(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 806 991**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.10.2017 PCT/EP2017/077330**

(87) Fecha y número de publicación internacional: **03.05.2018 WO18077960**

(96) Fecha de presentación y número de la solicitud europea: **25.10.2017 E 17797092 (8)**

(97) Fecha y número de publicación de la concesión europea: **22.04.2020 EP 3459278**

(54) Título: **Autentificación para sistemas de próxima generación**

(30) Prioridad:

31.10.2016 US 201662415006 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.02.2021

(73) Titular/es:

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

(72) Inventor/es:

BEN HENDA, NOAMEN;
LEHTOVIRTA, VESA y
CASTELLANOS ZAMORA, DAVID

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Autentificación para sistemas de próxima generación

Campo técnico

La presente divulgación se refiere a un método y a un aparato para autentificación secundaria en una red.

Antecedentes

El Proyecto de Asociación de 3ª Generación (3GPP) está desarrollando actualmente los estándares para 5G, también conocidos como sistemas de próxima generación (NG). Se espera que 5G sea compatible con muchos escenarios nuevos y casos de uso y sea un habilitador para Internet de las cosas (IoT). Se espera que los sistemas NG proporcionen conectividad a una amplia gama de dispositivos nuevos, tal como sensores, dispositivos portátiles inteligentes, vehículos, máquinas, etc. Por lo tanto, la flexibilidad es una propiedad clave en Sistemas de NG. Esto se refleja en el requisito de seguridad para el acceso a la red que exige el soporte de métodos de autentificación alternativos y diferentes tipos de credenciales, en comparación con las credenciales habituales de autentificación y acuerdo de clave (AKA) aprovisionadas previamente por un operador y almacenadas de forma segura en una tarjeta de circuito integrado universal (UICC). Esto permitiría a los propietarios de fábricas o empresas aprovechar sus propios sistemas de gestión de identidad y credenciales para la autentificación y la seguridad de la red de acceso.

Entre las nuevas características de sistemas de NG está el concepto de segmentación de red. Un segmento de red (NS) es básicamente una instancia de una red central dedicada para proporcionar un servicio particular. Esto permitirá a los operadores manejar una amplia variedad de nuevos casos de uso, cada uno con diferentes requisitos de servicio en términos de calidad de servicio (QoS). Por ejemplo, un operador podría estar ejecutando un NS para los servicios habituales de banda ancha móvil (MBB), en paralelo con un NS de misión crítica para servicios de seguridad pública (tal como la función de pulsar para hablar de misión crítica (MCPTT)) que requiere una latencia muy baja, más en paralelo con un NS de IoT para medidores de electricidad con muy poco ancho de banda.

Entre los temas que se estudian en relación con la segmentación de red se encuentra el desacoplamiento de los procedimientos de autentificación y autorización para acceder a diferentes NS.

Qualcomm Inc., LG Electronics: "Way forward on support of non-3GPP access and update o solution 8.6 for support of untrusted non-3GPP access", el Proyecto de Asociación de 3ª Generación (3GPP), Reunión SA WG2 #117, S2-166283, divulga un método de autentificación a través de acceso no fiable no 3GPP. Después de obtener conectividad IP a través de un acceso no fiable que no sea 3GPP, un UE descubre una puerta de enlace (llamada ngPDG) utilizando un mecanismo similar al descubrimiento de ePDG en el EPC. El UE luego realiza una conexión de red en dos etapas. En primer lugar, el UE establece un túnel IPSec con la ngPDG utilizando los mismos procedimientos definidos para la ePDG en EPC. En segundo lugar, una vez que se establece el túnel y, por lo tanto, el UE se autentifica, el UE envía la señalización NAS que contiene una solicitud de conexión. La red, al recibir la solicitud de conexión NAS del UE, verifica que el UE ya está autentificado y procesa el procedimiento de conexión sin volver a autentificar el UE.

Sumario

Un objeto de las realizaciones presentadas en el presente documento es permitir el desacoplamiento de la autentificación en sistemas de próxima generación.

Según un primer aspecto, se presenta un método para autentificación secundaria en una red. El método lo realiza un equipo de usuario (UE) y comprende establecer una autentificación primaria con una función de anclaje de seguridad (SEAF), establecer una sesión de plano de usuario (UP) o conexión con o mediante una función UP (UPF), recibir una solicitud de autentificación basada en el protocolo de autentificación extensible (EAP) desde la UPF, enviar una respuesta de autentificación basada en EAP a la UPF y recibir un resultado de autentificación basado en EAP de la UPF, el resultado de autentificación basado en EAP basado en una respuesta de verificación de un servidor externo de autentificación, autorización y contabilidad (AAA).

El UE puede ser además un UE de próxima generación (NG). La UPF puede ser además una NG UPF.

Según un segundo aspecto, se presenta un método para autentificación secundaria en una red. El método se realiza mediante una función de plano de usuario (UP) (UPF), y comprende establecer una sesión de plano de usuario (UP) o conexión con un equipo de usuario (UE), enviar una solicitud de autentificación basada en el protocolo de autentificación extensible (EAP) al UE, recibir una respuesta de autentificación basada en EAP del UE, enviar una solicitud de verificación de la respuesta de autentificación basada en EAP recibida a un servidor externo de autentificación, autorización y contabilidad (AAA), recibir una respuesta de verificación del servidor externo AAA y enviar un resultado de autentificación al UE, en el que el resultado de autentificación se basa en la respuesta de verificación desde el servidor externo AAA.

El UE puede ser además un UE de próxima generación (NG). La UPF puede ser además una NG UPF.

Según un tercer aspecto, se presenta un equipo de usuario (UE) para operar en una red. El UE comprende un procesador y un producto de programa de ordenador. El producto del programa de ordenador almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el UE establezca una autentificación primaria con una función de anclaje de seguridad (SEAF), establezca una sesión de plano de usuario (UP) o una conexión con una función UP (UPF), reciba una solicitud de autentificación basada en el protocolo de autentificación extensible (EAP) de la UPF, enviar una respuesta de autentificación basada en EAP a la UPF y recibir un resultado de autentificación basado en EAP a través de la UPF, el resultado de autentificación basado en EAP basado en una respuesta de verificación desde un servidor externo de autentificación, autorización y contabilidad (AAA).

El UE puede ser además un UE de próxima generación (NG). La UPF puede ser además una NG UPF.

Según un cuarto aspecto, se presenta una función de plano de usuario (UP) (UPF) operativa en una red. La UPF comprende un procesador y un producto de programa de ordenador. El producto del programa de ordenador almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que la UPF establezca una sesión de plano de usuario (UP) o una conexión con un equipo de usuario (UE), envíe una solicitud de autentificación basada en el protocolo de autentificación extensible (EAP) al UE, reciba una respuesta de autentificación basada en EAP del UE, envíe una solicitud de verificación de la respuesta de autentificación basada en EAP recibida a un servidor externo de autentificación, autorización y contabilidad (AAA), reciba una respuesta de verificación del servidor externo AAA y envíe un resultado de autentificación al UE, en el que el resultado de autentificación se basa en la respuesta de verificación desde el servidor externo AAA.

El UE puede ser además un UE de próxima generación (NG). La UPF puede ser además una NG UPF.

Según un ejemplo de la presente divulgación, se presenta un equipo de usuario (UE) para operar en una red. El UE comprende medios para establecer una sesión de plano de usuario (UP) o conexión con una función UP (UPF), medios para recibir una solicitud de autentificación basada en el protocolo de autentificación extensible (EAP) de la UPF, y medios para enviar una respuesta de autentificación basada en EAP a la UPF

El UE puede comprender además medios para establecer una autentificación primaria con una función de anclaje de seguridad (SEAF).

El UE puede comprender además medios para recibir un resultado de autentificación basado en EAP desde la UPF.

El UE puede ser además un UE de próxima generación (NG). La UPF puede ser además una NG UPF.

