(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 807 606**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04W 12/04 (2009.01)
H04L 12/26 (2006.01)
H04L 9/08 (2006.01)
H04W 80/04 (2009.01)
H04L 1/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.03.2015 PCT/SE2015/050357**

(87) Fecha y número de publicación internacional: **29.09.2016 WO16153402**

(96) Fecha de presentación y número de la solicitud europea: **25.03.2015 E 15717677 (7)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 3275149**

(54) Título: **Configuración de plazo de espera de comprobación de operatividad usando mensajes IKE**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.02.2021

(73) Titular/es:

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

(72) Inventor/es:

SEDLACEK, IVO;
ERIKSSON, RIKARD y
KELLER, RALF

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Configuración de plazo de espera de comprobación de operatividad usando mensajes IKE

Campo técnico

Las realizaciones presentadas en el presente documento se refieren a la comprobación de operatividad, y particularmente a métodos, a un equipo de usuario, a un nodo de red central, a programas informáticos y a un producto de programa informático para la configuración de la comprobación de operatividad usando mensajes de intercambio de claves de Internet.

Antecedentes

En las redes de comunicaciones, existe potencialmente el reto de obtener un buen rendimiento y buena capacidad para un protocolo de comunicaciones dado, sus parámetros y el entorno físico en el que se despliegue la red de comunicaciones.

Por ejemplo, un parámetro para proporcionar un buen rendimiento y buena capacidad para un protocolo de comunicaciones dado en una red de comunicaciones es la aptitud de proporcionar comprobación de operatividad eficiente y confiable, también llamada detección de pares muertos, a través, por ejemplo, de redes de acceso no confiables que no son del 3GPP, donde 3GPP es la abreviatura de programa de asociación de tercera generación.

La comprobación de operatividad permite garantizar que ambos extremos de una asociación de seguridad de intercambio de claves de Internet (tal como el intercambio v1 de claves de Internet, de IKEv1, o el intercambio v2 de claves de Internet, de IKEv2) están operativos.

En términos generales, una comprobación de operatividad puede implicar que un punto final de la asociación de seguridad de intercambio de claves de Internet envíe un mensaje de solicitud informativa sin cargas útiles (aparte de la carga útil cifrada vacía requerida por la sintaxis) al que el otro punto final de la asociación de seguridad de intercambio de claves de Internet responde con un mensaje informativo de respuesta. El protocolo de acuerdo con la RFC (Solicitud de comentarios) de la IETF (fuerza de tarea de ingeniería de Internet) 5996 espera que el mensaje de solicitud de información se envíe periódicamente, si el punto final no ha recibido ningún protocolo criptográficamente protegido de seguridad de Internet (IPSec) o paquete de intercambio de claves de Internet como parte de la asociación de seguridad de intercambio de claves de Internet para un plazo de espera dado.

Cuando el intercambio de claves de Internet se utiliza en una red de acceso no confiable, un equipo de usuario y una pasarela de paquetes de datos evolucionada (ePDG) actúan como puntos finales de la asociación de seguridad de intercambio de claves de Internet.

La ePDG puede enviar el mensaje de solicitud informativa para monitorizar la operatividad del equipo de usuario, pero esto requiere temporizadores en la ePDG.

El equipo de usuario puede enviar el mensaje de solicitud informativa para monitorizar la operatividad de la ePDG, pero el operador no tiene control de cuál es el plazo de espera. Por consiguiente, existe una posibilidad limitada para que la red controle el uso real de la comprobación de operatividad del equipo de usuario.

El borrador del 3GPP "Access to the 3GPP Evolved Packet Core via non-3GPP access networks" (acceso al núcleo de paquetes evolucionado de 3GPP mediante redes de acceso que no son del 3GPP) (3GPP TS 24.302 V12.7.0) publicado el 19 de diciembre de 2014 (19-12-2014), XP050906830, divulga que el tiempo de mantener la operatividad de túnel transversal de cortafuegos (FTT KAT) se establece mediante una ePDG que utiliza mensajes IKE CFG_SOLICITUD/CFG_RESPUESTA.

El documento IETF RFC 3706 por Huang G et al.: "A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers" (un método en base a el tráfico para detectar pares muertos de intercambio de claves de Internet (IKE), publicado en febrero de 2004, XP015009486, divulga que los intervalos para mantener la operatividad/las pulsaciones tienen que ser negociados por razones de escalabilidad.

Por consiguiente, existe la necesidad de una comprobación mejorada de la operatividad del equipo de usuario.

Sumario

La presente invención proporciona un método y un equipo de usuario como se especifican en las reivindicaciones.

En general, todos los términos utilizados en las reivindicaciones deben interpretarse de acuerdo con su significado ordinario en el campo técnico, a menos que se defina explícitamente lo contrario en el presente documento. Todas las referencias a "un/una/el/la" elemento, aparato, componente, medio, paso, etc." deben interpretarse abiertamente

como al menos un caso del elemento, aparato, componente, medio, paso, etc., a menos que se indique explícitamente lo contrario. Los pasos de cualquier método divulgado en el presente documento no tienen que realizarse en el orden exacto divulgado, a menos que se indique explícitamente.

Breve descripción de los dibujos

El concepto inventivo se describe ahora, a modo de ejemplo, con referencia a los dibujos que se acompañan, en los que:

La figura 1 es un diagrama esquemático que ilustra una red de comunicaciones de acuerdo con realizaciones.

La figura 2a es un diagrama esquemático que muestra unidades funcionales de un equipo de usuario, UE, de acuerdo con una realización;

La figura 2b es un diagrama esquemático que muestra módulos funcionales de un equipo de usuario de acuerdo con una realización;

La figura 3a es un diagrama esquemático que muestra unidades funcionales de un nodo de red central de acuerdo con una realización;

La figura 3b es un diagrama esquemático que muestra módulos funcionales de un nodo de red central de acuerdo con una realización;

La figura 4 muestra un ejemplo de un producto de programa informático que comprende medios legibles por ordenador de acuerdo con una realización;

Las figuras 5, 6, 7 y 8 son diagramas de flujo de métodos de acuerdo con realizaciones; y

La figura 9 es un diagrama de señalización de acuerdo con una realización; y

La figura 10 es una ilustración esquemática de un período de plazo de espera para el atributo de comprobación de operatividad de acuerdo con una realización.

Descripción detallada

El concepto inventivo se describirá ahora más completamente a continuación con referencia a los dibujos adjuntos, en los que se muestran ciertas realizaciones del concepto inventivo. Sin embargo, este concepto inventivo puede realizarse de muchas formas diferentes y no debe interpretarse como limitado a las realizaciones establecidas en el presente documento; más bien, estas realizaciones se proporcionan a modo de ejemplo para que esta divulgación sea exhaustiva y completa, y transmita completamente el alcance del concepto inventivo al experto en la técnica. Los números que son iguales se refieren a elementos similares a lo largo de toda la descripción. Cualquier paso o característica ilustrada por líneas discontinuas debe considerarse como opcional.

La figura 1 muestra una visión general esquemática de una red 10 de comunicaciones inalámbricas de ejemplo a la que se pueden aplicar las realizaciones presentadas en el presente documento. La red de 10 comunicaciones inalámbricas de la figura 1 está basada en la evolución a largo plazo (LTE). Debe señalarse que los términos "LTE" y "en base a LTE" se usan en el presente documento para comprender redes basadas en LTE presentes y futuras, tales como, por ejemplo, redes LTE avanzadas. Debe apreciarse que, aunque la figura 1 muestra una red de comunicaciones basada en LTE, las realizaciones de ejemplo en el presente documento pueden también utilizarse en conexión con otras redes de comunicaciones inalámbricas, tales como, por ejemplo, el sistema global de comunicación (GSM) o el sistema universal de telecomunicaciones móviles (UMTS), que comprenden nodos y funciones que corresponden a los nodos y funciones de la red de la figura 1.

La red de comunicaciones inalámbricas comprende una o más estaciones base en forma de eNodoB, conectadas operativamente a una pasarela de servicio (SGW), a su vez conectada operativamente a una entidad de gestión de movilidad (MME) y a una pasarela de red de paquetes de datos (PGW), que a su vez está operativamente conectada a una función de reglas de política y carga (PCRF). El eNodoB es un nodo de acceso de radio que interactúa con el equipo 11 de usuario. Los eNodoB de la red forman la denominada red de acceso de radio terrestre universal evolucionada (E-UTRAN) para comunicarse con el equipo de usuario a través de una interfaz aérea, tal como LTE-Uu La red central en LTE se conoce como núcleo evolucionado de paquetes (EPC), y el EPC junto con la E-UTRAN se conoce como sistema evolucionado de paquetes (EPS). La SGW enruta y reenvía los paquetes de datos del usuario a través de la interfaz de S1-U, al mismo tiempo que actúa como el ancla de movilidad para el plano del usuario durante los traspasos entre eNodoB y como el ancla para la movilidad entre LTE y otras tecnologías del proyecto de asociación de tercera generación (3GPP) (terminando la interfaz S4 y retransmitiendo el tráfico entre sistemas 2G/3G y PGW). Para el equipo de usuario en estado inactivo, el SGW termina la trayectoria de datos de enlace descendente y activa la radioseñalización cuando los datos del enlace descendente llegan para el

equipo de usuario, y gestiona y almacena adicionalmente los contextos del equipo de usuario, por ejemplo, parámetros del servicio portador de IP, información de enrutamiento interno de la red. La SGW se comunica con la MME mediante la interfaz S11 y con la PGW mediante la interfaz S5. Además, la SGW puede comunicarse mediante la interfaz S12 con los NodoB de la red de acceso de radio terrestre universal (UTRAN) y con los transceptores de la estación base (BTS) de la red de acceso de radio de GSM EDGE ("velocidades de datos mejoradas para la evolución del GSM") (GERAN).

La MME es responsable del procedimiento de rastreo y radioseñalización del equipo de usuario en modo inactivo, incluidas las retransmisiones. Está involucrada en el proceso de activación/desactivación del portador y también es responsable de elegir la SGW para un equipo de usuario en la conexión inicial y en el momento del traspaso intra-LTE que involucra la reubicación del nodo de red central. Es responsable de autenticar al usuario interactuando con el servidor de abonado doméstico (HSS). La señalización del estrato sin acceso (NAS) termina en la MME y es también responsable de la generación y asignación de identidades temporales al equipo de usuario mediante la interfaz de S1-MME. Comprueba la autorización del equipo de usuario para acampar en la red móvil terrestre pública (PLMN) del proveedor de servicios, y ejecuta las restricciones de itinerancia del equipo de usuario. La MME es el punto de terminación de la red para el cifrado/protección de integridad para la señalización NAS, y maneja la gestión de clave de seguridad. La MME también proporciona la función de plano de control para la movilidad entre las redes de acceso LTE y 2G/3G con la interfaz S3 que termina en la MME desde el nodo servidor de soporte del servicio general de radio de paquetes (SGSN) (SGPR). La MME también termina la interfaz S6a hacia el HSS doméstico para equipos de usuario itinerantes. Además, hay una interfaz S10 configurada para la comunicación entre las MME para la reubicación de la MME y para la transferencia de información de MME a MME.

La PGW proporciona conectividad, al equipo de usuario, a las redes externas de paquetes de datos (PDN) al ser el punto de salida y entrada de tráfico para el equipo de usuario. Un equipo de usuario puede tener conectividad simultánea con más de una PGW para acceder a múltiples PDN. La PGW realiza la aplicación de políticas, el filtrado de paquetes para cada usuario, el soporte de carga, la interceptación legal y la detección de paquetes. Otra función de la PGW es actuar como el ancla para la movilidad entre las tecnologías 3GPP y no 3GPP tales como WiMAX y 3GPP2 (CDMA 1X y EvDO). La interfaz entre la PGW y la red de paquetes de datos, que es, por ejemplo, Internet, es referida como SGi. La red de paquetes de datos puede ser una red de paquetes de datos pública o privada externa del operador o una red de paquetes de datos dentro del operador, por ejemplo para la provisión de servicios de subsistema multimedia de IP (IMS).

