemplo creado utilizando un procedimiento llevado a cabo de acuerdo con el IPsec. Si se desea, puede disponerse un temporizador para comprobar si el procedimiento de autenticación de acceso EAP ha sido iniciado dentro de un tiempo predeterminado. En otra alternativa, se determina mediante el UE vez que no habrá iniciación de comunicación EAP si se proporciona una dirección IP para conexión al UE 1 desde la respectiva red de acceso 3, 3', tal como, por ejemplo, mediante un DHCP (Dynamic Host Configuration Protocol, protocolo de configuración dinámica de anfitrión), no mostrado. Específicamente, si se utilizara autenticación EAP, ésta habría tenido lugar antes de la asignación de dirección IP.

4. De lo contrario, si la red de acceso 3, 3' respectiva no inicia la autenticación de acceso EAP, la red de acceso podría ser de confianza o no de confianza.

5. Para el caso de la etapa 2, el servidor AAA local 13, que sabe si el acceso es o no de confianza, incluye un parámetro en un mensaje EAP que informa de esto al UE 1. Tal como se ha mencionado anteriormente, este parámetro puede ser seguro e2e, es decir cifrado y/o de integridad protegida, entre el servidor AAA local y el UE.

6. El UE 1 verifica la autenticidad de la indicación y actúa en consecuencia, por ejemplo intenta o no establecer un túnel IPsec con una ePDG 9, etc. En caso de que no intente establecer un túnel IPsec, en su lugar intentará, por ejemplo, establecer un canal de comunicación IP normal no protegido.

7. Se llevan a cabo otros procedimientos que forman parte del establecimiento de conectividad, por ejemplo configuración de movilidad IP, etc., que pueden depender asimismo de la indicación anterior.

8. A continuación, el UE puede comunicar y/o utilizar otros servicios.

Los mensajes número 1, 2 y 3, cuyos títulos están escritos en cursiva en la figura 2 pueden utilizarse, tal como se ha mencionado anteriormente, para la indicación de información especial, por ejemplo conteniendo un "atributo de propiedad de acceso" o "atributos de propiedad de acceso". Por ejemplo, el mensaje de Desafío AKA puede contener seudónimos EAP (protegidos), y podría extenderse para incluir otros atributos, en este caso relativos a propiedades de la red de acceso. Debe observarse que los mensajes número 1 y número 2 son mensajes específicos de método AKA, mientras que el mensaje del Éxito AKA número 3 no es un mensaje específico de método AKA. Actualmente, está siendo definida una versión de EAP AKA, indicada EAP AKA', en el IETF a (Internet Engineering Task Force, grupo de trabajo de ingeniería de internet). Los mensajes específicos descritos anteriormente que son adecuados para transportar la propiedad existen asimismo en EAP AKA' y, por lo tanto, pueden utilizarse de manera similar.

De este modo, el "algoritmo" ejecutado en el UE 1 para determinar la confianza (u otras propiedades) de la red de acceso se realizaría de acuerdo con el siguiente código lógico general:

Si la red de acceso no utiliza EAP entonces

"acceso no de confianza" /*por ejemplo, se requiere establecer túnel IPsec*/

si no

ejecutar EAP (tal como se ha descrito anteriormente)

obtener valor de confianza y posiblemente otras propiedades de red a partir de la señalización EAP

ejecutar uno o varios procedimientos (seguridad/mobilidad/…) de acuerdo con el valor de confianza extraído y posiblemente propiedades de red/otras

fin si

Sin embargo, existe un problema asociado con este algoritmo. Antes de cualquier posible ejecución del EAP, el UE 1 realizará algún "contacto con la red" básico, es decir realizará alguna primera operación señalizando que desea conectar a la red de acceso respectiva. ¿Cuánto debería "esperar" después este contacto el UE para el EAP? Por ejemplo, el UE 1 podría asumir que después de esperar 2 segundos no se realizará un procedimiento de autenticación de acuerdo con el EAP, pero quizás se habría realizado si el UE hubiera esperado un segundo más.

Sin embargo, dado que en este caso el objetivo es proporcionar acceso IP para el UE 1, y puesto que el UE tiene que haber sido asignado a una dirección IP para poder establecer el IPsec, esto implica que una vez que el UE ha sido asignado a la dirección IP, el UE puede asumir que si no se ha ejecutado un procedimiento de acuerdo con el EAP antes de la asignación de dirección IP, por ejemplo mediante el DHCP, no se ejecutará ningún procedimiento en absoluto de acuerdo con el EAP para conseguir autenticación de acceso, compárese con la etapa 1 anterior.

En el caso especial de utilización de un procedimiento acorde con el AKA (EAP), la señalización podría realizarse en el campo "AMF" (Authentication Management Field, campo de gestión de autenticación), no mostrado. Este campo es una parte nativa del AKA y es transportado en el mensaje de Solicitud EAP/Desafío AKA, véase la figura 2, mensaje número 1, totalmente transparente para la capa EAP.