Según otro ejemplo de la presente divulgación, se presenta una función de plano de usuario (UP) operativa (UPF) en una red. La UPF comprende medios para establecer una sesión o conexión de plano de usuario (UP) con un equipo de usuario (UE), medios para enviar una solicitud de autentificación basada en el protocolo de autentificación extensible (EAP) al UE, y medios para recibir una respuesta de autentificación basada en EAP desde el UE

La UPF puede comprender además medios para enviar una solicitud de verificación de la respuesta de autentificación basada en EAP recibida a un servidor de autentificación, autorización y contabilidad (AAA); y medios para recibir una respuesta de verificación desde el servidor AAA.

La UPF puede comprender además medios para enviar un resultado de autentificación al UE, en el que la autentificación se basa en la respuesta de verificación desde el servidor AAA.

El UE puede ser además un UE de próxima generación (NG). La UPF puede ser además una NG UPF.

Según un séptimo aspecto, se presenta un programa de ordenador para autentificación secundaria en una red. El programa de ordenador comprende un código de programa de ordenador que, cuando se ejecuta en un equipo de usuario (UE), hace que el UE realice las etapas del primer aspecto.

El UE puede ser además un UE de próxima generación (NG). La UPF puede ser además una NG UPF.

Según un octavo aspecto, se presenta un programa de ordenador para autentificación secundaria en una red. El programa de ordenador que comprende código del programa de ordenador que, cuando se ejecuta en una función de plano de usuario (UP) (UPF), hace que la UPF realice las etapas del segundo aspecto.

El UE puede ser además un UE de próxima generación (NG). La UPF puede ser además una NG UPF.

Según un noveno aspecto, se presenta un producto de programa de ordenador. El producto de programa de ordenador comprende un programa de ordenador y un medio de almacenamiento legible por ordenador en el que se almacena el programa de ordenador. En general, todos los términos utilizados en las reivindicaciones se han de interpretar de acuerdo con su significado ordinario en el campo técnico, a menos que explícitamente se defina de otro modo en este documento. Todas las referencias a "un/el elemento, aparato, componente, medio, etapa, etc." deben interpretarse abiertamente como referencias a al menos una instancia del elemento, aparato, componente, medio, etapa, etc., a menos que se indique explícitamente lo contrario. Las etapas de cualquier método divulgado aquí no tienen que realizarse en el orden exacto descrito, a menos que se indique explícitamente.

Breve descripción de los dibujos

Ahora se describe el concepto inventivo, a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

La figura 1 es un diagrama esquemático que ilustra un entorno en el que se pueden aplicar las realizaciones presentadas en el presente documento;

La figura 2 muestra esquemáticamente un flujo para autentificación secundaria en LTE;

La figura 3 muestra esquemáticamente un flujo para autentificación secundaria basada en EAP en sistemas de próxima generación;

Las figuras 4-5 muestran esquemáticamente arquitecturas de protocolo para autentificación secundaria basadas en EAP para realizaciones presentadas en el presente documento;

Las figuras 6A-6B son diagramas de flujo que ilustran métodos para realizaciones presentadas en el presente documento;

Las figuras 7-8 son diagramas esquemáticos que ilustran algunos componentes de los dispositivos presentados en el presente documento; y

Las figuras 9-10 son diagramas esquemáticos que muestran módulos funcionales de dispositivos presentados en el presente documento.

Descripción detallada

El concepto inventivo se describirá ahora más completamente en lo sucesivo con referencia a los dibujos adjuntos, en los que se muestran ciertas realizaciones preferidas del concepto inventivo. Sin embargo, este concepto inventivo puede realizarse de muchas formas diferentes y no debe interpretarse como limitada a las realizaciones expuestas en este documento; más bien, estas realizaciones se proporcionan a modo de ejemplo, de modo que esta divulgación será minuciosa y completa, y transmitirá completamente el alcance del concepto inventivo a los expertos en la materia. Números similares se refieren a elementos similares en toda la descripción.

Un escenario posible para desacoplar los procedimientos de autentificación y autorización para acceder a diferentes segmentos de red (NS) es el siguiente. Para que un equipo de usuario NG (UE) acceda a un NS particular, el operador primero ejecutará una autentificación primaria (habitual) para el acceso inicial a la red seguido de una autentificación secundaria específica de NS. La autentificación secundaria específica de NS posiblemente esté bajo el control de un tercero. Esto supone una confianza entre el proveedor de servicios de terceros y el operador de red móvil (MNO) que, por ejemplo, ofrece servicios de acceso y transporte a este tercero en una instancia de NS dedicada.

En la evolución a largo plazo (LTE), existe un mecanismo que podría ser relevante para el escenario descrito. Este mecanismo se describe en la cláusula 5.3.2 del TS 23.401. Se basa en la llamada solicitud de opción cifrada y utiliza un elemento de información llamado opciones de configuración de protocolo (PCO).

El PCO es uno de los elementos de información en los mensajes de estrato sin acceso (NAS). El PCO se puede usar en varios tipos de mensajes, tal como una solicitud de conectividad de red de paquetes de datos (PDN) para enviar información de manera transparente a través de una entidad de gestión de movilidad (MME) y una puerta de enlace de servicio (S-GW) a una PDN-GW. Por ejemplo, el PCO puede incluir una preferencia de asignación de dirección que indica que el UE prefiere obtener una dirección de protocolo de Internet versión 4 (IPv4) solo después de una activación de portador predeterminada por medio del protocolo de configuración dinámica de servidor versión cuatro (DHCPv4).

Un caso de uso de PCO es la transferencia del protocolo de autentificación de contraseña (PAP) y los nombres de usuario y contraseñas del protocolo de autentificación de protocolo de enlace (CHAP) a la PDN-GW, que luego los ejecuta a través de un servidor de autentificación, autorización y contabilidad (AAA) para autorización de acceso. El servidor AAA puede estar ubicado en un dominio externo. Dado que los nombres de usuario y las contraseñas son confidenciales y deben protegerse, si el UE tiene la intención de enviar el PCO que requiera cifrado (por ejemplo, nombres de usuario y contraseñas PAP/CHAP), el UE establecerá un indicador de transferencia de opciones cifradas en un mensaje de solicitud de adjunto y enviará el PCO solo después de que se haya completado la autentificación y la configuración de seguridad NAS.

La figura 2 muestra el flujo de mensajes requerido para ejecutar dicho procedimiento de autentificación adicional (es decir, secundario) a través de PDN-GW en LTE. A continuación, se proporciona una descripción más detallada de las etapas a seguir.

Un UE está dentro del dominio de UE. Un MME, una S-GW, un servidor de abonado doméstico (HSS) y una PDN-GW están dentro del dominio MNO. Un servidor AAA está dentro de un dominio de terceros.

En la etapa 1, el UE envía un mensaje de solicitud de conexión con un indicador de transferencia de opciones cifrado establecido en el MME.

En la etapa 2, se ejecuta un procedimiento de autentificación y acuerdo de clave (AKA) entre el UE y el HSS. Tras una autentificación exitosa, se ejecutan las siguientes etapas.

En la etapa 3 se configura una seguridad NAS, utilizando el comando de modo seguro (SMC). Después de configurar la seguridad NAS, todos los mensajes NAS están protegidos con confidencialidad e integridad.

En la etapa 4, el MME envía un mensaje de solicitud de opciones cifradas al UE para recuperar el PCO.

En la etapa 5, el UE responde con un mensaje de respuesta de opciones cifradas que incluye el nombre de usuario y la contraseña PAP/CHAP en el elemento de información PCO. En caso de que el UE tenga suscripciones a múltiples PDN, el UE también incluye un nombre de punto de acceso (APN) en el mensaje.

En la etapa 6, el MME descifra los datos recibidos, utiliza los posibles APN proporcionados para identificar una PDN-GW y reenvía el PCO a través de la S-GW a la PDN-GW objetivo en un mensaje de solicitud de creación de sesión.

En la etapa 7, la PDN-GW envía la información PAP/CHAP recibida en un mensaje de solicitud de acceso de diámetro/radio a un servidor AAA externo. Tras el éxito, el procedimiento de creación de la sesión continúa como de costumbre.

