(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 703 555**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/04 (2009.01)
H04W 36/00 (2009.01)
H04W 84/12 (2009.01)
H04W 12/02 (2009.01)
H04W 12/10 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.04.2015 PCT/EP2015/058140**

(87) Fecha y número de publicación internacional: **12.11.2015 WO15169552**

(96) Fecha de presentación y número de la solicitud europea: **15.04.2015 E 15717469 (9)**

(97) Fecha y número de publicación de la concesión europea: **26.09.2018 EP 3140972**

(54) Título: **Protección de intercambio de mensajes WLCP entre TWAG y UE**

(30) Prioridad:

05.05.2014 US 201461988613 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.03.2019

(73) Titular/es:

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

(72) Inventor/es:

ROELAND, DINAND;
ROMMER, STEFAN;
NORRMAN, KARL y
LEHTOVIRTA, VESA

(74) Agente/Representante:

ELZABURU, S.L.P

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCION

Protección de intercambio de mensajes WLCP entre TWAG y UE

Campo técnico

La invención se refiere a métodos y dispositivos para proteger el intercambio de mensajes del Protocolo de Control (WLCP) de la Red de Area Local Inalámbrica (WLAN) entre una Pasarela de Acceso (WLAN) Fiable (TWAG) de una Red de Acceso (WLAN) Fiable (TWAN) y un Equipo de Usuario, (UE), así como los correspondientes programas de ordenador y productos de programas de ordenador.

Antecedentes

Un concepto básico en la arquitectura de Núcleo de Paquetes Evolucionado (EPC) 3GPP es la Red de Datos en Paquetes (PDN). Una PDN es una red de Protocolo de Internet (IP), por ejemplo, Internet, pero también puede ser una red corporativa cerrada o una red de servicio de operador tal como un Subsistema de Multimedia IP (IMS). Una PDN tiene uno o más nombres asociados, cada uno de los cuales está representado por una cadena llamada nombre del Punto de Acceso (APN). Una pasarela PDN (PDN-GW o PGW) es un nodo funcional que proporciona acceso a una o más PDNs. Para una descripción de los antecedentes relevantes, se hace referencia a las Especificaciones Técnicas (TS) 3GPP, en particular las TS 23.401 y TS 23.402.

Una conexión PDN proporciona un Equipo de Usuario (UE) con un canal de acceso a una PDN. Es un túnel lógico de IP entre el UE y la PGW. Cada conexión PDN tiene una sola dirección IP/prefijo. Un UE puede establecer múltiples conexiones PDN, posiblemente a la misma APN.

En la figura 1, se ilustra la arquitectura de red para integrar una Red de Acceso WLAN Fiable (TWAN) 110 en una red EPC. La figura 1 se reproduce de TS 23.402 (rev 12.3.0, figura 16.1.1-1) y muestra el escenario carente de función tránsito. Para los escenarios con tránsito, se hace referencia a TS 23.402.

La arquitectura interna de la TWAN 110 está fuera del alcance del 3GPP. Sin embargo, 3GPP ha definido una serie de funciones que deben soportarse en la TWAN 110 para permitir la inter operatividad con las redes EPC y los UE 3GPP 101. En la figura 2, también reproducida de TS 23.402 (rev 12.3.0, figura 16.1.2-1), se ilustra la funcionalidad TWAN que se requiere para la inter operatividad con EPC. Las funciones requeridas son:

- Una red de acceso WLAN (WLAN AN). La WLAN AN incluye una colección de uno o más Puntos de Acceso WLAN (AP) 111. Un punto de acceso termina el enlace WLAN IEEE 802.11 del UE.

- Una Pasarela de Acceso WLAN Fiable (TWAG) 112. Esta función finaliza el interfaz S2a y reenvía los paquetes entre el enlace UE-TWAG y el túnel S2a para esa Conexión UE y PDN.

- Un Proxy de Autenticación, Autorización y Contabilización (AAA) Fiable WLAN (TWAP) 113. Esta función finaliza el interfaz STa. Retransmite la información AAA entre la WLAN AN y el Servidor 103 3GPP AAA o Proxy desplegado en la red 3GPP (la Red Móvil Terrestre Pública Doméstica (HPLMN), en escenarios carentes de función tránsito)

Existe la necesidad de intercambiar información entre las diferentes funciones TWAN, pero como la arquitectura TWAN interna está fuera del alcance de 3GPP, los interfaces correspondientes no se muestran en la figura 2. Las funciones TWAN pueden realizarse de diferentes maneras, tanto situadas juntas así como separadas entre sí.