La PCRF determina las reglas de política en tiempo real con respecto al equipo de usuario de la red. Esto puede incluir, por ejemplo, la agregación de información en tiempo real desde y hacia la red central y los sistemas operativos de soporte, etc. de la red como para apoyar la creación de reglas y/o como para tomar automáticamente decisiones de política para el equipo de usuario actualmente activo en la red en base a tales reglas o similares. La PCRF proporciona a la PGW tales reglas y/o políticas o similares para que la PGW actúe como una función política y de ejecución de carga (PCEF) mediante la interfaz Gx. La PCRF se comunica adicionalmente con la red de paquetes de datos mediante la interfaz Rx.

Una función principal de la pasarela evolucionada 12 de paquetes de datos (ePDG) es asegurar la transmisión de datos con un equipo de usuario conectado al EPC a través de un acceso no confiable que no sea del 3GPP. Para este fin, la ePDG actúa como un nodo de terminación de túneles de IPsec establecidos con el equipo de usuario.

El servidor de AAA de 3GPP está ubicado dentro de la red móvil terrestre pública doméstica del 3GPP (HPLMN). Realiza funciones de autenticación, autorización y contabilidad (AAA) y puede también actuar como un servidor proxy de AAA. Para el acceso de IP de WLAN del 3GPP, proporciona autorización, ejecución de políticas e información de enrutamiento a la PDG, a la pasarela de acceso de la WLAN y a la red de acceso de la WLAN.

Como se indicó anteriormente, el equipo de usuario puede enviar el mensaje de solicitud de información para monitorizar la operatividad de la ePDG, pero el operador no tiene control de cuál es el plazo de espera. Por consiguiente, existe una posibilidad limitada para que la red controle el uso real de la comprobación de operatividad desde el equipo de usuario.

Puede ser útil habilitar un nodo en la red para configurar el equipo de usuario con respecto a cómo enviar mensajes de solicitud informativos con un plazo de espera especificado por la red. Esto permitiría a la red controlar y adaptar dinámicamente el uso de la comprobación de operatividad, por ejemplo, para evitar una carga de tráfico innecesaria en la red.

Además, puede ser útil requerir que el equipo de usuario envíe una solicitud informativa incluso si el equipo de usuario recibe un paquete de IPSec/ IKEv2 protegido criptográficamente pero no envía ningún paquete de IPSec/IKEv2 protegido criptográficamente como parte de la asociación de seguridad de IKEv2 para el plazo de espera dado. Esto eliminaría el requisito de hacer correr los temporizadores para la comprobación de operatividad en un nodo de red central, como una ePDG, y, en su lugar, recaería en que el equipo de usuario enviara un paquete de IPSec/ IKEv2 protegido criptográficamente dentro del plazo de espera dado (ya sea un paquete de IKEv2/IPSec o la solicitud informativa).

Como se indicó anteriormente, la ePDG puede enviar el mensaje de solicitud de información para monitorizar la operatividad del equipo de usuario, pero esto requiere temporizadores en la ePDG.

Existen problemas similares en de IKEv1, donde el protocolo de detección de pares muertos, de acuerdo con la IETF (fuerza de tarea de ingeniería de Internet), la RFC (solicitud de comentarios) 3706 se utiliza para detectar la comprobación de operatividad del par. En lugar de enviar un mensaje de solicitud de IKEv2 INFORMATIVO, se puede enviar un mensaje ESTÁS-ALLÍ definido por RFC3706. En lugar de enviar un mensaje de respuesta de IKEv2 INFORMATIVO, se puede enviar un mensaje ESTÁS-ALLÍ-ACK definido por RFC3706.

Las realizaciones descritas en el presente documento se refieren, de este modo, a la comprobación de operatividad usando mensajes de intercambio de claves de Internet. Con el fin de obtener tal comprobación de operatividad se proporciona un equipo de usuario, un método realizado por el equipo de usuario, un programa informático que comprende código, por ejemplo en forma de un producto de programa informático que, cuando se ejecuta en una unidad de procesamiento del equipo de usuario, hace que el equipo de usuario realice el método. Con el fin de obtener tal comprobación de operatividad, se proporciona adicionalmente un nodo de red central, tal como una ePDG, un método realizado por el nodo de red central, y un programa informático que comprende código, por ejemplo en forma de un producto de programa informático, que cuando se ejecuta, en una unidad de procesamiento del nodo de la red central, hace que el nodo de la red central realice el método.

La figura 2a ilustra esquemáticamente, en términos de una serie de unidades funcionales, los componentes de un equipo 11 de usuario de acuerdo con una realización. Se proporciona una unidad 21 de procesamiento usando cualquier elemento o combinación de elementos de entre una unidad central de procesamiento (CPU), un multiprocesador, un microcontrolador, un procesador de señal digital (DSP), un circuito integrado específico de aplicación (ASIC), matrices de puerta programables en campo (FPGA), etc., capaz/capaces de ejecutar instrucciones de equipo lógico informático (software) almacenadas en un producto 41a de programa informático (como en la figura 4), por ejemplo en forma de un medio 23 de almacenamiento. De este modo, la unidad 21 de procesamiento está dispuesta por ello para ejecutar métodos como los divulgados en el presente documento. El medio de almacenamiento 23 también puede comprender almacenamiento persistente, que, por ejemplo, puede ser cualquier elemento o combinación de elementos de entre una memoria magnética, una memoria óptica, una memoria de estado sólido o incluso una memoria montada remotamente. El equipo de usuario puede comprender adicionalmente una interfaz 22 de comunicaciones para comunicaciones con nodos, dispositivos, equipo de usuario y entidades lógicas de la red. Como tal, la interfaz 22 de comunicaciones puede comprender uno o más transmisores y receptores, que comprenden componentes analógicos y digitales y una cantidad adecuada de antenas para comunicaciones inalámbricas. La unidad 21 de procesamiento controla el funcionamiento general del equipo de usuario, por ejemplo enviando datos y señales de control a la interfaz 22 de comunicaciones y al medio 23 de almacenamiento, recibiendo datos e informes de la interfaz 22 de comunicaciones y recuperando datos e instrucciones del medio 23 de almacenamiento. Otros componentes, así como la funcionalidad relacionada, del equipo de usuario se omiten para no eclipsar los conceptos presentados en el presente documento. En términos generales, el equipo de usuario puede ser un dispositivo inalámbrico, tal como un dispositivo inalámbrico portátil, y puede proporcionarse como una estación móvil, un teléfono móvil, un teléfono, un teléfono de bucle local inalámbrico, un teléfono inteligente, un ordenador portátil, un ordenador de tableta, un módem inalámbrico, un sensor o un dispositivo de Internet de las cosas.

La figura 2b ilustra esquemáticamente, en términos de una serie de módulos funcionales, los componentes de un equipo 11 de usuario de acuerdo con una realización. El equipo de usuario de la figura 2b comprende una serie de módulos funcionales; un primer módulo 21a de transmisión configurado para actuar por debajo del paso S102, y un segundo módulo de recepción 21b configurado para actuar por debajo del paso S104. El equipo 11 de usuario de la figura 2b puede comprender adicionalmente una serie de módulos funcionales opcionales, tales como cualesquiera de entre un módulo 21c de comprobación de operatividad, configurado para actuar por debajo del paso S106, un módulo 21d de solicitud de transmisión configurado para actuar por debajo del paso S108, un módulo 21e de determinación de fallo configurado para actuar por debajo del paso S110, y un módulo 21f de descarte configurado para actuar por debajo de los pasos S112 y S114. La funcionalidad de cada módulo funcional 21a-e se describirá adicionalmente a continuación en el contexto en el cual se puedan usar los módulos funcionales 21a-e. En términos generales, cada módulo funcional 21a-e puede implantarse en equipo físico informático (hardware) o en equipo lógico informático (software). Preferiblemente, la unidad 21 de procesamiento puede implantar uno o más o todos los módulos funcionales 21a-e, posiblemente en cooperación con las unidades funcionales 22 y/o 23. De este modo, la unidad 21 de procesamiento puede disponerse desde el medio 23 de almacenamiento para obtener instrucciones como proporcionadas por un módulo funcional 21a-e y ejecutar estas instrucciones, realizando por ello los pasos que se divulgarán a continuación.

La figura 3a ilustra esquemáticamente, en términos de una serie de unidades funcionales, los componentes de un nodo 12 de red central de acuerdo con una realización. Se proporciona una unidad 31 de procesamiento que usa cualquier elemento o combinación de elementos de entre una adecuada unidad central de procesamiento (CPU), un multiprocesador, un microcontrolador, un procesador de señal digital (DSP), un circuito integrado específico de aplicación (ASIC), matrices de puerta programables en campo (FPGA), etc., capaz/capaces de ejecutar

instrucciones de software almacenadas en un producto 41a de programa informático (como en la figura 4), por ejemplo en forma de un medio 23 de almacenamiento. De este modo, la unidad 31 de procesamiento está dispuesta por ello para ejecutar métodos como los divulgados en el presente documento. El medio 33 de almacenamiento puede también comprender almacenamiento persistente, el cual puede ser, por ejemplo, cualquier elemento o combinación de elementos de entre memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada remotamente. El nodo 12 de red central puede comprender adicionalmente una interfaz 32 de comunicaciones para comunicaciones con nodos, dispositivos, equipo de usuario y entidades lógicas de la red. Como tal, la interfaz 32 de comunicaciones puede comprender uno o más transmisores y receptores, que comprenden componentes analógicos y digitales y una cantidad adecuada de antenas para comunicaciones inalámbricas y/o puertos para comunicaciones por cable. La unidad 31 de procesamiento controla el funcionamiento general del nodo 12 de red central, por ejemplo enviando datos y señales de control a la interfaz 32 de comunicaciones y al medio 33 de almacenamiento, recibiendo datos e informes de la interfaz 32 de comunicaciones, y recuperando datos e instrucciones del medio 33 de almacenamiento. Otros componentes, así como su funcionalidad relacionada, del nodo 12 de red central se omiten con el fin de no eclipsar los conceptos presentados en el presente documento. De acuerdo con una realización, el nodo de red central es una pasarela evolucionada de paquetes de datos (ePDG).

La figura 3b ilustra esquemáticamente, en términos de una serie de módulos funcionales, los componentes de un nodo 12 de red central de acuerdo con una realización. El nodo 12 de red central de la figura 3b comprende una serie de módulos funcionales; un primer módulo 31a de recepción configurado para actuar por debajo del paso S202, y un segundo módulo 31b de transmisión configurado para actuar por debajo del paso S210. El nodo 12 de red central de la figura 3b puede comprender adicionalmente una serie de módulos funcionales opcionales, tales como cualquiera de entre un módulo 31c de indicación, configurado para actuar por debajo del paso S206, un módulo 31d de recibir valor, configurado para actuar por debajo del paso S208, un módulo 31e de solicitud de recepción, configurado para actuar por debajo del paso S212, un módulo 31f de respuesta de transmisión, configurado para actuar por debajo del paso S214, y un módulo 31g de determinación, configurado para actuar por debajo del paso S204. La funcionalidad de cada módulo funcional 31a-g se describirá adicionalmente más adelante en el contexto en el cual se puedan usar los módulos funcionales 31a-g. En términos generales, cada módulo funcional 31a-g puede implantarse en hardware o en software. Preferiblemente, la unidad de procesamiento 31 puede implantar uno o más o todos los módulos funcionales 31a-g, posiblemente en cooperación con las unidades funcionales 32 y/o 33. De este modo, la unidad 31 de procesamiento puede disponerse desde el medio 33 de almacenamiento para obtener instrucciones como proporcionadas por un módulo funcional 31a-g y ejecutar estas instrucciones, realizando por ello cuales quiera pasos como se divulgará de aquí en adelante.

La figura 4 muestra un ejemplo de un producto 41a, 41b de programa informático que comprende medios 43 legibles por ordenador. En estos medios 43 legibles por ordenador, se puede almacenar un programa informático 42a, programa informático 42a, el cual, puede hacer que a la unidad 21 de procesamiento se acoplen entidades y dispositivos operativamente, tales como la interfaz 22 de comunicaciones y el medio 23 de almacenamiento, para ejecutar métodos de acuerdo con las realizaciones descritas en el presente documento. El programa informático 42a y/o el producto 41a de programa informático puede/n proporcionar, de este modo, medios para realizar cualesquiera pasos del equipo de usuario como se describe en el presente documento. En estos medios 43 legibles por ordenador se puede almacenar un programa informático 42b, programa informático 42b, el cual, puede hacer que la unidad de procesamiento 31 y las entidades y dispositivos acoplados operativamente a ella, tales como la interfaz 32 de comunicaciones y el medio 33 de almacenamiento, ejecuten métodos de acuerdo con realizaciones descritas en el presente documento. El programa informático 42b y/o el producto de programa informático 41b pueden, de este modo, proporcionar medios para realizar cualesquiera pasos del nodo de red central como se describe en el presente documento.