Si la propiedad de "confianza" tiene que ser decidida conjuntamente por la red local, es decir la red local (por ejemplo servidor AAA) y la red de acceso 3, 3' utilizada, el método y sistema descritos en la presente memoria podrían utilizarse junto con el proceso dado a conocer en la solicitud de patente internacional PCT/SE2008/050063. En dicha solicitud de patente internacional se da a conocer cómo cada una de la red local y la red de acceso comunican una "política de seguridad" dentro de la señalización de autenticación al UE. El UE 1 puede combinar las dos políticas en una "política de mínimo denominador común". En este caso, la diferencia es que en la citada solicitud de patente internacional se asume que ya se conoce qué protocolos utilizar, pero no qué políticas aplican a los mismos.

Deberá entenderse que aunque la realización descrita anteriormente comprende, por ejemplo, un servidor AAA 13 en la red local en forma de una red central conectada "detrás" de una red de acceso 3, 3', tal como se ve desde el UE 1, cualquier nodo adaptado en consecuencia para enviar Solicitudes EAP de manera similar a las realizaciones descritas anteriormente podría sin embargo conectarse en la red de acceso, por ejemplo un servidor de autenticación 14 conectado en la VPLMN 7 de la figura 1b.

Además, o en lugar de cualesquiera propiedades que indican si una red de acceso 3, 3' es o no de confianza, podrían señalizarse otras propiedades desde un servidor tal como 13, 14 al terminal o al UE 1, por ejemplo qué protocolos utilizar, ancho de banda, coste y servicios, para decidir qué acceso/modo de comunicaciones/señalización deberá ser seleccionado por el terminal.

Como alternativa a los elementos de información adicionales en una solicitud EAP, la señalización podría realizarse "incorporada" en elementos de información EAP AKA existentes. Por ejemplo, el servidor AAA local 13 podría enviar al UE EAP seudónimos que tienen su bit más significativo configurado a "1" para acceso de confianza y a "0" para acceso no de confianza, etc.

Aunque las realizaciones descritas anteriormente utilizan el EAP, otras realizaciones del método y sistema descritos en la presente memoria pueden utilizar algún protocolo no EAP en un procedimiento para establecer una conexión, en particular en una primera etapa o etapa inicial de dicho procedimiento, tal como en un procedimiento de autenticación, por ejemplo el PPP (Point-to-Point Protocol, protocolo punto a punto), el PAP (Password Authentication Protocol, protocolo de autenticación de contraseña), el CHAP (Challenge Handshake Authentication Protocol, protocolo de autenticación por desafío mutuo) y el SPAP (Shiva Password Authentication Protocol, protocolo de autenticación de contraseña de Shiva).

REIVINDICACIONES

1. Un método llevado a cabo por un equipo de usuario (1) para una comunicación a través una red de acceso (3, 3'), que comprende:

- recuperar información a partir de, o para interpretar una condición especial indicada en un mensaje enviado al equipo de usuario (1) desde un servidor AAA en una red local de equipo de usuario (1), en un procedimiento de autenticación que forma parte del establecimiento de una conexión desde el equipo de usuario (1) a través de la red de acceso (3, 3'), haciendo referencia la condición especial a si la red de acceso (3, 3') es o no de confianza, y

- utilizar, en una etapa siguiente del procedimiento de establecimiento de la conexión, la información recuperada o el resultado de la interpretación de la condición especial, para seleccionar un modo apropiado de establecer la conectividad a través de la red de acceso (3, 3').

2. Un método según la reivindicación 1, **caracterizado por que** el procedimiento de autenticación está basado en el EAP y por que dicho mensaje es un mensaje EAP enviado desde el servidor AAA.

3. Un método según la reivindicación 1, **caracterizado por que** el procedimiento de autenticación está basado en el EAP.

4. Un método según la reivindicación 3, **caracterizado por que** el procedimiento de autenticación está basado en el EAP AKA.

5. Un método según la reivindicación 4, **caracterizado por que** el mensaje es una señal de Solicitud EAP/Desafío AKA, una señal de Solicitud EAP/Notificación AKA o una señal de Éxito EAP.

6. Un método según la reivindicación 1, en el que la conectividad a establecer es una conexión IP, que incluye la etapa adicional de:

- asignar una dirección IP al equipo de usuario (1),

caracterizado por que en un procedimiento de establecimiento, si el equipo de usuario (1) ha sido asignado a una dirección IP antes de un posible inicio de un procedimiento de autenticación llevado a cabo de acuerdo con el EAP, se establece un túnel IPsec a una pasarela en la red local o una red relacionada con la misma, y si un comienzo de un procedimiento de autenticación llevado a cabo de acuerdo con el procedimiento EAP se produce antes de que el equipo de usuario (1) haya sido asignado a una dirección IP, se establece entonces un túnel IPsec si la red de acceso (3, 3') se señaliza como no de confianza o no se establece un túnel IPsec y se establece un canal normal de comunicación si la red de acceso (3, 3') se señaliza como de confianza.