Las etapas 4-7 anteriores representan, por lo tanto, una autentificación secundaria, realizada después de que se haya completado la primera autentificación en la etapa 2. Sin embargo, el uso de este mecanismo o extensión en sistemas NG proporcionaría algunos inconvenientes.

En primer lugar, el mecanismo es muy limitado en términos de posibles métodos de autentificación. Actualmente solo hay soporte para PAP y CHAP. Pero dado que PAP hoy es obsoleto desde un punto de vista de seguridad, solo CHAP es esencialmente posible de usar.

En segundo lugar, para admitir otros métodos y utilizar el elemento de información PCO para el transporte de información de autentificación, se requeriría el mecanismo para especificar mensajes especiales entre el MME y la S-GW y la S-GW y la PDN-GW dedicadas a este propósito. Es decir, manejar métodos de autentificación que requieren más de un solo viaje de ida y vuelta.

Además, es difícil ver cómo este mecanismo encajaría en la arquitectura NG, que se desglosará más adelante. De hecho, teniendo en cuenta las nuevas características arquitectónicas (TR 23.799), probablemente habrá más saltos en el camino entre el UE y la PDN-GW, por ejemplo, en relación con el trabajo en curso en la división del MME en una función de gestión de la movilidad (MMF) y una función de gestión de sesión SMF (TR 23.799) y el control y la separación del plano de usuario (CUPS) funcionan para el control y la división del plano de usuario (TR 23.714). Esto implica más sobrecarga y señalización en la red central (CN).

Finalmente, este mecanismo es una solución alternativa porque no existe un protocolo directo entre el UE y la PDN-GW. Hacerlo lo suficientemente genérico como para admitir otros métodos de autentificación sería técnicamente difícil, especialmente porque muchos métodos tienen recomendaciones y requisitos estrictos en la capa de transporte.

Ejecutando la autentificación secundaria en el plano de usuario (UP), una vez que se configura, se presenta. Se puede ejecutar una sesión UP limitada para el procedimiento de autentificación secundaria, en lugar de permitir el acceso total al PDN. Una vez que se completa la autentificación secundaria, una sesión UP limitada puede actualizarse a una que tenga acceso completo a una red de datos. También se presenta el uso de un protocolo de autentificación extensible (EAP), como se define en RFC3748. El EAP se utiliza para la autentificación entre el UE y un servidor AAA potencialmente externo, donde una función NG-UP (UPF), que desempeña un papel similar al del PDN-GWin LTE, respalda el papel de un autentificador EAP. Las cargas útiles de EAP serían transportadas por un protocolo para llevar autentificación para el acceso a la red (PANA), como se define en RFC5191, cuyo protocolo está basado en IP. Otra alternativa es que la NG-UPF respalde el papel del servidor EAP.

La solución presentada utiliza EAP, que es ampliamente utilizado y proporciona soporte para muchos métodos de autentificación, tal como la seguridad de la capa de transporte EAP (TLS), la autentificación EAP y el acuerdo de clave (AKA), el TLS tunelizado EAP (TTLS) y el protocolo de autentificación extensible protegido EAP (PEAP). La solución presentada está basada en IP y, por lo tanto, es independiente del tipo de red de acceso (AN). Además, dado que está basado en UP, la autentificación secundaria se puede realizar de forma independiente sobre una base específica de NS incluso para escenarios en los que el NG-UE admite múltiples conexiones NS posiblemente simultáneas. Al usar el EAP, la solución también admite diferentes tipos de credenciales y métodos de autentificación. El intercambio de EAP puede beneficiarse de la protección sobre una interfaz aérea.

La autentificación secundaria se ejecuta así de los portadores de UP una vez que el NG-UE tiene asignada una dirección IP. Luego, el EAP se usa para la autentificación entre el NG-UE y el servidor AAA (potencialmente externo)

donde la NG-UPF respalda el papel del autentificador de EAP.

Una realización en la que la NG-UPF actúa como un autentificador de EAP se presenta con referencia a la figura 3.

La figura 3 muestra un flujo en el que se ejecuta una autentificación secundaria basada en UP con un servidor externo AAA. El NG-UE está en el dominio del UE. La función de gestión de movilidad NG (MMF), la función de gestión de sesión NG (SMF), la función de anclaje de seguridad NG (SEAF) y NG-UPF están en el dominio MNO. La NG-UPF es una UPF correspondiente a un PDN-GWin LTE. El servidor AAA está en un dominio de terceros. Los requisitos en la NG-UPF es incluir el soporte de PANA y EAP, posiblemente además del soporte de todas las características UP necesarias de la PDN-GW en LTE, tal como el soporte de una interfaz SGi. En general, se utiliza un prefijo NG para la función del sistema NG correspondiente a los conceptos LTE.

En la etapa 1, el NG-UE envía una solicitud de conexión iniciando el procedimiento de conexión. La solución presentada en el presente documento no depende de cómo se admite el corte de red, por ejemplo, cómo se seleccionan las instancias NS y cómo se dirige el NG-UE a las apropiadas.

En la etapa 2, el NG-UE ejecuta una autentificación primaria con el NG SEAF. El NG SEAF puede conectarse además a una función del servidor de autentificación NG (AUSF). Una autentificación secundaria posterior no depende de cómo se implementen NG SEAF y NG MMF (es decir, colocados o divididos) ni de la ubicación de NG SEAF (red móvil terrestre pública local o visitada (PLMN)).

En la etapa 3 se establece una seguridad del plano de control entre el NG-UE y el punto final del NG NAS. El punto final del NG NAS puede ser, por ejemplo, el NG MMF o el NG SMF.

En la etapa 4, se establece una sesión de unidad de datos de protocolo (PDU) para el transporte de datos UP entre el NG-UE y una red de datos a través de la NG-UPF. La etapa 4 puede ser una sesión limitada que solo permite ejecutar el procedimiento de autentificación secundaria. La autentificación secundaria posterior depende de la configuración del UP, ya que establece la conectividad IP entre el NG-UE y la NG-UPF.

En la etapa 5, se ejecuta una autentificación secundaria basada en EAP entre el NG-UE y la NG-UPF, respaldando aquí el papel de un autentificador EAP y confiando en un servidor AAA externo de extremo trasero. A partir de entonces, se le otorga acceso al NG-UE en la red de datos en función del resultado de este procedimiento de autentificación.

Esta solución presentada es independiente de cómo se integrará el acceso no 3GPP y si las etapas 1 a 3 se ejecutan exactamente como se muestra aquí o de manera diferente. Mientras se establezca una conectividad IP entre el NG-UE y la NG-UPF, lo que se logra en la etapa 4, la autentificación basada en EAP se puede ejecutar en la etapa 5. En caso de que se haya establecido la seguridad de la red de acceso de radio (RAN) antes de la etapa 5, entonces el intercambio de EAP estaría protegido también en la interfaz aérea.

La figura 4 muestra una arquitectura de protocolo para la autentificación secundaria basada en EAP, entre la NG-UPF y el NG-UE con la NG-UPF como autentificador EAP, como se describe con referencia a la figura 3. La arquitectura mostrada en la figura 4 es similar a la arquitectura de LTE con respecto al transporte del tráfico UP entre el UE y la PDN-GW. Los cuadros en gris resaltan las capas de protocolo adicionales requeridas para proporcionar la autentificación secundaria basada en EAP descrita anteriormente.

Con referencia a la figura 5, se presenta una realización con una arquitectura de protocolo para la autentificación secundaria basada en EAP con NG-UPF como servidor EAP.

En esta realización, la NG-UPF termina el intercambio EAP y respalda el papel de un servidor EAP completo. El flujo de mensajes para esta realización es, por lo tanto, similar al de la figura 3, excepto que en la etapa 5 no se contacta con un servidor AAA externo.