En el ejemplo de la figura 4, el producto 41a, 41b de programa informático se ilustra como un disco óptico, tal como un CD (disco compacto) o un DVD (disco versátil digital) o un disco Blu-Ray. El producto 41a, 41b de programa informático también podría incorporarse como una memoria, tal como una memoria de acceso aleatorio (RAM), una memoria de sólo lectura (ROM), una memoria de sólo lectura programable borrable (EPROM) o una memoria programable borrable eléctricamente memoria de sólo lectura (EEPROM), y, más particularmente, como medio de almacenamiento no volátil de un dispositivo en una memoria externa tal como una memoria USB (bus de serie universal) o una memoria Flash, tal como una memoria Flash compacta. De este modo, mientras el programa informático 42a, 42b se muestra en el presente documento esquemáticamente como una pista en el disco óptico representado, el programa informático 42a, 42b puede almacenarse de cualquier manera que sea adecuada para el producto 41a, 41b de programa informático.

Las figuras 5 y 6 son diagramas de flujo que ilustran realizaciones de métodos para la configuración de la comprobación de operatividad utilizando mensajes de intercambio de claves de Internet según los realiza el equipo 11 de usuario. Las figuras 7 y 8 son diagramas de flujo que ilustran realizaciones de métodos para la configuración de la comprobación de operatividad usando mensajes de intercambio de claves de Internet según los realiza el nodo 11 de red central. Los métodos se proporcionan ventajosamente como programas informáticos 42a, 42b.

Se hace referencia ahora a la figura 5 que ilustra un método para la configuración de la comprobación de

operatividad usando mensajes de intercambio de claves de Internet según los realiza el equipo 11 de usuario de acuerdo con una realización.

El equipo de usuario está configurado para, en un paso S102, transmitir, a un nodo de red central, un primer mensaje de intercambio de claves de Internet. El primer mensaje de intercambio de claves de Internet comprende un atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad.

Como se describirá adicionalmente más adelante, se asume que este mensaje es recibido por el nodo de red central, el cual, a su vez, responde a este mensaje. Por consiguiente, el equipo de usuario está configurado para, en un paso S104, recibir, desde el nodo de red central, un segundo mensaje de intercambio de claves de Internet. El segundo mensaje de intercambio de claves de Internet comprende un atributo de configuración que indica un período de plazo de espera para la comprobación de operatividad.

Ahora se divulgarán realizaciones relacionadas para más detalle de la comprobación de operatividad usando mensajes de intercambio de claves de Internet según los realiza el equipo 11 de usuario.

Puede haber diferentes maneras de proporcionar el primer mensaje de intercambio de claves de Internet y el segundo mensaje de intercambio de claves de Internet. Las realizaciones relacionadas con esto se describirán, a su vez, ahora. De acuerdo con una realización, el primer mensaje de intercambio de claves de Internet es un mensaje de solicitud de IKE_AUT. De acuerdo con una realización, el segundo mensaje de intercambio de claves de Internet es un mensaje de respuesta de IKE_AUT.

Puede haber diferentes maneras de proporcionar el atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad y el atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad. Las realizaciones relacionadas con esto se describirán, a su vez, ahora. De acuerdo con una realización, el atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad es un período de plazo de espera para el atributo de comprobación de operatividad con el campo de longitud establecido en cero. De acuerdo con una realización, el atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad se proporciona en una carga útil de configuración de CFG_SOLICITUD. De acuerdo con una realización, el atributo de configuración que indica un período de plazo de espera para dicha comprobación de operatividad es un período de plazo de espera para el atributo de comprobación de operatividad con un campo de período de plazo de espera. De acuerdo con una realización, el atributo de configuración que indica un período de plazo de espera para dicha comprobación de operatividad se proporciona en una carga útil de configuración de CFG_ RESPUESTA.

El atributo de configuración que indica un período de plazo de espera para la comprobación de operatividad se puede basar en una política local. Alternativamente, el atributo de configuración que indica un período de plazo de espera para la comprobación de operatividad se basa en información de un sistema de configuración o de un sistema de gestión. Se proporcionarán más detalles al respecto más adelante.

Se hace referencia ahora a la figura 6, que ilustra métodos para la configuración de la comprobación de operatividad utilizando mensajes de intercambio de claves de Internet según lo realizado por el equipo 11 de usuario de acuerdo con realizaciones adicionales.

El primer mensaje de intercambio de claves de Internet puede transmitirse en un mensaje de intercambio de claves de Internet de versión 2 (de IKEv2), y el segundo mensaje de intercambio de claves de Internet puede recibirse en un mensaje de IKEv2. Con más detalle, en una realización, si el UE soporta la competencia de ser configurado para la comprobación de operatividad, el UE incluye un atributo de configuración de IKEv2 que indica la competencia de ser configurado para la comprobación de operatividad en un mensaje de IKEv2 enviado al nodo 12 de red central. En esta realización, si el UE soporta la competencia de ser configurado para la comprobación de operatividad y el atributo de configuración de IKEv2 que indica el período de plazo de espera para la comprobación de operatividad en el mensaje de IKEv2 recibido, entonces el UE realiza la comprobación de operatividad de acuerdo con el valor de este atributo configuración de IKEv2. Por consiguiente, el equipo de usuario puede configurarse para, en un paso S106, realizar la comprobación de operatividad de acuerdo con el atributo de configuración que indica un período de plazo de espera para la comprobación de operatividad.

En una realización, el atributo de configuración de IKEv2 comprende adicionalmente una indicación de si se requiere que el UE envíe una solicitud de IKEv2 INFORMATIVO también cuando el UE recibe un protocolo de seguridad de Internet protegido criptográficamente (IPSec) o un paquete de IKEv2 durante el plazo de espera dado pero que no se envíe ningún paquete de IPSec/de IKEv2 protegido criptográficamente como parte de la asociación de seguridad de IKEv2 para el plazo de espera dado. El atributo de configuración del segundo mensaje de intercambio de claves de Internet puede comprender una indicación de si se requiere o no que el equipo de usuario transmita una solicitud informativa, también de si el equipo de usuario recibe al menos un elemento de entre un paquete de IPSec protegido criptográficamente y un paquete de intercambio de claves de Internet criptográficamente durante el plazo de espera.

La solicitud informativa puede estar incluida en el mensaje de solicitud de IKEv2 INFORMATIVO.

La comprobación de operatividad puede ser parte de una asociación de seguridad de intercambio de claves de Internet, y el equipo de usuario no transmite ningún paquete de IPSec protegido criptográficamente ni paquete de intercambio de claves de Internet criptográficamente como parte de la asociación de seguridad de intercambio de claves de Internet durante dicho período de plazo de espera. Por consiguiente, el equipo de usuario puede configurarse para, en un paso S108, transmitir una solicitud informativa sin carga útil si se incluye un período de plazo de espera para el atributo de comprobación de operatividad en el atributo de configuración recibido indicando un período de plazo de espera para dicha comprobación de operatividad, y en ausencia de recibir un paquete de IPSec protegido criptográficamente o un paquete de intercambio de claves de Internet criptográficamente durante el período de plazo de espera para la comprobación de operatividad.

En las realizaciones en las que la comprobación de operatividad es parte de una asociación de seguridad de intercambio de claves de Internet, el equipo de usuario está configurado para, en ausencia de recibir una respuesta informativa en respuesta a la solicitud informativa transmitida sin carga útil, en un paso S110, determinar un fallo de la asociación de seguridad de intercambio de claves de Internet. El equipo de usuario está configurado adicionalmente para, en un paso S112, descartar cualquier información de estado asociada con la asociación de seguridad de intercambio de claves de Internet; y/o, en un paso S114, descartar cualquier asociación de seguridad de IPSec negociada utilizando la asociación de seguridad de intercambio de claves de Internet.

En una realización, la versión 1 de intercambio de claves de Internet (de IKEvl) se usa junto con el protocolo de detección de pares muertos (RFC3706). Es decir, en lugar de utilizar los atributos de configuración de IKEv2 como se describió anteriormente, se utilizan nuevos atributos de IKEv1 que llevan la información. Es decir que, de acuerdo con una realización, el primer mensaje de intercambio de claves de Internet se transmite en un mensaje de IKEv1, y el segundo mensaje de intercambio de claves de Internet se recibe en un mensaje de IKEv1.

Además, en lugar de enviar un mensaje de solicitud de IKEv2 INFORMATIVO, se envía un mensaje ESTÁS-ALLÍ definido por RFC3706, y en lugar de enviar un mensaje de respuesta IKEv2 INFORMATIVO, se envía un mensaje ESTÁS-ALLÍ-ACK definido por RFC3706. Es decir que, de acuerdo con una realización, el atributo de configuración del segundo mensaje de intercambio de claves de Internet comprende una indicación de si se requiere que el equipo de usuario transmita un mensaje de estás allí o no, también si el equipo de usuario recibe al menos un elemento de entre un paquete de IPSec criptográficamente protegido y un paquete de intercambio de claves de Internet criptográficamente durante el período de plazo de espera. El mensaje de estás allí puede incluirse en un mensaje de ESTÁS-ALLÍ definido por RFC3706.

Se hace referencia ahora a la figura 7 que ilustra un método para la configuración de la comprobación de operatividad usando mensajes de intercambio de claves de Internet según lo realiza el nodo 12 de red central de acuerdo con una realización.

Como se indicó anteriormente, el equipo 11 de usuario en el paso S102 transmite un mensaje a un nodo 12 de red central. Se asume, con el fin de divulgar el concepto inventivo divulgado en el presente documento, que este mensaje es recibido por un nodo 12 de red central. Por consiguiente, el nodo de red central está configurado para, en un paso S202, recibir, desde un equipo 11 de usuario, un primer mensaje de intercambio de claves de Internet que comprende un atributo de configuración que indica soporte para recibir un período de plazo de espera para comprobación de operatividad. El nodo 12 de red central responde a este mensaje recibido. En particular, el nodo de red central está configurado para, en un paso S210, transmitir, al equipo de usuario, un segundo mensaje de intercambio de claves de Internet que comprende un atributo de configuración que indica un período de plazo de espera para la comprobación de operatividad.

Ahora se describirán realizaciones relacionadas con detalles adicionales de la comprobación de operatividad que usan mensajes de intercambio de claves de Internet según son realizadas por el nodo 12 de red central.

Se hace referencia ahora a la figura 8 que ilustra métodos para la configuración de la comprobación de operatividad usando mensajes de intercambio de claves de Internet según son realizados por el nodo 12 de red central de acuerdo con realizaciones adicionales.

En una realización, si el nodo 12 de red central soporta la competencia de ser capaz de configurar el equipo de usuario para la comprobación de operatividad y se incluye en el mensaje de IKEv2 recibido un atributo de configuración de IKEv2 que indique la competencia de estar configurado para la comprobación de operatividad, entonces el nodo 12 de red central incluirá un atributo de configuración de IKEv2 que indique el período de plazo de espera para la comprobación de operatividad en un mensaje de IKEv2 enviado al equipo de usuario.

Puede haber diferentes maneras para que el nodo 12 de red central determine el contenido del atributo de configuración indicando un período de plazo de espera. Se describirán ahora, a su vez, diferentes realizaciones relacionadas con ellas.

Por ejemplo, el nodo 12 de red central puede determinar el contenido del atributo de configuración que indica un período de plazo de espera en base a una política local. Por consiguiente, de acuerdo con una realización, el nodo de red central está configurado para, en un paso S204, determinar, en base a una política local, un valor del período de plazo de espera en el atributo de configuración que indica un período de plazo de espera para la comprobación de operatividad.

Por ejemplo, el nodo 12 de red central puede determinar el contenido del atributo de configuración que indica un período de plazo de espera en base a la información de otra configuración o de otro sistema de gestión.