7. Un equipo de usuario (1) para una comunicación a través de una red de acceso (3, 3'), que comprende:

- una unidad para recuperar (15) información especial desde, o para interpretar una condición especial indicada en un mensaje enviado al equipo de usuario (1) desde un servidor AAA en una red local al equipo de usuario, en un procedimiento de autenticación que forma parte del establecimiento de una conexión desde el equipo de usuario a través de la red de acceso (3, 3'), haciendo referencia la condición especial a si la red de acceso (3, 3') es o no de confianza, y

- una unidad para utilizar (19), en una etapa siguiente del procedimiento de establecimiento de la conexión, la información recuperada o el resultado de la interpretación de la condición especial para seleccionar un modo apropiado de establecer la conectividad a través de la red de acceso (3, 3').

8. Un equipo de usuario (1) según la reivindicación 7, **caracterizado por que**

- la unidad para utilizar (19) está dispuesta para establecer un túnel de seguridad para comunicación si la información recuperada indica que la red de acceso (3, 3') no es de confianza y para establecer un canal normal de comunicación si la información recuperada indica que la red de acceso (3, 3') es de confianza.

9. Un equipo de usuario (1) según la reivindicación 7 ú 8, **caracterizado por que** el procedimiento de autenticación está basado en EAP.

10. Un equipo de usuario (1) según la reivindicación 9, **caracterizado por que** el procedimiento de autenticación está basado en EAP AKA.

11. Un equipo de usuario (1) según la reivindicación 10, **caracterizado por que** dicho mensaje es una señal de Solicitud EAP/Desafío AKA, una señal de Solicitud EAP/Notificación AKA o una señal de Éxito EAP.

12. Un servidor AAA en una red local de un equipo de usuario (1), estando dispuesto el servidor AAA para enviar información al equipo de usuario (1) en un procedimiento de autenticación que forma parte del establecimiento de conectividad desde el equipo de usuario a través de una red de acceso (3, 3'), en el que el servidor AAA está

dispuesto para introducir, en un mensaje incluido en dicha información enviada al equipo de usuario (1), información especial que indica una condición especial que hace referencia a si la red de acceso (3, 3') es o no de confianza, o modificar dicho mensaje a efectos de indicar la condición especial.

13. Un servidor AAA según la reivindicación 12, **caracterizado por que** el servidor AAA está dispuesto para introducir la información especial en el mensaje EAP.

14. Un servidor AAA según la reivindicación 13, **caracterizado por que** el mensaje EAP es una señal de Solicitud EAP/Desafío AKA, una señal de Solicitud EAP/Notificación AKA o una señal de Éxito EAP.

15. Un producto de programa informático comprendido en, o para su utilización por un equipo de usuario (1) relacionado con un servidor AAA en una red local del equipo de usuario, estando el producto de programa informático en una memoria y comprendiendo medios de código legible por ordenador que cuando son ejecutados por el equipo de usuario (1) hacen que el equipo de usuario (1)

– recupere información especial desde, o para interpretar una condición especial indicada en un mensaje enviado al equipo de usuario (1) desde el servidor AAA con el que está relacionado el equipo de usuario (1), en un procedimiento de autenticación que forma parte del establecimiento de una conexión desde el equipo de usuario (1) a través de una red de acceso (3, 3'), haciendo referencia la condición especial a si la red de acceso (3, 3') es o no de confianza, y

- utilice, en una etapa siguiente del procedimiento de establecimiento de la conexión, la información recuperada o el resultado de la interpretación de la condición especial, para seleccionar un modo apropiado de establecer la conectividad a través de la red de acceso (3, 3').

16. Un producto de programa informático, comprendido en, o para utilizar por un servidor AAA relacionado con equipos de usuario, siendo el producto de programa informático una memoria y comprendiendo medios de código legible por ordenador que, cuando son ejecutados por el servidor AAA hacen que el servidor AAA introduzca, en un mensaje incluido en información enviada a uno de los equipos de usuario relacionados con el servidor AAA, información especial que indica una condición especial relativa a si es o no de confianza la red de acceso (3, 3'), a través de la cual debe de establecerse una conexión de dicho equipo de usuario (1), o modifique dicho mensaje para indicar la condición especial.