Se ha presentado un mecanismo para autentificación adicional o secundaria en sistemas NG entre el NG-UE y la NG-UPF que termina el tráfico UP dentro de la red central y posiblemente interactúa con un servidor AAA externo. La NG-UPF corresponde a la PDN-GW en LTE. El mecanismo se basa en el tráfico EAP sobre IP sobre UP de modo que la NG-UPF respalda el papel de autentificador EAP o el papel del servidor EAP.

Una red de comunicación 4, en la que las realizaciones descritas en el presente documento pueden implementarse se presenta en la figura 1. Un equipo de usuario (UE) 1 se puede conectar de forma inalámbrica a una estación base (BS) 2. La BS 2 está conectada a una red central (CN) 3.

Un método, según una realización, para la autentificación secundaria en una red se presenta con referencia a la figura 6A. El método lo realiza un equipo de usuario (UE) de próxima generación (NG), y comprende establecer 110 una sesión de plano de usuario (UP) o conexión con una función NG-UP (UPF), recibir 130 una solicitud de autentificación basada en protocolo de autentificación extensible (EAP) desde la NG-UPF, y enviar 140 una respuesta de autentificación basada en EAP a la NG-UPF.

El método puede comprender además establecer 100 una autentificación primaria con un NG SEAF.

El método puede comprender además recibir un resultado de autentificación basado en EAP desde la UPF.

Un método, según una realización, para la autentificación secundaria en una red central se presenta con referencia a la figura 6B. El método se realiza mediante una función de plano de usuario (UP) (UPF) de próxima generación (NG), y comprende establecer 110 una sesión de plano de usuario (UP) o conexión con un equipo de usuario NG (UE), enviando a 120 una solicitud de autentificación basada en el protocolo de autentificación extensible (EAP) en el NG UE, y recibir 150 una respuesta de autentificación basada en EAP desde el NG UE.

El método puede comprender además enviar 160 una solicitud de verificación de la respuesta de autentificación basada en EAP recibida a un servidor de autentificación, autorización y contabilidad (AAA), y recibir 170 una respuesta de verificación desde el servidor AAA.

El método puede comprender además enviar un resultado de autentificación al UE, en el que la autentificación se basa en la respuesta de verificación desde el servidor AAA.

Un NG UE, de acuerdo con una realización, para operar en una red se presenta con referencia a la figura 7. El NG UE 1 comprende un procesador 10 y un producto de programa de ordenador 12, 13. El producto del programa de ordenador almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el NG UE establezca 110 una sesión UP o conexión con una NG-UPF, reciba 130 una solicitud de autentificación basada en EAP desde la NG-UPF y envíe 140 una respuesta de autentificación basada en EAP a la NG-UPF.

Una NG-UPF de acuerdo con una realización, operativa en una red central se presenta con referencia a la figura 8. La NG-UPF comprende un procesador 10, y un producto de programa de ordenador 12, 13 que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que la NG-UPF establezca 110 una sesión UP o conexión a un NG UE, envíe 120 una solicitud de autentificación basada en EAP al NG UE y reciba 150 una respuesta de autentificación basada en EAP desde el NG UE.

Un NG UE, según una realización, para operar en una red, se presenta con referencia a la figura 9. El NG UE comprende un administrador de comunicación 61 para establecer 110 una sesión UP o conexión con una NG-UPF, recibir 130 una solicitud de autentificación basada en EAP desde la NG-UPF y enviar 140 una respuesta de autentificación basada en EAP a la NG-UPF.

Una NG-UPF, de acuerdo con una realización, operativo en una red se presenta con referencia a la figura 10. La NG-UPF comprende un administrador de comunicación 71 para establecer 110 una sesión UP o conexión con un NG UE, enviar 120 una solicitud de autentificación basada en EAP al NG UE, y para recibir 150 una respuesta de autentificación basada en EAP desde el NG UE.

Se presenta un programa de ordenador 14, 15, según una realización, para autentificación secundaria en una red. El programa de ordenador comprende un código de programa de ordenador que, cuando se ejecuta en un NG UE, hace que el NG UE establezca 110 una sesión UP o una conexión con una NG-UPF, reciba 130 una solicitud de autentificación basada en EAP desde la NG-UPF y envíe 140 una respuesta de autentificación basada en EAP a la NG-UPF.

Se presenta un programa de ordenador 14, 15, según una realización, para autentificación secundaria en una red. El programa de ordenador comprende un código de programa de ordenador que, cuando se ejecuta en una NG-UPF, hace que la NG-UPF establezca 110 una sesión UP o una conexión con un NG UE, envíe 120 una solicitud de autentificación basada en EAP al NG UE y reciba 150 una respuesta de autentificación basada en EAP desde el NG UE.

Se presenta un producto de programa de ordenador 12, 13, según una realización. El producto de programa de ordenador comprende un programa de ordenador 14, 15 como se presentó anteriormente y un medio de almacenamiento legible por ordenador en el que se almacena el programa de ordenador 14, 15.

La figura 7 es un diagrama esquemático que muestra algunos componentes del NG UE 1. Se puede proporcionar un procesador 10 usando cualquier combinación de una o más de una unidad de procesamiento central adecuada, CPU, multiprocesador, microcontrolador, procesador de señal digital, DSP, circuito integrado específico de la aplicación, etc., capaz de ejecutar instrucciones de software de un programa de ordenador 14 almacenado en una memoria. Por lo tanto, se puede considerar que la memoria es o forma parte del producto de programa de ordenador 12. El procesador 10 puede configurarse para ejecutar métodos descritos en el presente documento con referencia a las figuras 12 y 13.

La memoria puede ser cualquier combinación de memoria de lectura y escritura y memoria de solo lectura, ROM. La memoria también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota.

También se puede proporcionar un segundo producto de programa de ordenador 13 en forma de memoria de datos, por ejemplo, para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 10.

La memoria de datos puede ser cualquier combinación de memoria de lectura y escritura y memoria de solo lectura, ROM, y también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota. La memoria de datos puede contener, por ejemplo, otras instrucciones de software 15, para mejorar la funcionalidad del NG UE 1.

El NG UE 1 puede comprender además una entrada/salida, I/0, interfaz 11 que incluye, por ejemplo, una interfaz de usuario. El NG UE 1 puede comprender además un receptor configurado para recibir señalización de otros nodos, y un transmisor configurado para transmitir señalización a otros nodos (no ilustrados). Se omiten otros componentes de la NG UE 1 para no oscurecer los conceptos presentados en el presente documento.

La figura 9 es un diagrama esquemático que muestra bloques funcionales del NG UE 1. Los módulos pueden implementarse solo como instrucciones de software, como un programa de ordenador que se ejecuta en el servidor de caché o solo hardware, como circuitos integrados específicos de la aplicación, matrices de puertas programables en campo, componentes lógicos discretos, transceptores, etc., o como una combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales pueden implementarse mediante software y otros mediante hardware. Los módulos corresponden a las etapas del método ilustrado en la figura 6A, que comprende una unidad de gestión de comunicación 61 y una unidad de módulo de determinación 60. En las realizaciones donde uno o más de los módulos son implementados por un programa de ordenador, se entenderá que estos módulos no corresponden necesariamente a módulos de proceso, sino que pueden escribirse como instrucciones de acuerdo con un lenguaje de programación en el que se implementarían, ya que algunos lenguajes de programación no suelen contener módulos de proceso.

El administrador de comunicación 61 es para operar en una red. Este módulo corresponde a la etapa UP de establecimiento 110, la etapa 130 de solicitud de recepción y la etapa 140 de respuesta de envío de la figura 6A. Este módulo puede ser implementado, por ejemplo, por el procesador 10 de la figura 7, cuando se ejecuta el programa de ordenador.

El administrador de determinación 60 es para operar en una red. Este módulo corresponde a la etapa de autentificación primaria 100 de la figura 6A. Este módulo puede ser implementado, por ejemplo, por el procesador 10 de la figura 7, cuando se ejecuta el programa de ordenador.