Por ejemplo, el nodo 12 de red central puede determinar el contenido del atributo de configuración que indica un período de plazo de espera indicando a una PGW que el nodo de red central soporta la competencia de ser capaz de configurar el equipo de usuario para la comprobación de operatividad y dónde la PGW proporciona, por ejemplo mediante GTP o PMIP, un valor del atributo de configuración al nodo de red central. Por consiguiente, de acuerdo con una realización, el nodo de red central está configurado para, en un paso S206, indicar a una pasarela de red de paquetes de datos, PGW, que el nodo de red central soporta recibir un período de plazo de espera para dicha comprobación de operatividad. El nodo de red central puede entonces configurarse para, en un paso S208, recibir, de la PGW, un valor del atributo de configuración que indica un período de plazo de espera para la comprobación de operatividad. El valor puede recibirse mediante un protocolo general de tunelización de servicios de radio por paquetes (GTP).

Alternativamente, el valor puede recibirse mediante un protocolo de Internet móvil proxy (PMIP).

A continuación, se describirán ejemplos adicionales del atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad. Por ejemplo, el atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad puede ser un período de plazo de espera para el atributo de comprobación de operatividad con un campo de longitud establecido en cero. Por ejemplo, el atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad se puede proporcionar en una carga útil de configuración CFG_SOLICITUD. Por ejemplo, el atributo de configuración que indica un período de plazo de espera para la comprobación de operatividad puede ser un período de plazo de espera para el atributo de comprobación de operatividad con un campo de período de plazo de espera. Por ejemplo, el atributo de configuración que indica un período de plazo de espera para la comprobación de operatividad se puede proporcionar en una carga útil de configuración CFG_RESPUESTA.

Como se indicó anteriormente para las realizaciones relacionadas con el equipo de usuario, en una realización los mensajes se basan en IKEv1 usada junto con el protocolo de detección de pares muertos (RFC3706). Tal realización es igualmente aplicable al nodo de red central. Por consiguiente, en lugar de usar atributos de configuración de IKEv2 como se describe en el presente documento, se usan nuevos atributos de IKEv1 que llevan la información. En lugar de enviar/recibir un mensaje de solicitud de IKEv2 INFORMATIVO, se puede enviar/recibir un mensaje de ESTÁS-ALLÍ definido por RFC3706. En lugar de enviar/recibir un mensaje de respuesta de IKEv2 INFORMATIVO, se puede enviar/recibir un mensaje de ESTÁS-ALLÍ-ACK definido por RFC3706. Por consiguiente, de acuerdo con una realización, el nodo de red central está configurado para, en un paso S212, recibir un mensaje informativo de solicitud del equipo de usuario; y en respuesta a él, en un paso S214, transmitir un mensaje informativo de respuesta al equipo de usuario. El mensaje informativo de respuesta puede incluirse en un mensaje de respuesta de IKEv2 INFORMATIVO. El mensaje informativo de respuesta puede incluirse en un mensaje de ESTÁS-ALLÍ-ACK definido por RFC3706.

Una realización particular para la configuración de la comprobación de operatividad utilizando mensajes de intercambio de claves de Internet en base a al menos algunas de las realizaciones descritas anteriormente, y en 3GPP TS 24.302, versión 13.0.0, sección 7.2.2 y 7.4.1., será ahora divulgada en detalle. La realización particular se basa en establecer un túnel. En esta realización, la funcionalidad del nodo de red central se proporciona en una ePDG.

Una vez que se ha seleccionado la ePDG, el equipo de usuario inicia un procedimiento de establecimiento de túnel de IPsec usando el protocolo de IKEv2 de acuerdo con IETF RFC 5996 y con 3GPP TS 33.402, por ejemplo versión 12.5.0, sección 8.2.2.

El equipo de usuario envía un mensaje de solicitud de IKE_SA_INIC a la ePDG seleccionada con el fin de configurar una asociación de seguridad de IKEv2. Al recibir una respuesta de IKE_SA_INIC, el equipo de usuario envía un mensaje de solicitud de IKE_AUT a la ePDG, incluido el tipo de dirección de IP (dirección de IPv4 o prefijo de IPv6 o ambos), que debe configurarse en una carga útil de configuración de IKEv2 CFG_SOLICITUD. Si el equipo de usuario solicita tanto la dirección de IPv4 como el prefijo de IPv6, el equipo de usuario envía dos atributos de configuración en la carga útil de configuración CFG_SOLICITUD, un atributo de configuración para la dirección de IPv4 y un atributo de configuración para el prefijo de IPv6. El mensaje de solicitud de IKE_AUT comprende en la carga útil de "IDr" el APN, y en la carga útil de "IDi" el NAI. El equipo de usuario indica una solicitud para la APN predeterminada al omitir la carga útil de IDr, que está de acuerdo con el protocolo de IKEv2 de acuerdo con IETF RFC 5996. El mensaje de solicitud de IKE_AUT puede incluir, en una carga útil de notificación, una indicación de

que el denominado MOBIKE es soportado por el equipo de usuario. El equipo de usuario también puede incluir el atributo de DNS_IP6_INTERNO o de DNS_IP4_INTERNO en la carga útil de configuración CFG_SOLICITUD. El equipo de usuario puede obtener cero o más servidores de DNS direccionados en la carga útil de CFG_RESPUESTA de acuerdo con IETF RFC 5996. El equipo de usuario puede también incluir el atributo P-CSCF_IP6_DIRECCIÓN, el atributo P-CSCF_IP4_DIRECCIÓN o ambos en la carga útil de configuración CFG_SOLICITUD. El equipo de usuario puede obtener cero o más direcciones de servidor de P-CSCF en la carga útil de configuración CFG_RESPUESTA, como se especifica en IETF draft-gundavelli-ipsecme-3gpp-ims-options. El equipo de usuario también puede incluir el atributo de TIEMPODEESPERA_PARA_COMPROBACIÓN_OPERATIVIDAD, como se divulga en el presente documento, que indica el soporte del período de plazo de espera de recepción para la comprobación de operatividad en la carga útil de configuración CFG_SOLICITUD. Si el atributo de TIEMPODEESPERA_PARA_COMPROBACIÓN_OPERATIVIDAD como se describe en el presente documento (es decir, indicando el período de plazo de espera para la comprobación de operatividad) se incluye en la carga útil de configuración CFG_RESPUESTA, el equipo de usuario realiza comprobaciones de operatividad del túnel.

Durante el establecimiento de la asociación de seguridad y autenticación de IKEv2, si el equipo de usuario soporta una indicación explícita sobre los protocolos de movilidad soportados, el equipo de usuario proporciona una indicación.

Durante la autenticación de IKEv2 y el establecimiento del túnel para la conexión inicial, el equipo de usuario proporciona una indicación sobre el tipo de conexión, que indica la conexión inicial. Para indicar la conexión debido a la conexión inicial, el equipo de usuario incluye o bien el atributo de DIRECCIÓN_IP4_INTERNA o bien el de DIRECCIÓN_IP6_INTERNA o ambos en la carga útil de configuración CFG_SOLICITUD dentro del mensaje de solicitud de IKE_AUT. El DIRECCIÓN_IP4_INTERNA no comprende ningún valor, y el campo de longitud se establece en 0 (es decir, en cero). El DIRECCIÓN_IP6_INTERNA no comprende ningún valor, y el campo de longitud se establece en 0 (es decir, en cero).

Durante la autenticación de IKEv2 y el establecimiento del túnel para el traspaso, un equipo de usuario que no soporta la preservación de la dirección de IP para NBM indica la conexión inicial, como se describió anteriormente.

Durante el establecimiento de la asociación de seguridad y de la autenticación de IKEv2 para el traspaso, un equipo de usuario, que soporta la preservación de la dirección de IP para NBM, proporciona una indicación sobre el tipo de conexión, que indica la conexión de traspaso. Para indicar la conexión debida al traspaso, el equipo de usuario incluye la información de la dirección de origen previamente asignada durante el establecimiento del túnel de IPSec. Dependiendo de la versión del IP, el equipo de usuario incluye o bien el atributo de DIRECCIÓN_IP4_INTERNA o bien el de DIRECCIÓN_IP6_INTERNA o ambos en la carga útil de configuración CFG_SOLICITUD dentro del mensaje de solicitud de IKE_AUT para indicar la información de la dirección de origen que está de acuerdo con el protocolo de IKEv2. El equipo de usuario soporta IPSec ESP con el fin de proporcionar túneles seguros entre el equipo de usuario y la ePDG.

El equipo de usuario puede soportar múltiples intercambios de autenticación en el protocolo de IKEv2 con el fin de soportar la autenticación y la autorización con un servidor externo de AAA que permita que el UE soporte el procedimiento de autenticación PAP, o el procedimiento de autenticación CHAP, o ambos.

Si se usa NBM y el equipo de usuario desea acceder a una PDN externa y, por lo tanto, necesita realizar autenticación y autorización con un servidor de AAA externo, el equipo de usuario realiza lo siguiente:

Si la respuesta de IKE_SA_INIC contiene una carga útil de notificación de "MULTIPLE_AUT_SOPORTADA", entonces el equipo de usuario incluye una carga útil de notificación de "MULTIPLE_AUT_SOPORTADA" en una solicitud de IKE_AUT y realiza pasos adicionales de autenticación.

Si la respuesta de IKE_SA_INIC no contiene una carga útil de notificación de "MULTIPLE_AUT_SOPORTADA", entonces el equipo de usuario realiza la desconexión iniciada por el equipo de usuario. La acción subsiguiente del equipo de usuario depende de la implantación (por ejemplo, dependiendo de si se selecciona o no una nueva ePDG).

Si se utiliza NBM y el equipo de usuario recibe de la ePDG un mensaje de respuesta de IKE_AUT que contiene una carga útil de notificación con un tipo PDN_CONEXIÓN_RECHAZO de mensaje privado de notificación que incluye una información de dirección de IP en el campo de datos de notificación, el equipo de usuario no intenta restablecer esta conexión de PDN mientras esté conectado operativamente a la ePDG actual, y el equipo de usuario cierra los estados de asociación de seguridad de IKEv2 relacionados.

Si se utiliza NBM y el equipo de usuario recibe de la ePDG un mensaje de respuesta de IKE_AUT que contiene una carga útil de notificación con un tipo PDN_CONEXIÓN_RECHAZO de mensaje privado de notificación y ningún campo de datos de notificación, el equipo de usuario no intenta establecer conexiones de PDN adicionales con este APN mientras esté conectado a la ePDG actual. El equipo de usuario cierra los

estados de asociación de seguridad de IKEv2 relacionados. Subsiguientemente, el equipo de usuario puede intentar establecer conexiones de PDN adicionales con el APN dado si se liberan una o más conexiones existentes de PDN con el APN dado. Mientras está conectado operativamente a la ePDG actual, si esta conexión de PDN es la primera conexión de PDN para la APN dada, el equipo de usuario no intenta establecer una conexión de PDN a la APN dada.

Si se utiliza NBM y el equipo de usuario recibe de la ePDG un mensaje de respuesta de IKE_AUT que comprende una carga útil de notificación con un tipo MAX_CONEXIÓN_ALCANZADA de mensaje privado de notificación, el equipo de usuario no intenta establecer ninguna conexión de PDN adicional mientras esté conectado operativamente a la ePDG actual. El equipo de usuario cierra los estados de asociación de seguridad de IKEv2 relacionados. Subsiguientemente, el equipo de usuario puede intentar establecer conexiones de PDN adicionales si se liberan una o más conexiones de PDN existentes.

Después de la autenticación exitosa con el servidor de AAA del 3GPP, el equipo de usuario recibe de la ePDG un mensaje de respuesta de IKE_AUT que comprende una única carga útil de configuración CFG_ RESPUESTA que incluye la información de la dirección de IP remota asignada (dirección de IPv4 o prefijo de IPv6). Dependiendo del mecanismo de gestión de movilidad de IP utilizado, se pueden diferenciar los siguientes casos:

Si se utiliza DSMIPv6 para la gestión de movilidad de IP, el equipo de usuario configura una dirección remota de IP en base a la información de la dirección de IP contenida en el atributo de DIRECCIÓN_IP4_INTERNA o de SUBRED_IP6_INTERNA de la carga útil de configuración CFG_RESPUESTA. El equipo de usuario utiliza la dirección remota de IP como dirección a cuidar para contactar con el HA (agente de origen).