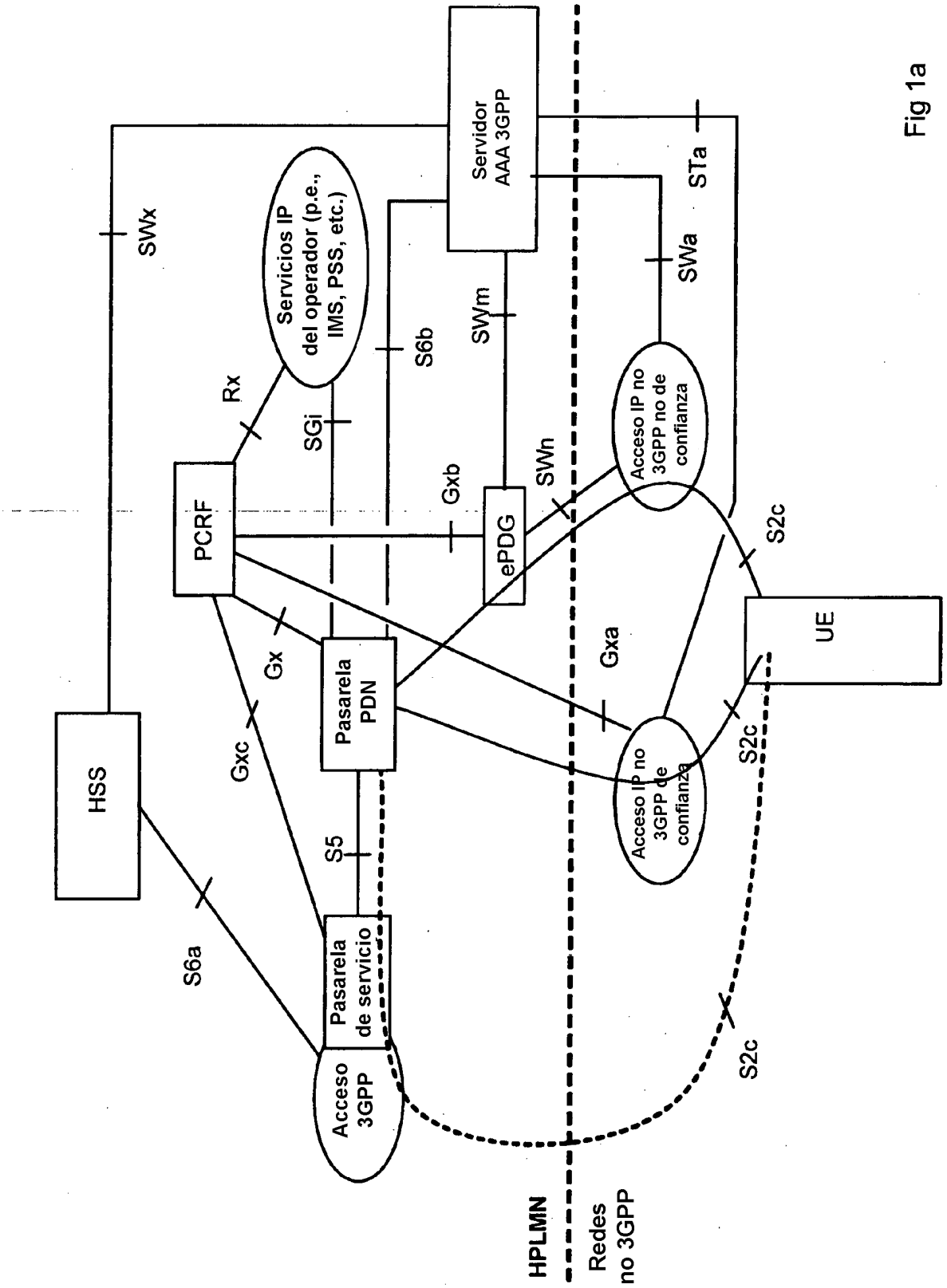
Servidor AAA 3GPP
Servicios IP del operador (p.e., IMS, PSS, etc.)
SWx
STa
SWa
SWm
S6b
Rx
SGi
Gxb
SWn
PCRF
ePDG
Acceso IP no 3GPP no de confianza
S2c
UE
Gx
Gxa
Pasarela PDN
HSS
Gxc
S5
S2c
Acceso IP no 3GPP de confianza
S6a
Pasarela de servicio
Acceso 3GPP
S2c
HPLMN
Redes no 3GPP