La figura 8 es un diagrama esquemático que muestra algunos componentes de la NG-UPF 3. Se puede proporcionar un procesador 10 usando cualquier combinación de una o más de una unidad de procesamiento central adecuada, CPU, multiprocesador, microcontrolador, procesador de señal digital, DSP, circuito integrado específico de la aplicación, etc., capaz de ejecutar instrucciones de software de un programa de ordenador 14 almacenado en una memoria. Por lo tanto, se puede considerar que la memoria es o forma parte del producto de programa de ordenador 12. El procesador 10 puede configurarse para ejecutar los métodos descritos en el presente documento con referencia a la figura 6B.

La memoria puede ser cualquier combinación de memoria de lectura y escritura, RAM, y memoria de solo lectura, ROM. La memoria también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota.

También se puede proporcionar un segundo producto de programa de ordenador 13 en forma de memoria de datos, por ejemplo, para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 10. La memoria de datos puede ser cualquier combinación de memoria de lectura y escritura y memoria, RAM, de solo lectura, ROM, y también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota. La memoria de datos puede, por ejemplo, contener otras instrucciones de software 15, para mejorar la funcionalidad de la NG-UPF 3.

La NG-UPF 3 puede comprender además una entrada/salida, I/0, interfaz 11 que incluye, por ejemplo, una interfaz de usuario. La NG-UPF 3 puede comprender además un receptor configurado para recibir señalización desde otros nodos, y un transmisor configurado para transmitir señalización a otros nodos (no ilustrados). Se omiten otros componentes de la NG-UPF 3 para no oscurecer los conceptos presentados en el presente documento.

La figura 10 es un diagrama esquemático que muestra bloques funcionales de la NG-UPF 3. Los módulos pueden implementarse solo como instrucciones de software, como un programa de ordenador que se ejecuta en el servidor de caché o solo hardware, como circuitos integrados específicos de la aplicación, matrices de puertas programables en campo, componentes lógicos discretos, transceptores, etc., o como una combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales pueden implementarse mediante software y otros mediante hardware. Los módulos corresponden a las etapas de los métodos ilustrados en la figura 6B, que comprenden una unidad de gestión de comunicación 71 y una unidad de gestión de determinación 70. En las realizaciones donde uno o más de los módulos son implementados por un programa de ordenador, se entenderá que estos módulos no corresponden necesariamente a módulos de proceso, sino que pueden escribirse como

instrucciones de acuerdo con un lenguaje de programación en el que se implementarían, ya que algunos lenguajes de programación no suelen contener módulos de proceso.

El administrador de comunicación 71 es para operar en una red central. Este módulo corresponde a la etapa UP de establecimiento 110, la etapa 120 de solicitud de envío y la etapa 150 de respuesta de recepción de la figura 6B. Este módulo puede ser implementado, por ejemplo, por el procesador 10 de la figura 8, cuando se ejecuta el programa de ordenador.

La unidad de gestión de determinación 70 es para operar en una red central. Este módulo corresponde a la etapa 160 de solicitud de verificación y a la etapa 170 de respuesta de verificación de la figura 6B. Este módulo puede ser implementado, por ejemplo, por el procesador 10 de la figura 8, cuando se ejecuta el programa de ordenador.

El concepto inventivo se ha descrito principalmente anteriormente con referencia a unas pocas realizaciones. Sin embargo, como apreciará fácilmente una persona experta en la técnica, otras realizaciones que las descritas anteriormente son igualmente posibles dentro del alcance de las reivindicaciones de patente adjuntas.

REIVINDICACIONES

1. Un método para autentificación secundaria en una red, realizado por un equipo de usuario (UE), comprendiendo el método:

establecer (100) una autentificación primaria con una función de anclaje de seguridad, SEAF;

establecer (110) una sesión o conexión de plano de usuario, UP, con o mediante una función UP, UPF;

recibir (130) una solicitud de autentificación basada en un protocolo de autentificación extensible, EAP, a través de la UPF;

enviar (140) una respuesta de autentificación basada en EAP a la UPF; y

recibir un resultado de autentificación basado en EAP a través de la UPF, el resultado de autentificación basado en EAP basado en una respuesta de verificación desde un servidor externo de autentificación, autorización y contabilidad, AAA.

2. El método según la reivindicación 1, en el que el equipo de usuario, UE, es un UE de próxima generación, NG.

3. El método según la reivindicación 1, en el que la función de plano de usuario, UPF, es una UPF de próxima generación, NG.

4. El método según la reivindicación 1, en el que la SEAF está conectada además a una función del servidor de autentificación, AUSF.

5. Un método para autentificación secundaria en una red, realizado por una función UP de plano de usuario, UPF, comprendiendo el método:

establecer (110) una sesión UP o conexión a un equipo de usuario, UE;

enviar (120) una solicitud de autentificación basada en un protocolo de autentificación extensible, EAP, al UE;

recibir (150) una respuesta de autentificación basada en EAP desde el UE;

enviar (160) una solicitud de verificación de la respuesta de autentificación basada en EAP recibida a un servidor externo de autentificación, autorización y contabilidad, AAA;

recibir (170) una respuesta de verificación desde el servidor externo AAA; y

enviar un resultado de autentificación al UE, en el que el resultado de autentificación se basa en la respuesta de verificación desde el servidor externo AAA.

6. El método según la reivindicación 5, en el que el equipo de usuario, UE, es un equipo de usuario, UE, de próxima generación.

7. El método según la reivindicación 5, en el que la función de plano de usuario, UPF, es una UPF de próxima generación, NG.

8. Un equipo de usuario, UE, para operar en una red, comprendiendo el UE:

un procesador (10); y

un producto de programa de ordenador (12, 12) que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el UE:

establezca (100) una autentificación primaria con una función de anclaje de seguridad, SEAF;

establezca (110) una sesión o conexión de plano de usuario, UP, con o mediante una función UP, UPF;

reciba (130) una solicitud de autentificación basada en un protocolo de autentificación extensible, EAP, a través de la UPF;

envíe (140) una respuesta de autentificación basada en EAP a la UPF; y

reciba un resultado de autentificación basado en EAP a través de la UPF, el resultado de autentificación basado en EAP basado en una respuesta de verificación desde un servidor externo de autentificación, autorización y contabilidad, AAA.

9. El equipo de usuario, UE, según la reivindicación 8, en el que el UE es un UE de próxima generación, NG.

10. El equipo de usuario, UE, según la reivindicación 8, en el que la UPF es una UPF de próxima generación, NG.

11. El equipo de usuario, UE, según la reivindicación 8, en el que la SEAF está conectada además a una función de servidor de autentificación, AUSF.

12. Una función de plano de usuario, UP, UPF, operativa en una red, comprendiendo la UPF:

un procesador (10); y

un producto de programa de ordenador (12, 13) que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que la UPF:

establezca (110) una sesión UP o conexión con un equipo de usuario, UE;

envíe (120) una solicitud de autentificación basada en un protocolo de autentificación extensible, EAP, a la UPF;

reciba (150) una respuesta de autentificación basada en EAP desde el UE;

envíe (160) una solicitud de verificación de la respuesta de autentificación basada en EAP recibida a un servidor externo de autentificación, autorización y contabilidad, AAA;

reciba (170) una respuesta de verificación desde el servidor externo AAA; y

envíe un resultado de autentificación al UE, en el que el resultado de autentificación se basa en la respuesta de verificación desde el servidor externo AAA.

13. La función de plano de usuario, UP, UPF, según la reivindicación 12, en la que la UPF es una próxima generación, NG, UPF.

14. La función de plano de usuario, UP, UPF, según la reivindicación 12, en la que el UE es una próxima generación, NG, UE.