Si se utiliza NBM para la gestión de la movilidad de IP y el equipo de usuario realiza una conexión inicial, el equipo de usuario configura una dirección de origen en base a la información de la dirección de la carga útil de configuración CFG_RESPUESTA. De lo contrario, si se utiliza NBM y el equipo de usuario realiza una conexión de traspaso, el equipo de usuario continúa usando su dirección de IP configurada antes del traspaso, si la información de la dirección proporcionada en la carga útil de configuración CFG_RESPUESTA coincide con la dirección de IP del equipo de usuario que se configura antes del traspaso. Si la dirección de IP del equipo de usuario no coincide con la información de la dirección de la carga útil de configuración CFG_RESPUESTA, el equipo de usuario configura una nueva dirección de origen en base a la información de la dirección de IP contenida en el atributo de DIRECCIÓN_IP4_INTERNA o de SUBRED_IP6_INTERNA de la carga útil de configuración CFG_RESPUESTA. En este último caso, la preservación de la dirección de IP no es posible.

Si el equipo de usuario soporta DSMIPv6, el equipo de usuario puede solicitar la dirección o las direcciones de IP del HA, al incluir una carga útil correspondiente de configuración CFG_SOLICITUD que contenga un atributo de DIRECCIÓN_AGENTE_ORIGEN. Las direcciones de IP del HA solicitadas en este atributo de son para el APN para el que está establecido el túnel de IPsec con la ePDG. En la CFG_SOLICITUD, el equipo de usuario establece respectivamente el campo de dirección de IPv6 y el campo de dirección de IPv4 opcional del atributo de DIRECCIÓN_AGENTE_ORIGEN en 0::0 y 0.0.0.0. Si el equipo de usuario no puede obtener las direcciones de IP del HA mediante la señalización de IKEv2, el equipo de usuario utiliza el descubrimiento de la dirección del agente de origen.

En caso de que el equipo de usuario quiera establecer múltiples conexiones de PDN, y si el equipo de usuario usa DSMIPv6 para la gestión de movilidad, el equipo de usuario usa DNS para descubrir la dirección o las direcciones de IP del HA para las conexiones de PDN adicionales después de que se estableciera la asociación de seguridad de IKEv2 para la ePDG.

Si el atributo de PERIODO_TIEMPODEESPERA_PARA_COMPROBACIÓN_OPERATIVIDAD que indica el período de plazo de espera para la comprobación de operatividad fue incluido en una carga útil de configuración CFG_RESPUESTA y el equipo de usuario no ha recibido ningún mensaje de IKEv2 o de IPSec protegido criptográficamente durante el período de espera para la comprobación de operatividad indicada en el atributo de PERIODO_TIEMPODEESPERA_PARA_COMPROBACIÓN_OPERATIVIDAD del usuario, el equipo de usuario envía una solicitud INFORMATIVA sin cargas útiles. Si no se recibe una respuesta INFORMATIVA a la solicitud INFORMATIVA, el equipo de usuario considera que la asociación de seguridad de IKEv2 ha fallado, y descarta todos los estados asociados con la asociación de seguridad de IKEv2 y con cualesquiera asociaciones de seguridad de IPSec que habían sido negociados utilizando la asociación de seguridad de IKE.

Al recibir un mensaje de solicitud de IKE_AUT del equipo de usuario solicitando el establecimiento de un túnel, la ePDG procede con una autenticación y una autorización, de lo cual se ofrecen detalles adicionales a continuación.

Durante el procedimiento de autenticación y autorización del equipo de usuario, el servidor de AAA del 3GPP

proporciona a la ePDG una indicación sobre el mecanismo de movilidad de IP seleccionado.

La ePDG procede con la finalización de la configuración del túnel de IPsec y se retransmite en la carga útil de configuración de IKEv2 (CFG_RESPUESTA) del mensaje final de respuesta de IKE_AUT de la información de la dirección de IP remota al equipo de usuario. Si se utiliza NBM como mecanismo de movilidad de IP, la ePDG asigna o bien una dirección de IPv4 o bien un prefijo de red doméstica de IPv6 o ambos al equipo de usuario mediante una única carga útil de configuración CFG_RESPUESTA. Si el equipo de usuario solicita tanto la dirección de IPv4 como el prefijo IPv6, pero la ePDG sólo asigna una dirección de IPv4 o un prefijo de red doméstica de IPv6 debido a restricciones de suscripción o a preferencia de red, la ePDG incluye la información de la dirección de IP remota asignada (dirección de IPv4 o prefijo IPv6) mediante una única carga útil de configuración CFG_RESPUESTA. Si la ePDG asigna una dirección de IPv4, la CFG_RESPUESTA comprende el atributo de DIRECCIÓN_IP4_INTERNA. Si la ePDG asigna un prefijo de red doméstica de IPv6, la CFG_RESPUESTA comprende el atributo de configuración de SUBRED_IP6_INTERNA. La ePDG obtiene la dirección de IPv4 y/o el prefijo de red doméstica de IPv6 de la GW de PDN (PGW). Si el equipo de usuario no proporciona un APN a la ePDG durante el establecimiento del túnel, la ePDG incluye el APN por defecto en la carga útil de IDr del mensaje de respuesta de IKE_AUT. Si el equipo de usuario incluía el DNS_IP6_INTERNO o el DNS_IP4_INTERNO en la carga útil de configuración CFG_SOLICITUD, la ePDG incluye el mismo atributo en la carga útil de configuración CFG_RESPUESTA que incluye cero o más direcciones de servidor del DNS, de acuerdo con IETF RFC 5996. Si el equipo de usuario incluye el atributo de P-CSCF_IP6_DIRECCIÓN, el atributo de P-CSCF_IP4_DIRECCIÓN o ambos en la carga útil de configuración CFG_SOLICITUD, la ePDG puede incluir uno o más casos del mismo atributo en la carga útil de configuración CFG_RESPUESTA como se especifica en IETF draft-gundavelli-ipsecme-3gpp-ims-options. Si el equipo de usuario incluyó el atributo de PERIODO_TIEMPODEESPERA_PARA_COMPROBACIÓN_OPERATIVIDAD que indica el soporte del período de plazo de espera de recepción para la comprobación de operatividad en la carga útil de configuración CFG_SOLICITUD, la ePDG puede incluir el atributo de PERIODO_TIEMPODEESPERA_PARA_COMPROBACIÓN_OPERATIVIDAD que indica el período de plazo de espera para la comprobación de operatividad en la carga útil de configuración CFG_RESPUESTA.

Si se utiliza DSMIPv6 como mecanismo de movilidad IP, dependiendo de la información proporcionada por el equipo de usuario en la carga útil de CFG_SOLICITUD, las ePDG asignan al equipo de usuario o bien una dirección local de IPv4 o bien una dirección local de IPv6 (o un prefijo local de IPv6) a través de una única carga útil de configuración CFG_RESPUESTA. Si la ePDG asigna una dirección local de IPv4, la CFG_RESPUESTA comprende el atributo de DIRECCIÓN_IP4_INTERNA. Si la ePDG asigna una dirección local de IPv6 o un prefijo local de IPv6, la CFG_RESPUESTA comprende correspondientemente el atributo de DIRECCIÓN_IP6_INTERNA o de SUBRED_IP6_INTERNA. Si el equipo de usuario proporcionó un APN a la ePDG durante el establecimiento del túnel, la ePDG no cambia el APN proporcionado e incluye el APN en la carga útil de IDr del mensaje de respuesta de IKE_AUT. Ahora se establece un túnel de IPsec entre el equipo de usuario y la ePDG.

Si se utiliza NBM y si la ePDG necesita rechazar una conexión de PDN, por ejemplo debido a condiciones específicas, a las políticas de red o a las competencias de ePDG para indicar que no se pueden aceptar más solicitudes de conexión de PDN del APN dado para el equipo de usuario, la ePDG incluye, en el mensaje de respuesta de IKE_AUT, una notificación de carga útil con un tipo PDN_CONEXIÓN_RECHAZO de mensaje privado de notificación. Además, si el mensaje de solicitud de IKE_AUT del equipo de usuario indica conexión de traspaso, el campo de datos de notificación de la carga útil de notificación incluye la información de la dirección de IP de la indicación de la conexión de traspaso. Si el equipo de usuario indicó conexión inicial, se omite el campo datos de notificación. Si la ePDG necesita rechazar una conexión de PDN debido a las políticas o competencias de la red para indicar que no se pueden aceptar más solicitudes de conexión de PDN con ningún APN para el equipo de usuario, la ePDG incluye en el mensaje de respuesta de IKE_AUT que contiene la carga útil de IDr una carga útil de notificación con un tipo MAX_CONEXIÓN_ALCANZADA de mensaje privado de notificación. Si la ePDG determina que al equipo de usuario no se le permite acceder a un EPC, la ePDG incluye, en el mensaje de respuesta de IKE_AUT, una carga útil de notificación con un tipo AUTENTIFICACIÓN_FALLIDA de mensaje de notificación.

Si el equipo de usuario indica conexión de traspaso incluyendo la información de la dirección de origen previamente asignada y la ePDG obtiene una o más identidades de GW de PDN del servidor de AAA del 3GPP, la ePDG usa estas GW de PDN identificadas en el proceso subsiguiente de selección de GW de PDN. Si el equipo de usuario indica conexión inicial, es decir, información de la dirección de origen no incluida, la ePDG puede ejecutar su proceso de selección inicial de GW de PDN para determinar la GW de PDN sin utilizar las identidades de GW de PDN recibidas.

La ePDG soporta ESP de IPSec con el fin de proporcionar túneles seguros entre el equipo de usuario y la ePDG.

Durante la autenticación de IKEv2 y el establecimiento del túnel, si el equipo de usuario solicitó la dirección o

las direcciones del IP de HA y si se eligió DSMIPv6 y si la dirección o las direcciones de HAIP están disponibles, la ePDG proporciona las direcciones de IP del HA (dirección de IPv6 y opcionalmente, dirección de IPv4) para el APN correspondiente especificado por la carga útil de "IDr" en el mensaje de solicitud de IKE_AUT al incluir en la carga útil de configuración CFG_RESPUESTA un atributo de DIRECCIÓN_AGENTE_ORIGEN. En CFG_RESPUESTA, la ePDG establece, respectivamente, el campo de dirección del agente de origen de IPv6, y, opcionalmente, el campo de dirección del agente de origen de IPv4 del atributo de DIRECCIÓN_AGENTE_ORIGEN a la dirección de IPv6 del HA y a la dirección de IPv4 del HA. Si no hay una dirección de IPv4 del HA disponible en la ePDG o si no fue solicitada por el equipo de usuario, la ePDG omite el campo dirección de IPv4 del agente de origen. Si la ePDG no puede proporcionar una dirección de IPv6 del HA para el APN correspondiente, entonces la ePDG no incluye un atributo de DIRECCIÓN _AGENTE_ORIGEN en la CFG_RESPUESTA.

El ePDG puede admitir múltiples intercambios de autenticación en el protocolo de IKEv2 con el fin de soportar la autenticación y la autorización adicionales del equipo de usuario con un servidor de AAA externo.

Si la ePDG soporta la autenticación y la autorización del equipo de usuario con un servidor de AAA externo, al recibir un mensaje de IKE_SA_INIC, la ePDG incluye una carga útil de notificación de tipo "MULTIPLE_AUT_SOPORTADA" en el mensaje de respuesta de IKE_SA_INIC al equipo de usuario.

Al completar con éxito el procedimiento de autenticación y autorización del equipo de usuario que accede a EPC y al recibir una solicitud de IKE_AUT que contiene una carga útil de notificación de tipo "OTRA_AUT_SIGUE", la ePDG envía una respuesta de IKE_AUT que contiene la carga útil de "AUT".

Al recibir una solicitud subsiguiente de IKE_AUT del equipo de usuario que comprende la identidad del usuario en la red privada dentro de la carga útil de "IDi", la ePDG realiza lo siguiente:

Si se requiere autenticación de PAP, la ePDG envía una solicitud de EAP-GTC al equipo de usuario dentro de un mensaje de respuesta de IKE_AUT. Al recibir una respuesta de EAP-GTC del equipo de usuario, la ePDG autentica al usuario (equipo de usuario) con el servidor externo de AAA.