Fig 1a

Fig. 1b

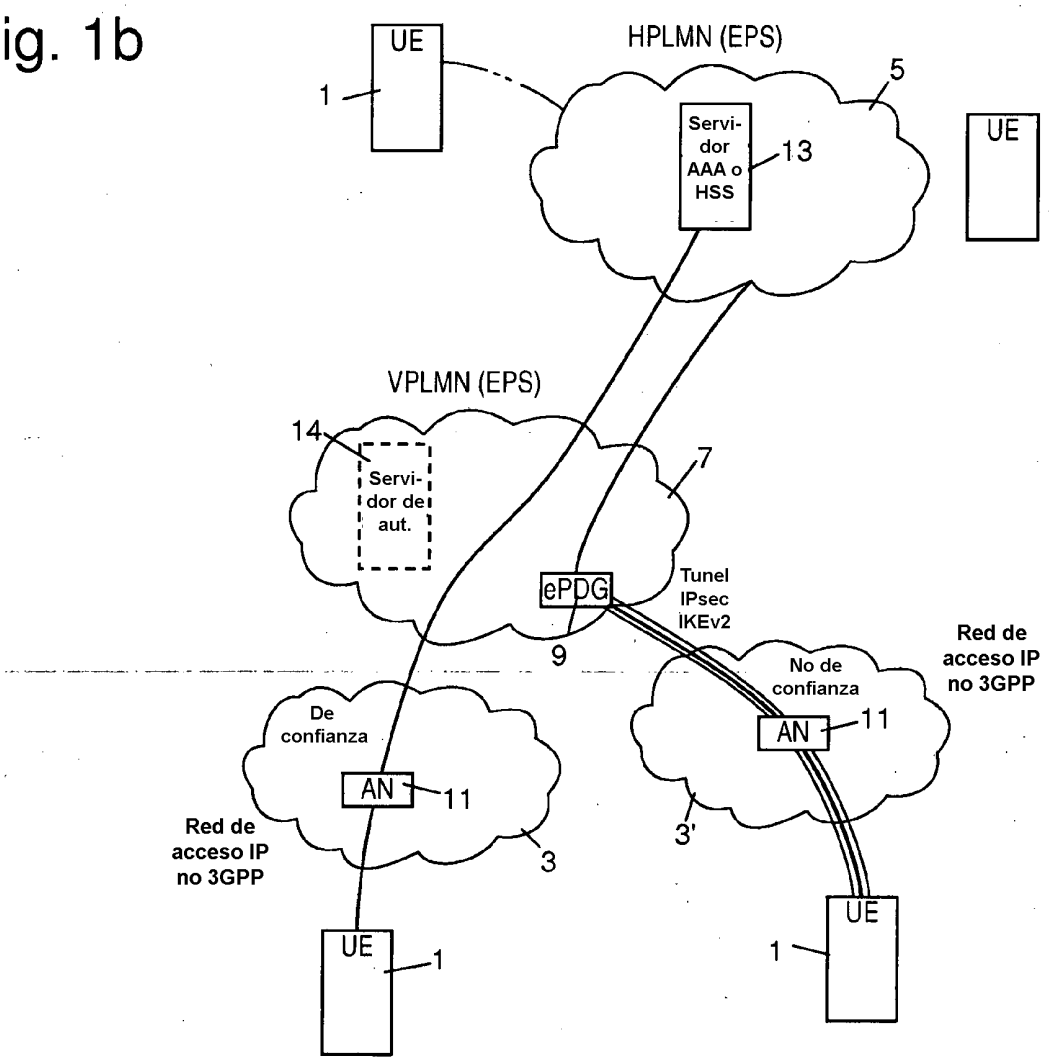
UE
1
HPLMN (EPS)
5
Servi-
dor
AAA o
HSS
13
UE
VPLMN (EPS)
14
Servi-
dor de
aut.
7
ePDG
Tunel
IPsec
IKEv2
9
Red de
acceso IP
no 3GPP
No de
confianza
AN
11
3'
De
confianza
AN
11
Red de
acceso IP
no 3GPP
3
UE
1
UE
1

Fig. 2

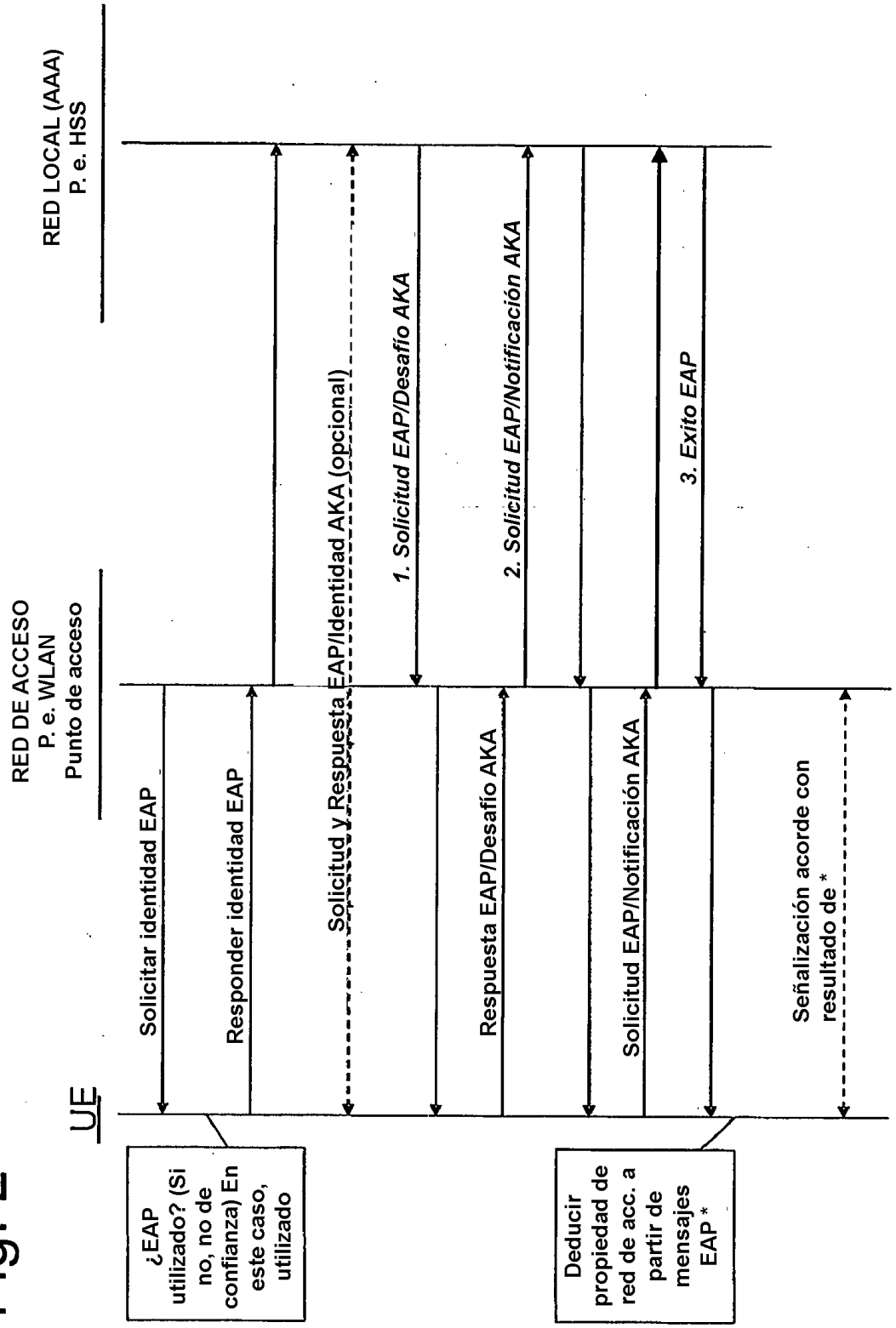
UE
RED DE ACCESO
P. e. WLAN
Punto de acceso
RED LOCAL (AAA)
P. e. HSS
Solicitar identidad EAP
Responder identidad EAP
Solicitud y Respuesta EAP/Identidad AKA (opcional)
1. Solicitud EAP/Desafío AKA
Respuesta EAP/Desafío AKA
2. Solicitud EAP/Notificación AKA
Solicitud EAP/Notificación AKA
3. Éxito EAP
Señalización acorde con resultado de *
¿EAP utilizado? (Si no, no de confianza) En este caso, utilizado
Deducir propiedad de red de acc. a partir de mensajes EAP *