15. Un programa de ordenador (14, 15) para autentificación secundaria en una red, comprendiendo el programa de ordenador un código de programa de ordenador que, cuando se ejecuta en un equipo de usuario, UE, hace que el UE:

establezca (100) una autentificación primaria con una función de anclaje de seguridad, SEAF;

establezca (110) una sesión o conexión de plano de usuario, UP, con o mediante una función UP, UPF;

reciba (130) una solicitud de autentificación basada en un protocolo de autentificación extensible, EAP, a través de la UPF;

envíe (140) una respuesta de autentificación basada en EAP a la UPF;

y reciba un resultado de autentificación basado en EAP a través de la UPF, el resultado de autentificación basado en EAP basado en una respuesta de verificación desde un servidor externo de autentificación, autorización y contabilidad, AAA.

16. Un programa de ordenador (14, 15) para autentificación secundaria en una red, comprendiendo el programa de ordenador un código de programa de ordenador que, cuando se ejecuta en una función de plano de usuario, UP, UPF, hace que la UPF:

establezca (110) una sesión o conexión de plano de usuario, UP, a un equipo de usuario, UE;

envíe (120) una solicitud de autentificación basada en un protocolo de autentificación extensible, EAP, a la UPF;

reciba (150) una respuesta de autentificación basada en EAP desde el UE;

envíe (160) una solicitud de verificación de la respuesta de autentificación basada en EAP recibida a un servidor externo de autentificación, autorización y contabilidad, AAA;

reciba (170) una respuesta de verificación desde el servidor externo AAA; y

envíe un resultado de autentificación al UE, en el que la autentificación se basa en la respuesta de verificación desde el servidor externo AAA.

17. Un producto de programa de ordenador (12, 13) que comprende un medio de almacenamiento legible por ordenador en el que se almacena un programa de ordenador (14, 15) de acuerdo con una cualquiera de las reivindicaciones 15 o 16.

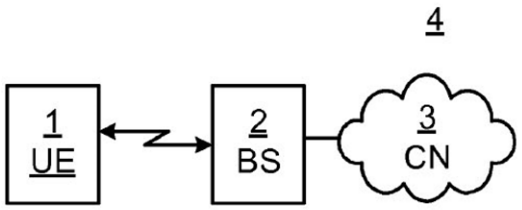
4
1
UE
2
BS
3
CN

Fig. 1

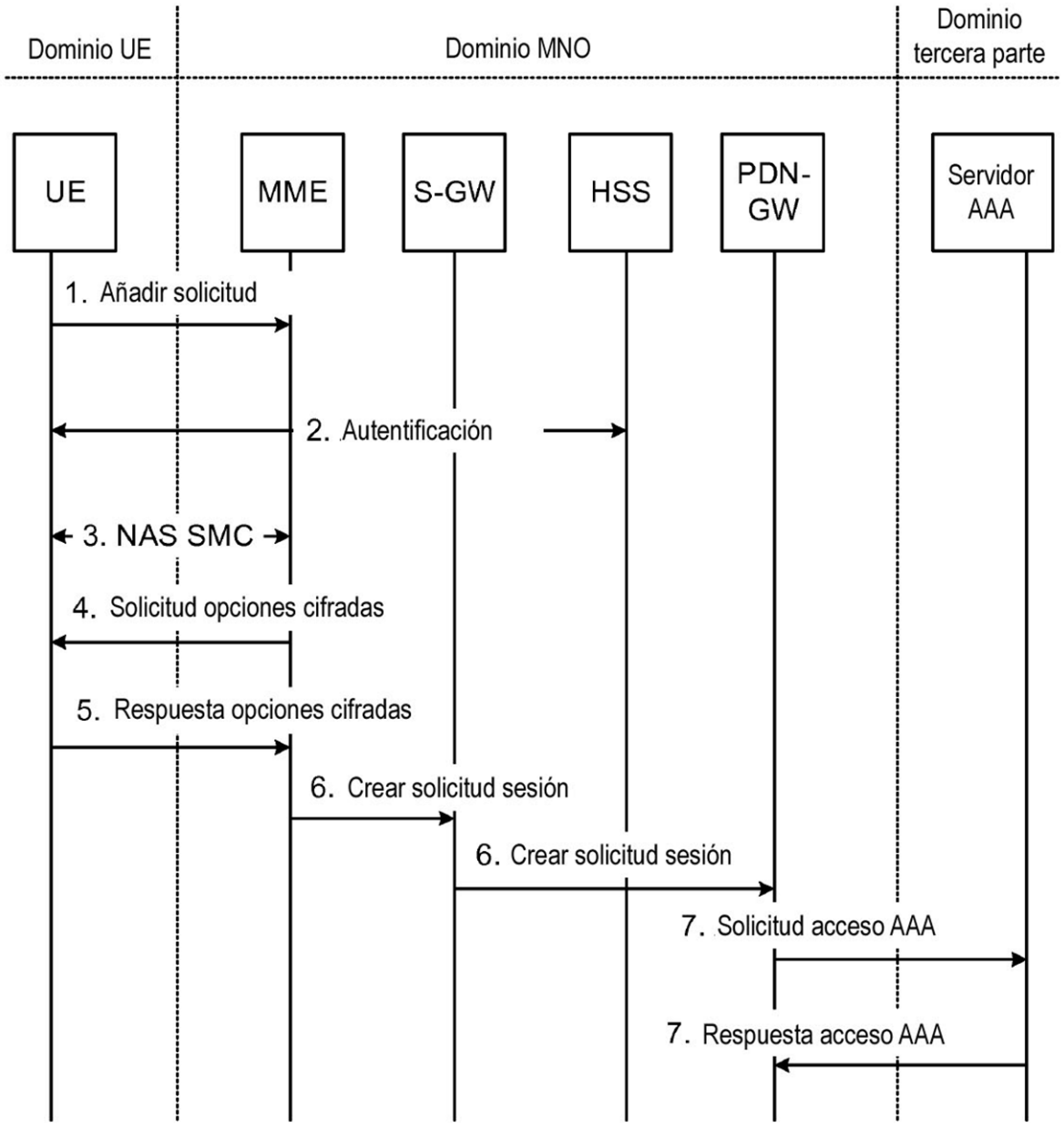
Dominio UE
Dominio MNO
Dominio tercera parte
UE
MME
S-GW
HSS
PDN-GW
Servidor AAA
1. Añadir solicitud
2. Autentificación
3. NAS SMC
4. Solicitud opciones cifradas
5. Respuesta opciones cifradas
6. Crear solicitud sesión
6. Crear solicitud sesión
7. Solicitud acceso AAA
7. Respuesta acceso AAA