Si se requiere autenticación de CHAP, la ePDG envía una solicitud de MD5-Cuestionamiento de EAP al equipo de usuario. Al recibir una respuesta MD5-Cuestionamiento de EAP dentro de un mensaje de solicitud de IKE_AUT del equipo de usuario, la ePDG autentica al usuario (equipo de usuario) con el servidor externo de AAA. Si la ePDG recibe la respuesta Nak-heredado que comprende el tipo de EAP-GTC del equipo de usuario, la ePDG puede cambiar el procedimiento de autenticación y autorización. Si la ePDG no cambia el procedimiento de autenticación y autorización o si la ePDG recibe una respuesta de Nak-heredado que no comprende EAP-GTC, la ePDG envía EAP-Fallo al equipo de usuario.

La señalización general fluye para autenticación y autorización con un servidor externo de AAA.

En términos generales, los requisitos de IETF RFC 5996 aplican a esta realización.

El atributo de PERIODO_TIEMPODEESPERA_PARA_COMPROBACIÓN_OPERATIVIDAD de acuerdo con esta realización se muestra en la figura 10.

En la figura 10, las entradas del atributo se codifican de la siguiente manera: El bitio R en el primer octeto. El campo de tipo de atributo que indica PERIODO_TIEMPODEESPERA_PARA_COMPROBACIÓN_OPERATIVIDAD es del valor xx. El campo de longitud se establece en cero o cuatro. Si el campo de longitud se establece en cero, el campo del período de plazo de espera no se incluye. Si el campo del período de plazo de espera no está incluido, esto indica soporte del período de plazo de espera de recepción para la comprobación de operatividad. Si se incluye el campo del período de plazo de espera, el campo del período de plazo de espera indica el período de plazo de espera para la comprobación de operatividad en segundos.

En esta realización, el punto final del túnel en la red es la ePDG. Como parte del intento de establecimiento del túnel, se solicita el uso de cierto APN. Cuando el UE realiza un nuevo intento de establecimiento de túnel, el UE usa IKEv2. La autenticación del UE en su papel de iniciador de IKEv2 termina en el servidor de AAA del 3GPP. El UE envía mensajes de EAP a través de IKEv2 a la ePDG. La ePDG extrae los mensajes de EAP recibidos del UE a través de IKEv2 y los envía al servidor de AAA del 3GPP. El UE utiliza la carga útil de configuración de IKEv2 para obtener la dirección remota de IP.

En lo que sigue, se omiten los parámetros y procedimientos del mensaje de EAP-AKA con respecto a la autenticación; sólo se divulgan las decisiones y los procesos relevantes para el uso de EAP-AKA dentro de IKEv2.

El flujo de mensajes para la autenticación completa se ilustra en el diagrama de señalización de la figura 9.

Como el equipo de usuario y la ePDG generan números aleatorios usados solo una vez, como entrada para derivar

las claves de cifrado y autenticación en IKEv2, se proporciona protección de respuesta. Al menos por esta razón, no es necesario que el servidor de AAA de 3GPP solicite nuevamente la identidad del usuario utilizando los métodos específicos de EAP-AKA, porque el servidor de AAA de 3GPP está seguro de que ningún nodo intermedio ha modificado o cambiado la identidad del usuario.

S301. El UE y la ePDG intercambian un primer par de mensajes, conocidos como IKE_SA_INIC, en donde la ePDG y el UE negocian algoritmos criptográficos, intercambian números aleatorios usados solo una vez y realizan un intercambio Diffie_Hellman. En el diagrama de señalización de la figura 9, el atributo de X en el paso S301 representa un atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad.

S302. El UE envía la identidad del usuario (en la carga útil de IDi) y la información de APN (en la carga útil de IDr) en este primer mensaje de la fase de IKE_AUT, y comienza la negociación de las asociaciones de seguridad infantil. El UE omite el parámetro de AUT para indicarle a la ePDG que quiere usar EAP a través de IKEv2. La identidad del usuario cumple con un formato de Identificador de acceso a la red (NAI), que contiene el IMSI o el seudónimo, tal como se define para EAP-AKA. El UE envía la carga útil de configuración (CFG_SOLICITUD) dentro del mensaje de solicitud de IKE_AUT para obtener una dirección de IP de origen de IPv4 y/o de IPV6 y/o una dirección de agente de origen.

S303. La ePDG envía el mensaje de solicitud de autenticación y autorización al servidor de AAA del 3GPP, que contiene la identidad del usuario y el APN. El UE usa el NAI; el servidor de AAA del 3GPP identifica, en base a la parte del terreno del NAI, que la autenticación y autorización combinadas se están realizando para el establecimiento del túnel con una ePDG que sólo permite EAP-AKA (y no una PDG de I-WLAN, que permitiría también EAP-SIM). Las diferentes ID de aplicación Diameter ayudarán al servidor de AAA del 3GPP a distinguir entre las autenticaciones para el acceso confiable (que requiere autenticación de EAP-AKA) y las autenticaciones para el establecimiento del túnel en el EPS (que sólo permite EAP-AKA).

S304. El servidor de AAA del 3GPP obtiene los vectores de autenticación de HSS/HLR (si estos parámetros no están disponibles en el servidor de AAA del 3GPP). El servidor de AAA del 3GPP realiza una búsqueda del IMSI del usuario autenticado (UE) en base a la identidad del usuario recibida (NAI de raíz o seudónimo) e incluye el EAP-AKA como método de autenticación solicitado en la solicitud enviada al HSS. Después, el HSS genera vectores de autenticación con bitio = 0 de separación de AMF y los envía de vuelta al servidor de AAA de 3GPP.

S305. El servidor de AAA del 3GPP inicia el cuestionamiento de autenticación. La identidad del usuario no se solicita nuevamente.

S306. La ePDG responde con su identidad, un certificado, y envía el parámetro de AUT para proteger el mensaje anterior que envió al UE (en el intercambio de IKE_SA_INIC). El mensaje de EAP recibido del servidor de AAA de 3GPP (EAP-Solicitud/AKA-Cuestionamiento) se incluye con el fin de iniciar el procedimiento de EAP a través de IKEv2.

S307. El UE verifica los parámetros de autenticación y responde al cuestionamiento de autenticación. La única carga útil (aparte del encabezado) en el mensaje de IKEv2 es el mensaje de EAP.

S308. La ePDG reenvía el mensaje de EAP-Respuesta/AKA-Cuestionamiento al servidor de AAA de 3GPP.

S308.a El servidor de AAA del 3GPP verifica si la respuesta de autenticación es correcta.

S308.b-e Si la selección dinámica de movilidad de IP se ejecuta integrada en la autenticación y la autorización, el modo de movilidad seleccionado se envía al usuario (UE) en una solicitud de AKA-Notificación, a través de la respuesta de A&A de Diameter y del mensaje de IKE_AUT. El UE responde a esto a través de IKEv2 y la ePDG reenvía la respuesta al servidor de AAA de 3GPP.

S308A. El servidor de AAA del 3GPP inicia la recuperación del perfil del abonado y el registro del servidor de AAA del 3GPP en el HSS. El servidor de AAA del 3GPP comprueba en la subscripción del equipo de usuario si el usuario está autorizado para acceso de no 3GPP.

S309. Cuando todas las comprobaciones son exitosas, el servidor de AAA del 3GPP envía una respuesta final de autenticación y autorización (con un código de resultado que indica éxito) que incluye la información relevante de autorización de servicio, un éxito de EAP y el material clave para la ePDG. Este material clave comprende la MSK generada durante el proceso de autenticación. Cuando las interfaces SWm y SWd entre la ePDG y el servidor de AAA del 3GPP se implantan utilizando Diameter, la MSK (clave maestra de sesión) es encapsulada en los protocolos EAP-Clave Maestra-Sesión-AVP.

S310. La ePDG utiliza la MSK para generar los parámetros de AUT con el fin de autenticar los mensajes de

fase de IKE_SA_INIC. Estos dos primeros mensajes no se habían autenticado antes ya que no había material clave disponible todavía. El secreto compartido generado en un intercambio de EAP (MSK), cuando se usa a través de IKEv2, se usa para generar los parámetros de AUT.

S311. El mensaje de Éxito/Fallo del EAP se reenvía al equipo de usuario a través de IKEv2.

S312. El equipo de usuario toma su propia copia del MSK como entrada para generar el parámetro de AUT para autenticar el primer mensaje de IKE_SA_INIC. El parámetro de AUT se envía a la ePDG.

S313. La ePDG comprueba la exactitud de la AUT recibida del equipo de usuario. En este momento, el equipo de usuario está autenticado. Si se usa el caso S2b, la señalización de PMIP entre la ePDG y la GW de PDN puede ahora comenzar. La ePDG continúa con el siguiente paso en el procedimiento aquí descrito sólo después de completar con éxito el procedimiento de actualización de enlace de PMIP.

S314. La ePDG calcula el parámetro de AUT que autentica el segundo mensaje de IKE_SA_INIC. La ePDG envía la dirección remota asignada de IP en la carga útil de configuración (CFG_RESPUESTA).

S315. El parámetro de AUT se envía al UE junto con la carga útil de configuración, las asociaciones de seguridad y el resto de los parámetros de IKEv2 y la negociación de IKEv2 finalizan. En el diagrama de señalización de la figura 9, el atributo de Yin paso S315 representa un atributo de configuración que indica un período de plazo de espera para la comprobación de operatividad.

El concepto inventivo anteriormente se ha descrito principalmente con referencia a unas pocas realizaciones. Sin embargo, como puede apreciar fácilmente el experto en la técnica, otras realizaciones distintas de las divulgadas anteriormente son igualmente posibles dentro del alcance del concepto inventivo, como se define en las reivindicaciones de patente adjuntas.

REIVINDICACIONES

1. Un método para la configuración y la realización de una comprobación de operatividad utilizando mensajes de intercambio de claves de Internet, siendo el método realizado por un equipo (11) de usuario, comprendiendo el método:

transmitir (S102), a un nodo (12) de red central, un primer mensaje de intercambio de claves de Internet que comprende un atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad, en el que el atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad es un período de plazo de espera para el atributo de comprobación de operatividad con el campo de longitud establecido en cero,

recibir (S104) del nodo de red central, un segundo mensaje de intercambio de claves de Internet que comprende un atributo de configuración que indica un período de plazo de espera para dicha comprobación de operatividad,

realizar (S106) dicha comprobación de operatividad de acuerdo con el atributo de configuración que indica un período de plazo de espera para dicha comprobación de operatividad, que comprende:

transmitir (S108) una solicitud informativa sin carga útil si se incluye un período de plazo de espera para el atributo de comprobación de operatividad en el atributo de configuración recibido que indica un período de plazo de espera para dicha comprobación de operatividad, y, en ausencia de recibir un paquete de seguridad de protocolo de Internet criptográficamente protegido, IPSec, o un paquete de intercambio de claves de Internet criptográficamente durante el período de plazo de espera para dicha comprobación de operatividad, y en el que, en ausencia de recibir una respuesta informativa en respuesta a la solicitud informativa transmitida sin carga útil, realizar una acción o más de entre:

determinar (S110) el fallo de la asociación de seguridad de intercambio de claves de Internet;

descartar (S112) cualquier información de estado asociada con la asociación de seguridad de intercambio de claves de Internet; y/o

descartar (S114) cualesquiera asociaciones de seguridad de seguridad de protocolo de Internet, IPSec, negociadas utilizando la asociación de seguridad de intercambio de claves de Internet.

2. El método de acuerdo con la reivindicación 1, en el que el atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad se proporciona en una carga útil de configuración CFG_SOLICITUD.

3. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el atributo de configuración que indica un período de plazo de espera para dicha comprobación de operatividad es un período de plazo de espera para el atributo de comprobación de operatividad con un campo de período de plazo de espera.

4. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el atributo de configuración que indica un período de plazo de espera para dicha comprobación de operatividad se proporciona en una carga útil de configuración CFG_RESPUESTA.

5. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que dicho atributo de configuración que indica un período de plazo de espera para dicha comprobación de operatividad se basa en información de un sistema de configuración o de un sistema de gestión.

6. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el primer mensaje de intercambio de claves de Internet se transmite en un mensaje de intercambio de claves de Internet de versión 2, IKEv2, y en el que el segundo mensaje de intercambio de claves de Internet se recibe en un mensaje de IKEv2.

7. Un equipo de usuario (11) para la configuración y la realización de una comprobación de operatividad que usa mensajes de intercambio de claves de Internet, comprendiendo el equipo de usuario una unidad (21) de procesamiento, estando la unidad de procesamiento configurada para hacer que el equipo de usuario:

transmita, a un nodo (12) de red central, un primer mensaje de intercambio de claves de Internet que comprende un atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad; en el que el atributo de configuración que indica soporte para recibir un período de plazo de espera para la comprobación de operatividad es un período de plazo de espera para el atributo de comprobación de operatividad con el campo de longitud establecido en cero,

reciba, desde el nodo de red central, un segundo mensaje de intercambio de claves de Internet que comprende un atributo de configuración que indica un período de plazo de espera para dicha comprobación de operatividad, y

realice dicha comprobación de operatividad de acuerdo con el atributo de configuración que indica un período de plazo de espera para dicha comprobación de operatividad, que comprende:

transmitir una solicitud informativa sin carga útil si se incluye un período de plazo de espera para el atributo de comprobación de operatividad en el atributo de configuración recibido que indica un período de plazo de espera para dicha comprobación de operatividad, y, en ausencia de recibir un paquete de seguridad de protocolo de Internet, IPSec, criptográficamente protegido o un paquete de intercambio de claves de Internet criptográficamente durante el período de plazo de espera para dicha comprobación de operatividad, y en el que, en ausencia de recibir una respuesta informativa en respuesta a la solicitud informativa transmitida sin carga útil, adicionalmente:

determinar el fallo de la asociación de seguridad de intercambio de claves de Internet;

descartar cualquier información de estado asociada con la asociación de seguridad de intercambio de claves de Internet; y/o

descartar cualesquiera asociaciones de seguridad de seguridad de protocolo de Internet, IPSec, negociadas utilizando la asociación de seguridad de intercambio de claves de Internet.

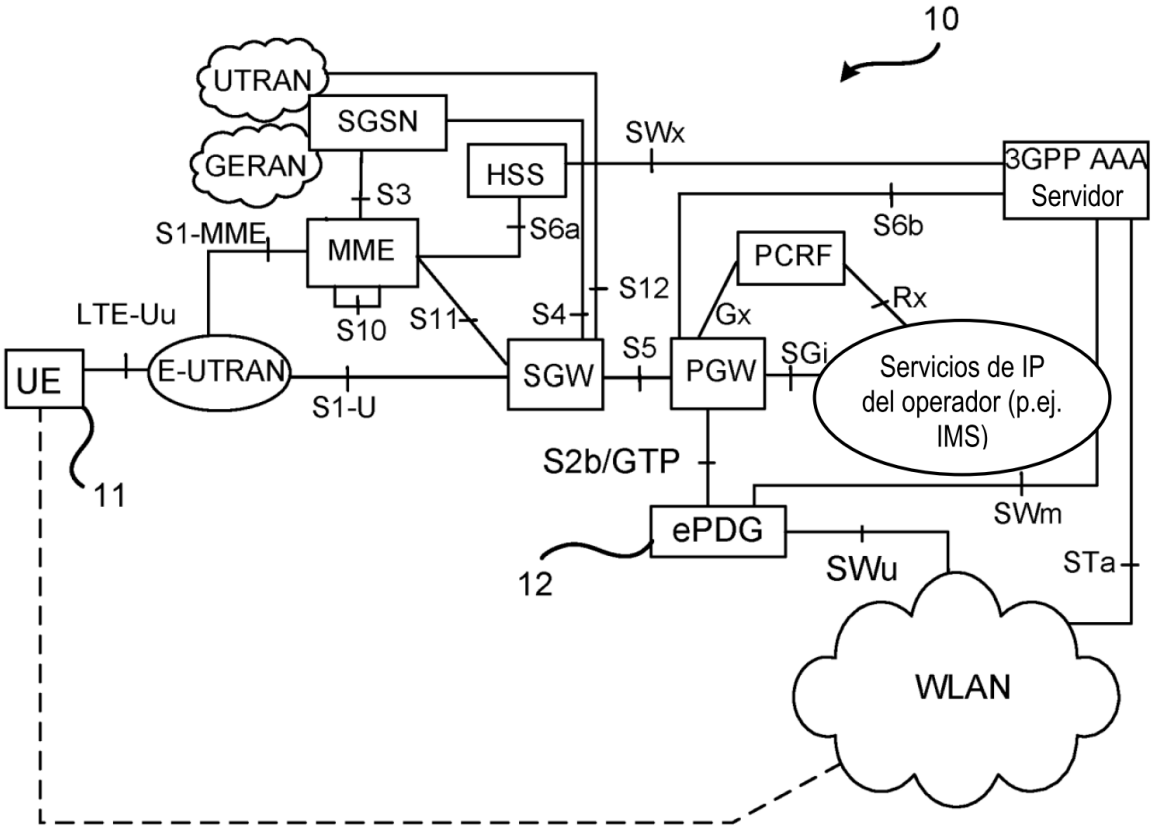
10
UTRAN
SGSN
GERAN
HSS
SWx
3GPP AAA Servidor
S3
S6a
S6b
S1-MME
MME
PCRF
S12
Rx
LTE-Uu
S10
S11
S4
Gx
S5
SGi
UE
E-UTRAN
SGW
PGW
Servicios de IP del operador (p.ej. IMS)
S1-U
S2b/GTP
11
ePDG
SWm
12
SWu
STa
WLAN