Fig. 3

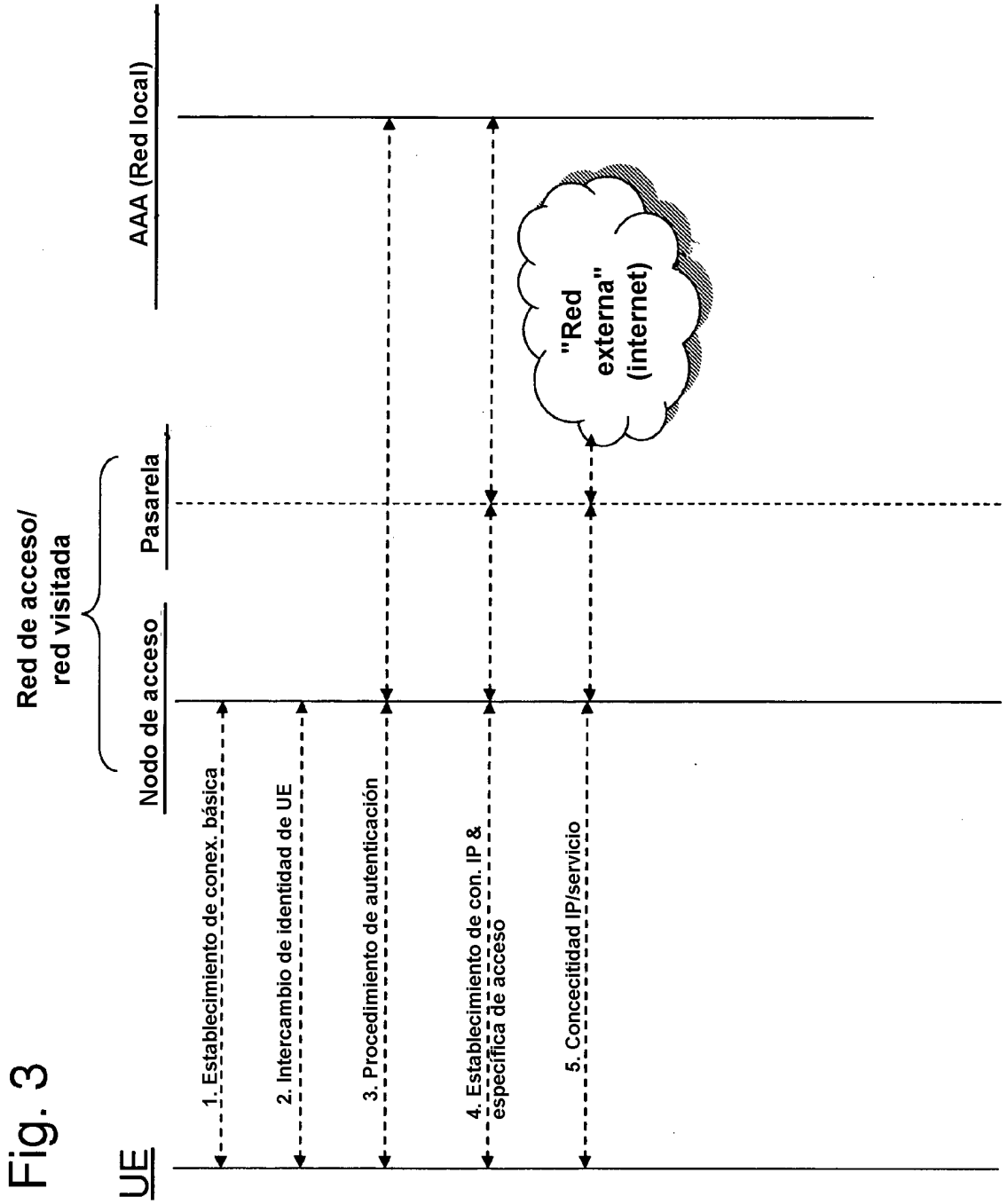
UE
Nodo de acceso
Pasarela
Red de acceso/
red visitada
AAA (Red local)
"Red
externa"
(internet)
1. Establecimiento de conex. básica
2. Intercambio de identidad de UE
3. Procedimiento de autenticación
4. Establecimiento de con. IP &
específica de acceso
5. Concecitidad IP/servicio