Fig. 2

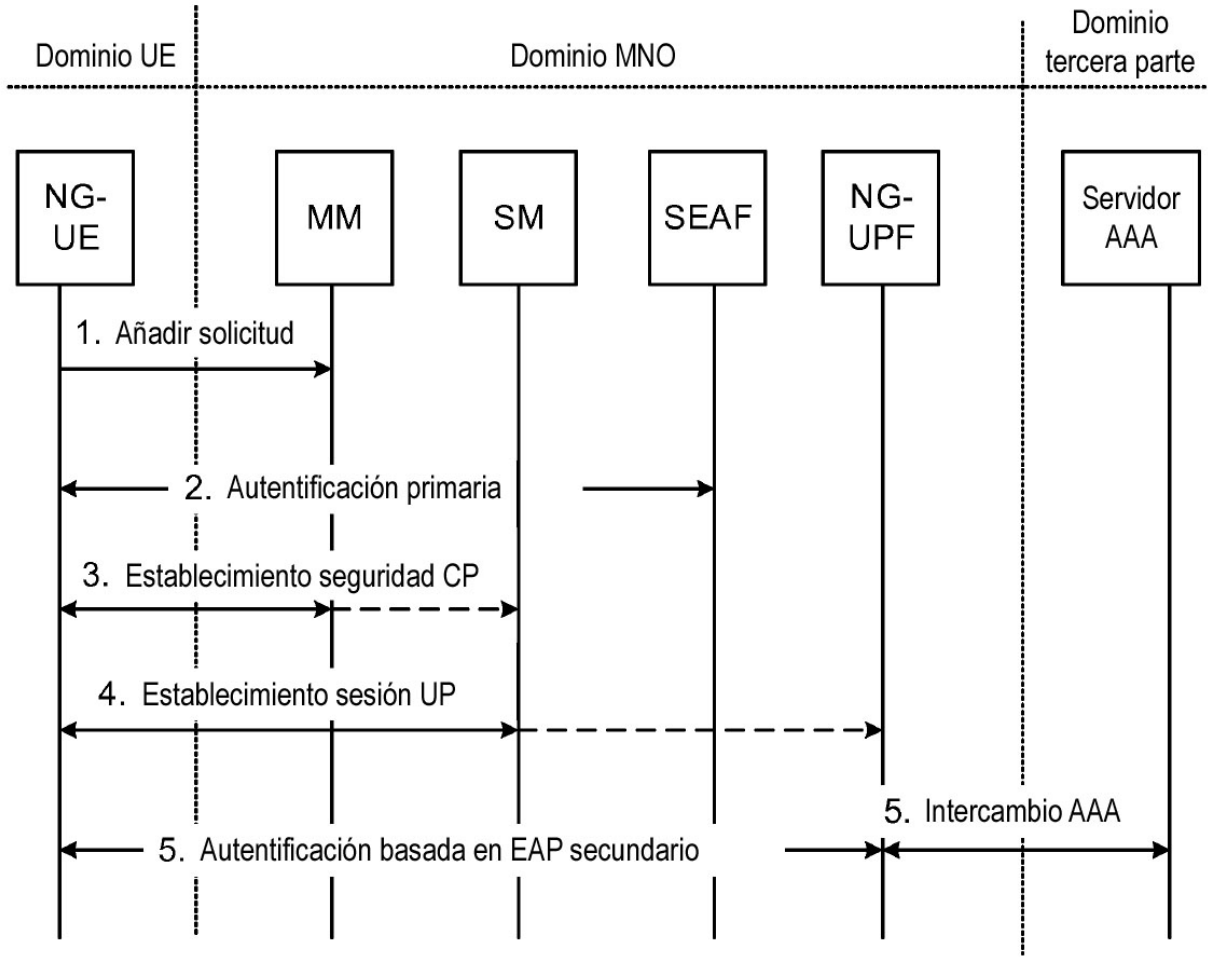
Dominio UE
Dominio MNO
Dominio tercera parte
NG-UE
MM
SM
SEAF
NG-UPF
Servidor AAA
1. Añadir solicitud
2. Autentificación primaria
3. Establecimiento seguridad CP
4. Establecimiento sesión UP
5. Intercambio AAA
5. Autentificación basada en EAP secundario

Fig. 3

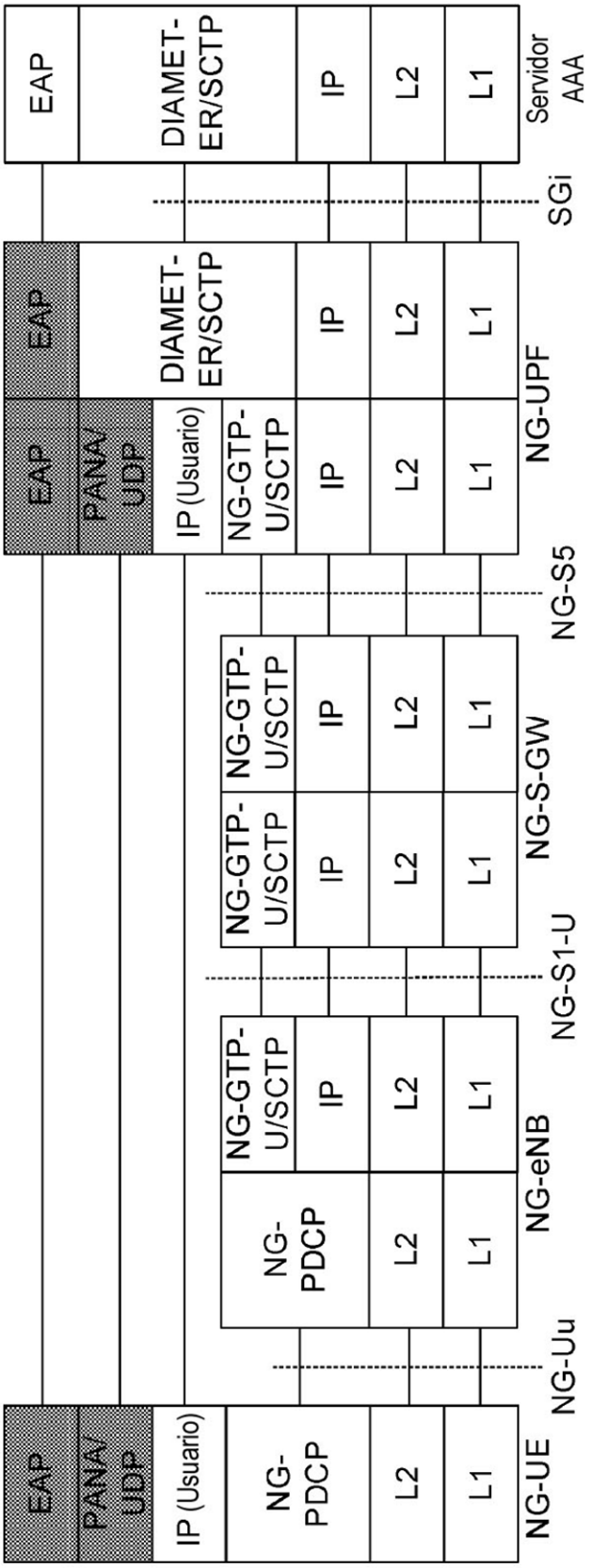
EAP
PANA/ UDP
IP (Usuario)
NG-PDCP
L2
L1
NG-UE
NG-Uu
NG-PDCP
NG-GTP-U/SCTP
IP
L2
L1
NG-eNB
NG-S1-U
NG-GTP-U/SCTP
IP
L2
L1
NG-S-GW
NG-S5
EAP
PANA/ UDP
IP (Usuario)
DIAMET-ER/SCTP
NG-GTP-U/SCTP
IP
L2
L1
NG-UPF
SGi
EAP
DIAMET-ER/SCTP
IP
L2
L1
Servidor AAA