Fig. 1

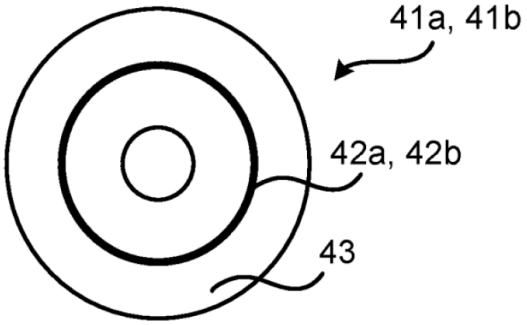
41a, 41b
42a, 42b
43

Fig. 4

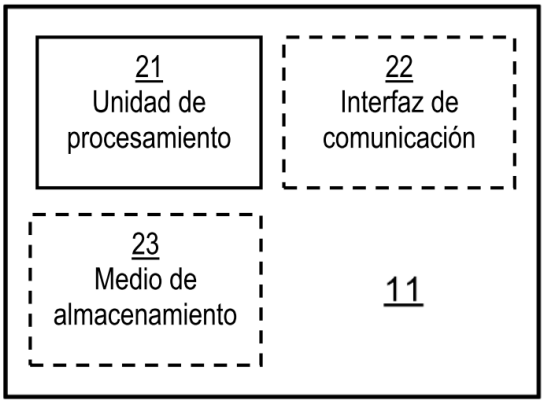

Fig. 2a

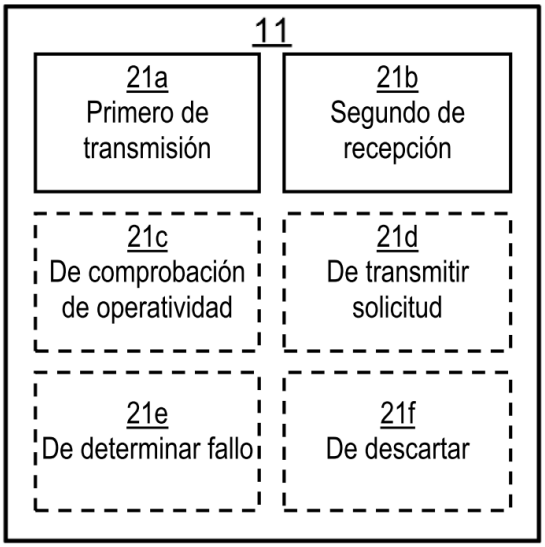

Fig. 2b

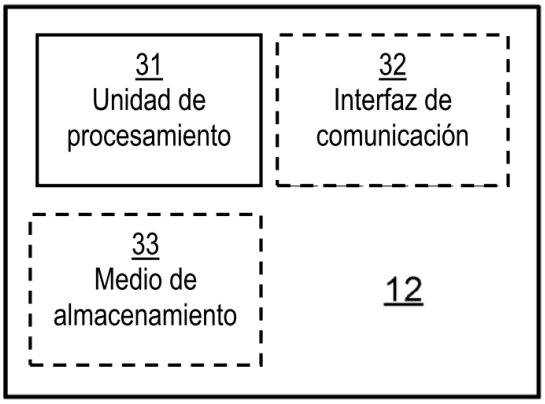

Fig. 3a

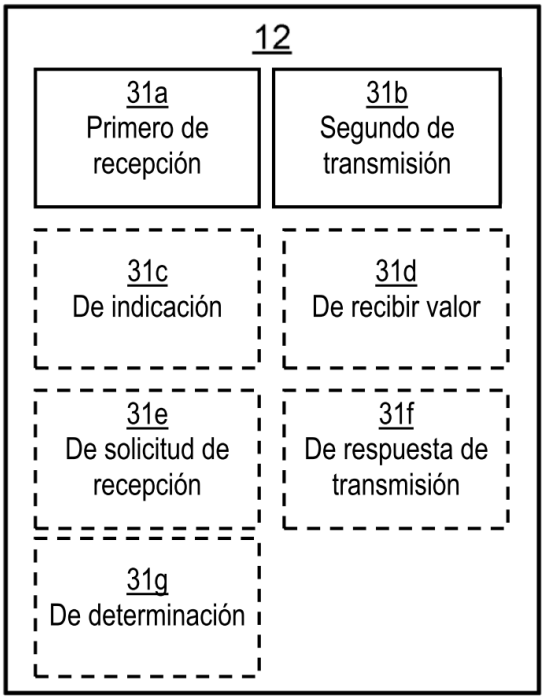

Fig. 3b

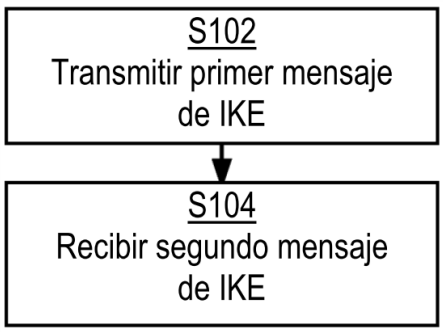

Fig. 5

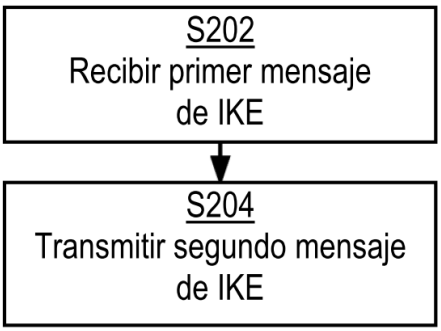

Fig. 7

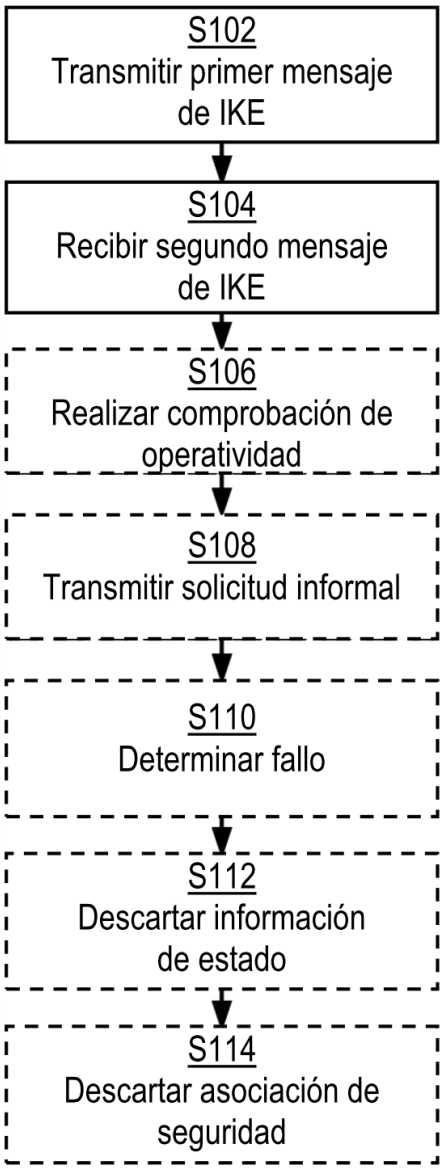

Fig. 6

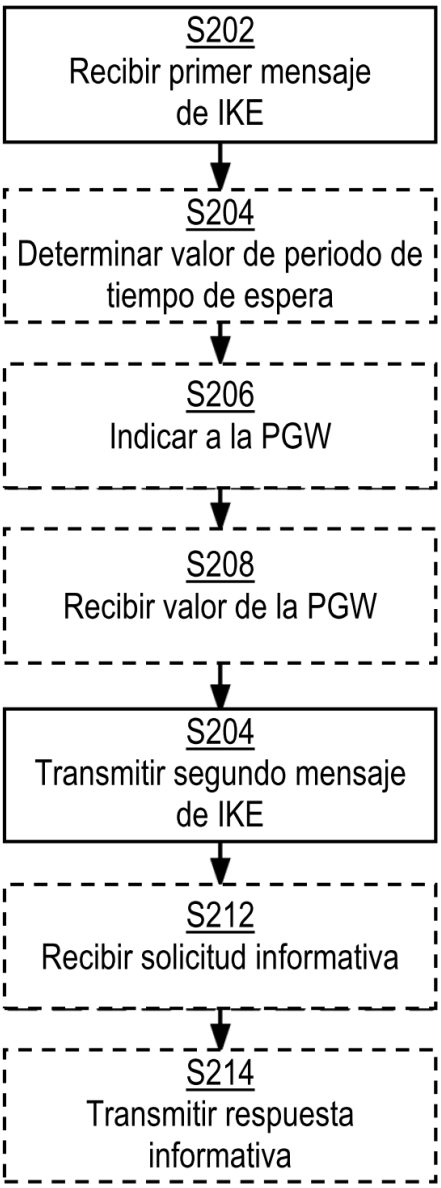

Fig. 8

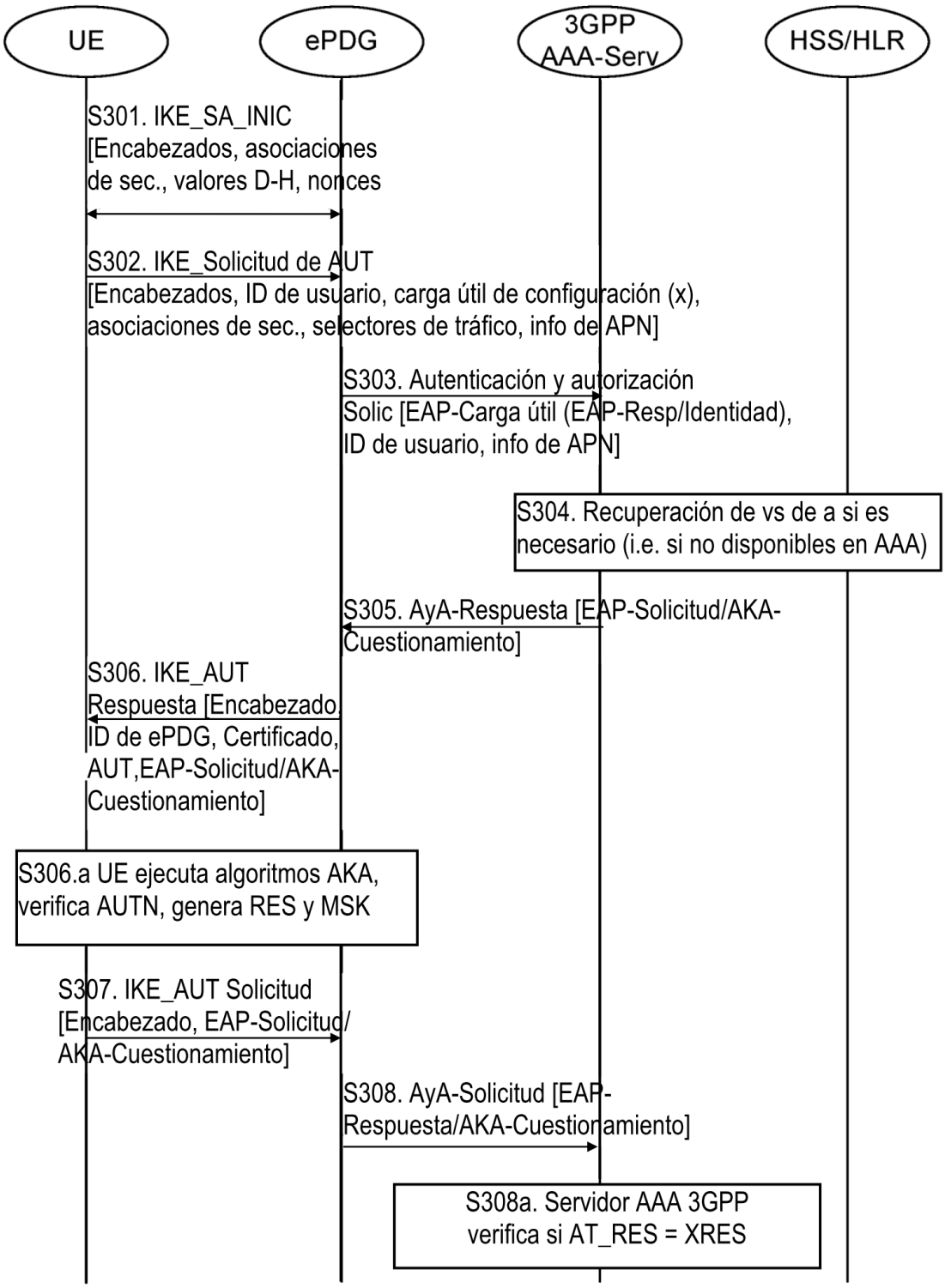
UE
ePDG
3GPP AAA-Serv
HSS/HLR
S301. IKE_SA_INIC [Encabezados, asociaciones de sec., valores D-H, nonces
S302. IKE_Solicitud de AUT [Encabezados, ID de usuario, carga útil de configuración (x), asociaciones de sec., selectores de tráfico, info de APN]
S303. Autenticación y autorización Solic [EAP-Carga útil (EAP-Resp/Identidad), ID de usuario, info de APN]
S304. Recuperación de vs de a si es necesario (i.e. si no disponibles en AAA)
S305. AyA-Respuesta [EAP-Solicitud/AKA-Cuestionamiento]
S306. IKE_AUT Respuesta [Encabezado, ID de ePDG, Certificado, AUT,EAP-Solicitud/AKA-Cuestionamiento]
S306.a UE ejecuta algoritmos AKA, verifica AUTN, genera RES y MSK
S307. IKE_AUT Solicitud [Encabezado, EAP-Solicitud/ AKA-Cuestionamiento]
S308. AyA-Solicitud [EAP-Respuesta/AKA-Cuestionamiento]
S308a. Servidor AAA 3GPP verifica si AT_RES = XRES

Fig. 9 (Parte 1)

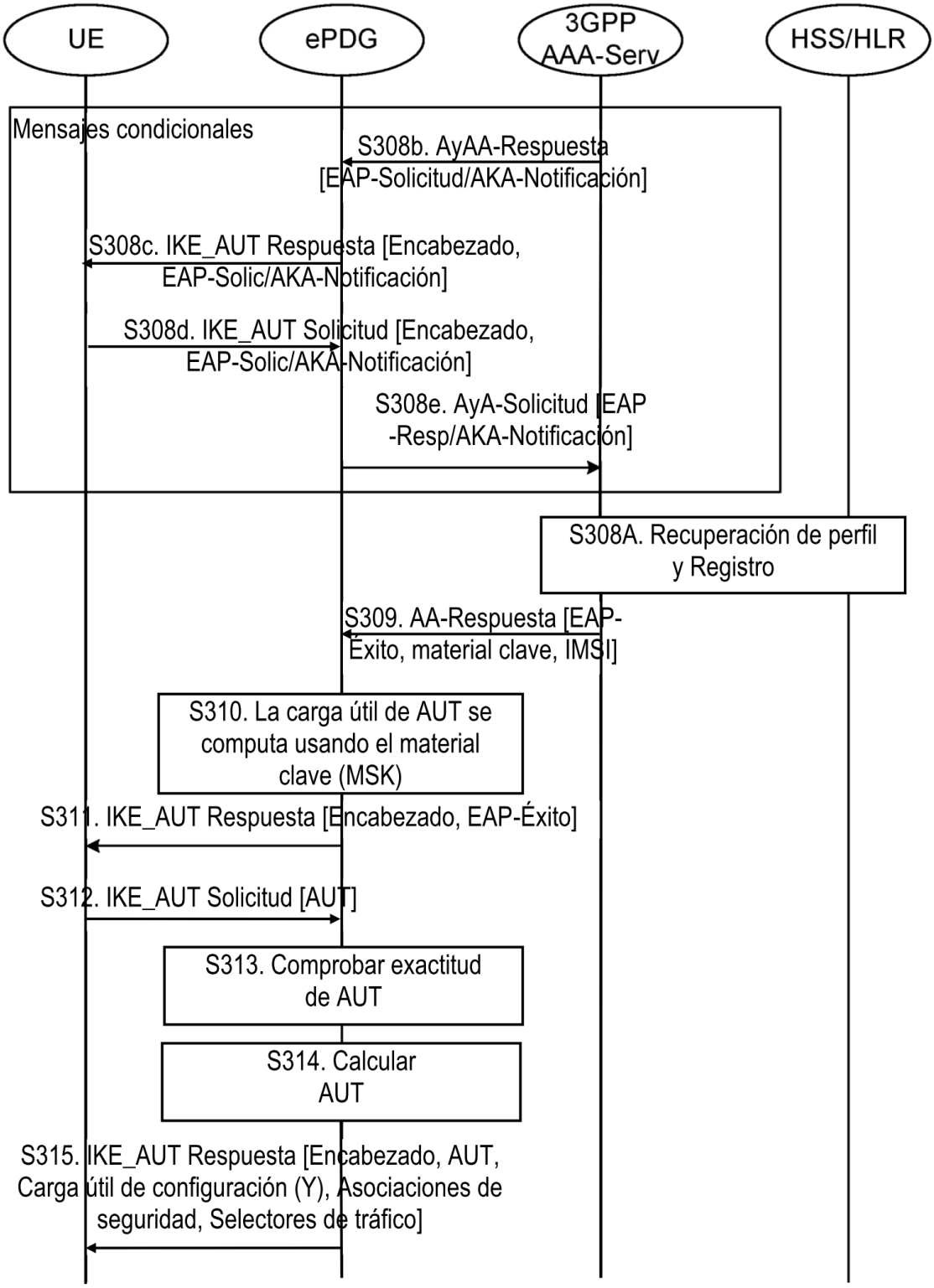
UE
ePDG
3GPP AAA-Serv
HSS/HLR
Mensajes condicionales
S308b. AyAA-Respuesta [EAP-Solicitud/AKA-Notificación]
S308c. IKE_AUT Respuesta [Encabezado, EAP-Solic/AKA-Notificación]
S308d. IKE_AUT Solicitud [Encabezado, EAP-Solic/AKA-Notificación]
S308e. AyA-Solicitud [EAP -Resp/AKA-Notificación]
S308A. Recuperación de perfil y Registro
S309. AA-Respuesta [EAP-Éxito, material clave, IMSI]
S310. La carga útil de AUT se computa usando el material clave (MSK)
S311. IKE_AUT Respuesta [Encabezado, EAP-Éxito]
S312. IKE_AUT Solicitud [AUT]
S313. Comprobar exactitud de AUT
S314. Calcular AUT
S315. IKE_AUT Respuesta [Encabezado, AUT, Carga útil de configuración (Y), Asociaciones de seguridad, Selectores de tráfico]

Fig. 9 (Parte 2)


Bitios
7 6 5 4 3 2 1 0
R
Tipo de atributo
Tipo de atributo
Longitud
Periodo de tiempo de espera
1
2
3,4
5-8
Octetos

Fig. 10