Fig. 4a

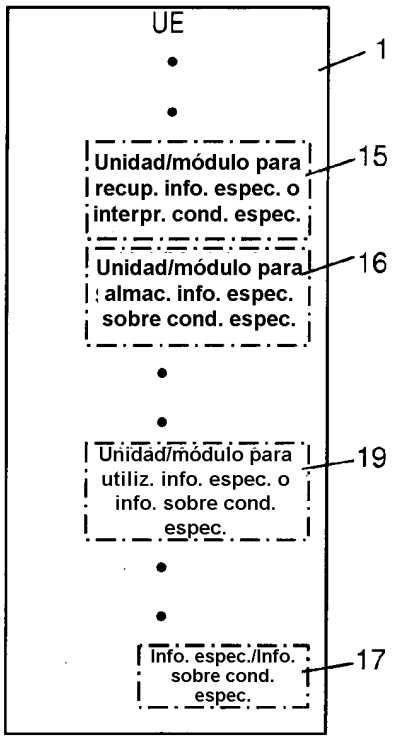

Fig. 4b

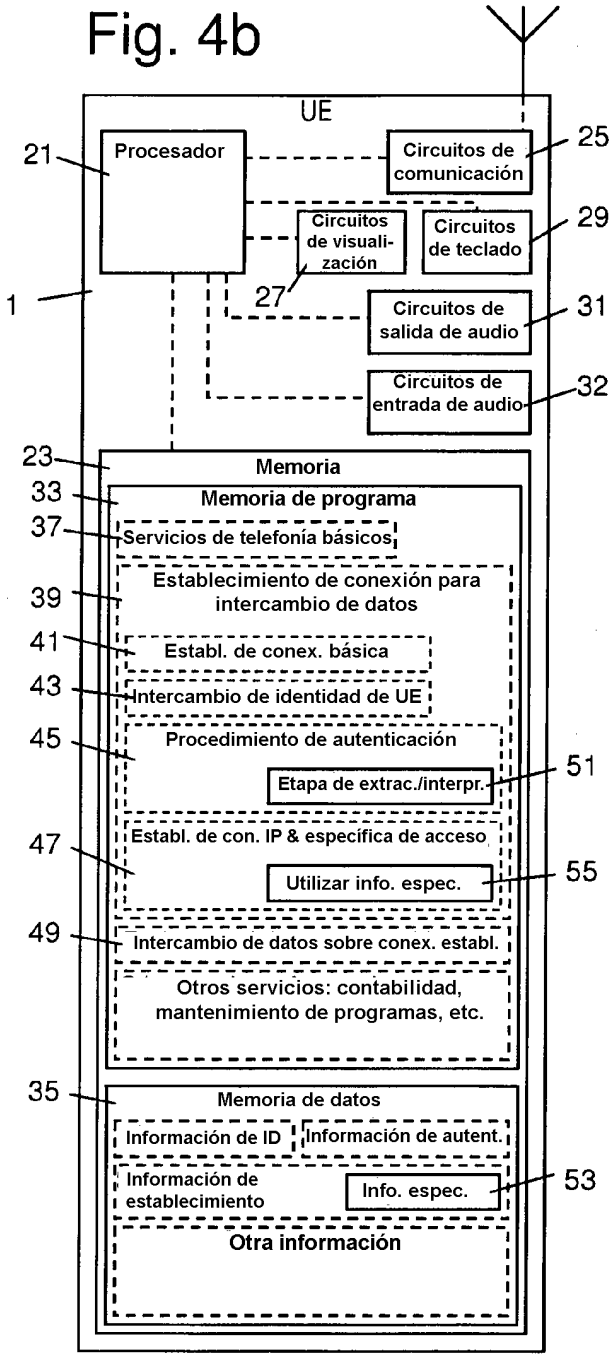

Fig. 4c

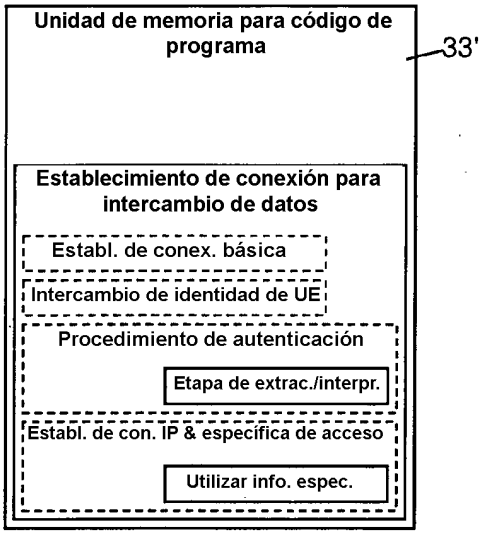