Fig. 4

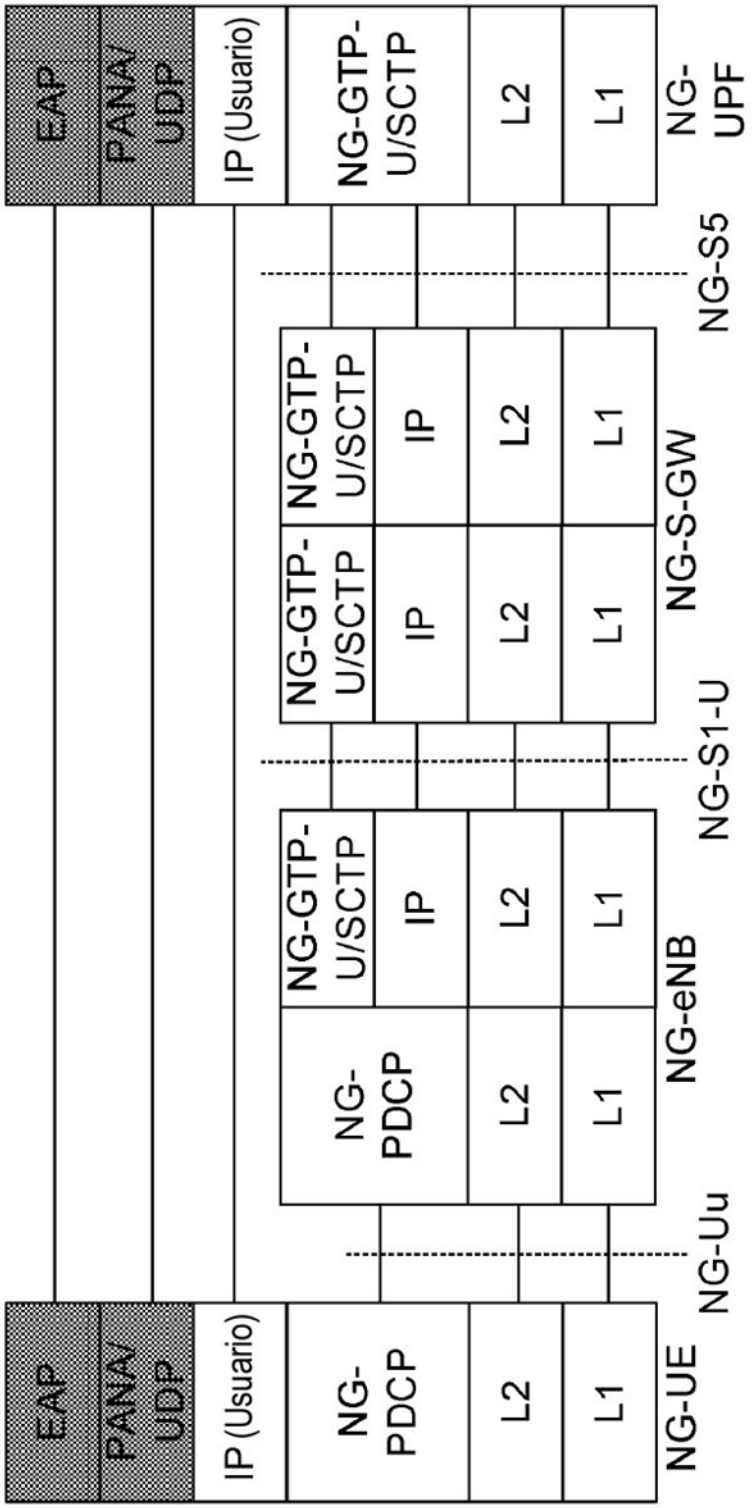
EAP
PANA/ UDP
IP (Usuario)
NG-PDCP
L2
L1
NG-UE
NG-Uu
NG-eNB
NG-GTP-U/SCTP
IP
NG-S1-U
NG-S-GW
NG-S5
NG-UPF

Fig. 5

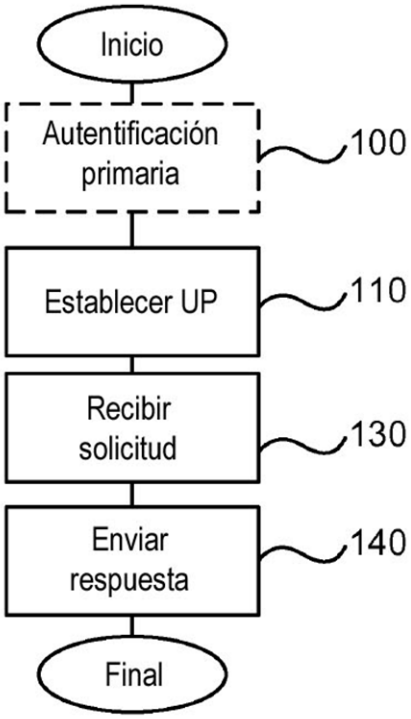
Inicio
Autentificación primaria
100
Establecer UP
110
Recibir solicitud
130
Enviar respuesta
140
Final

Fig. 6A

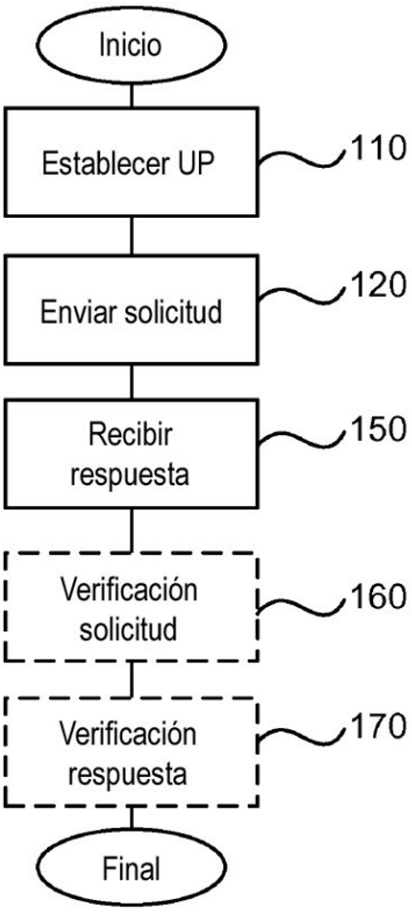
Inicio
Establecer UP
110
Enviar solicitud
120
Recibir respuesta
150
Verificación solicitud
160
Verificación respuesta
170
Final

Fig. 6B

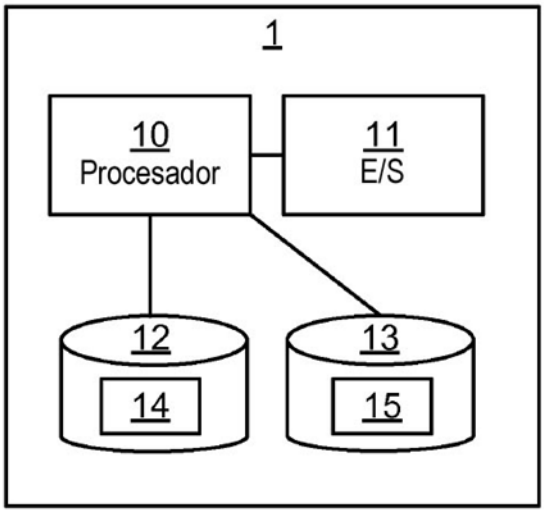

Fig. 7

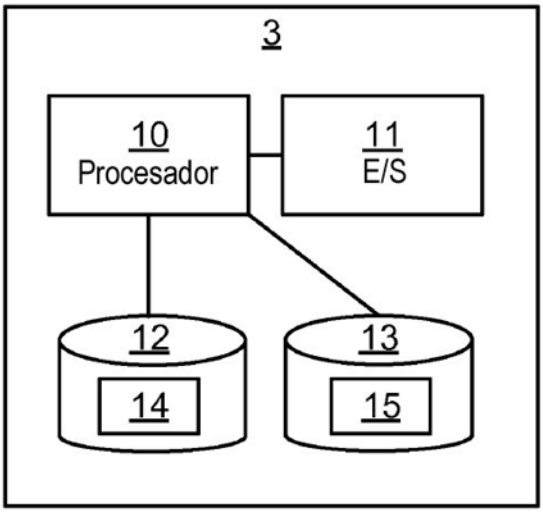

Fig. 8

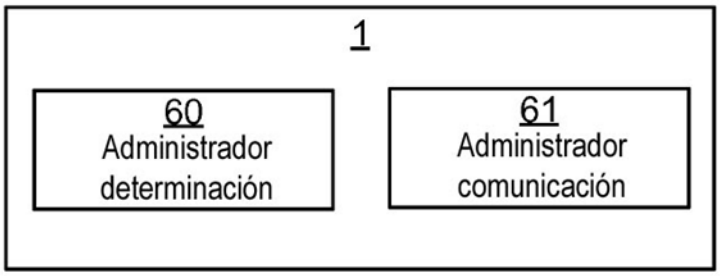

Fig. 9

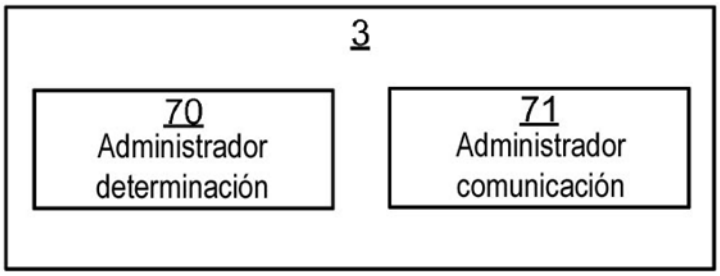

Fig. 10