Fig. 5a

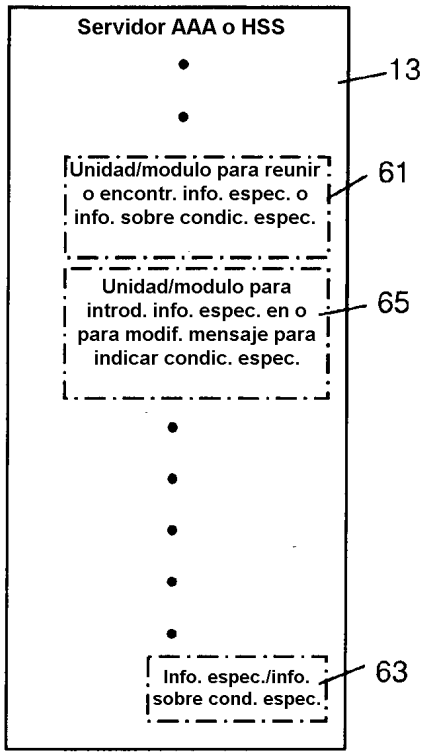

Fig. 5b

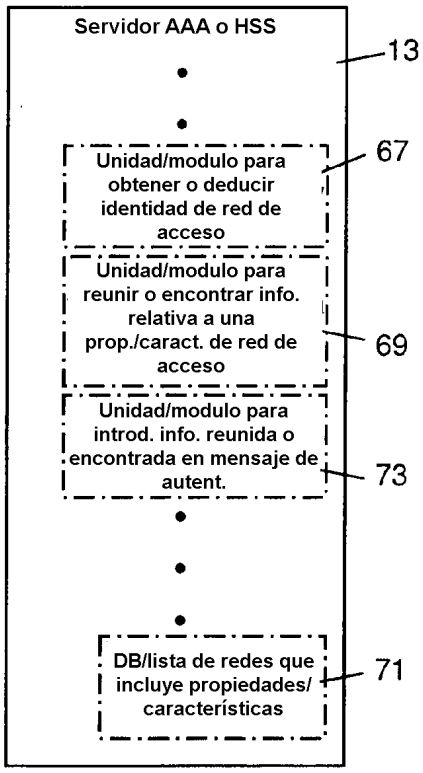

Fig. 5c

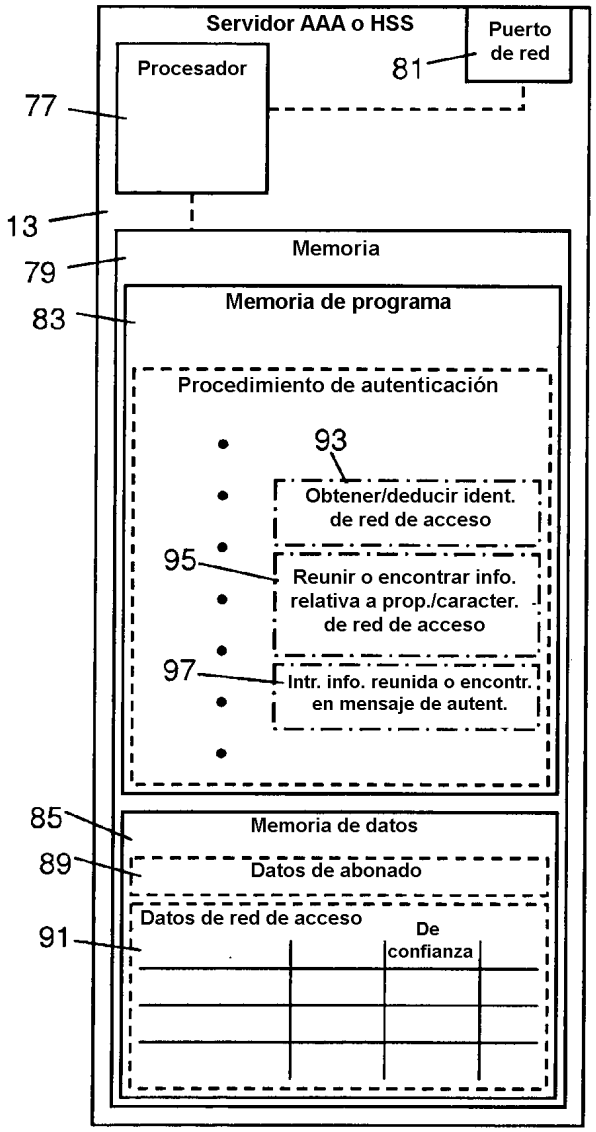

Fig. 5d