De acuerdo con las especificaciones 3GPP, existen dos "escenarios" para determinar cómo se pueden manejar las conexiones PDN entre el UE y la red en el caso de TWAN. A continuación, se hace referencia a estos escenarios como Modo de Conexión Simple (SCM) y Modo de Conexión Múltiple (MCM).

En SCM, solo se soporta una única sesión de IP por UE a través de WLAN. El UE usa el Protocolo de Autenticación Extensible (EAP) para proporcionar información relativa a qué tipo de sesión IP se solicita (por ejemplo, proporcionando una APN).

En MCM, múltiples sesiones IP simultáneas por UE son soportadas sobre WLAN. En este modo, un nuevo protocolo de control entre el UE 111 y la TWAG 112, el Protocolo de Control de WLAN (WLCP), está actualmente siendo especificado por 3GPP para administrar las Conexiones de PDN (ver, por ejemplo, TS 23.402 y TS 24.244). El WLCP se utiliza para solicitar el establecimiento y la desconexión de las conexiones de PDN y para llevar los parámetros asociados con cada conexión de PDN como APN, tipo PDN, y similares. Se ha acordado que WLCP se transmita a través del Protocolo de Datagramas de Usuario (UDP)/IP.

Un problema de la solución actual es que no existe protección de la señalización WLCP entre el UE 101 y la TWAG 112. Depender de la protección del tráfico en el enlace aéreo 802.11 existente, basada en las normas IEEE 802.11, se asocia con los problemas descritos a continuación.

La protección en el enlace aéreo 802.11 solo cubre la ruta entre el UE 101 y el AP 111. Además, solo se basa en el uso de las direcciones de Control de Acceso a los Medios (MAC) del UE 101 y del AP 111 como identificadores del

tráfico. Sin embargo, con WLCP, el tráfico se envía entre el UE 101 y la TWAG 112, a través del AP 111. Dado que los paquetes IP enviados a través del enlace aéreo 802.11 están protegidos por medio del enlace aéreo, el UE 101 y la TWAG 112 podrían autenticar potencialmente el mensaje WLCP recibido basándose en la dirección MAC de origen. Esta solución, sin embargo, se basa en dos suposiciones:

- El primer supuesto es que el AP 111, y el enlace entre el AP 111 y la TWAG 112, son seguros. Si este es el caso, se puede suponer que los paquetes no pueden ser manipulados entre el UE 101 y la TWAG 112 incluso si solo el enlace UE-AP está íntegramente protegido.

- El segundo supuesto es que el receptor puede autenticar el paquete basándose en la dirección MAC de origen.

La primera suposición puede ser válida en muchos casos, por ejemplo, en redes WLAN/WiFi desplegadas por el operador. Sin embargo, incluso en ese caso, el enlace entre el AP 111 y la TWAG 112 puede ser accesible a terceros y difícil de proteger del acceso físico.

La segunda suposición se basa en que el receptor del paquete WLCP puede usar la dirección MAC para identificar al remitente del mensaje. En muchos sistemas, por ejemplo, en realizaciones regulares de UE de clientes UDP, la dirección MAC no está disponible para una aplicación UDP. Por lo tanto, el software WLCP en el UE no sabrá la dirección MAC utilizada para llevar el mensaje. Si bien se puede argumentar que este es un problema de realización ya que las capas más bajas en el UE podrían pasar la dirección MAC de origen a las capas más altas (es decir, UDP), este es un requisito importante para poner en todos los sistemas operativos, tales como Android, iOS y similares, y dificulta el despliegue de WLCP.

En el "Security Analysis of WLCP", 3GPP TSG SA WG3 (Security), Reunión # 75, 12-16 de mayo de 2014 Sapporo (Japón), documento S3-140812, se analizan los aspectos de seguridad de la señalización WLCP. Se describió que WLCP se usa entre el UE y la TWAG y se transporta a través de UDP/IP, y que los mensajes WLCP están encriptados y protegida su integridad entre el UE y el AP.

El documento US 2013/0176897 A1 describe métodos y aparatos para la configuración de enlaces acelerados en redes IEE 802.11. Una estación (STA) puede adquirir información sobre un AP de una red IEEE 802.11 por adelantado a través de un interfaz IEEE 802.11 previamente conectado y/o un interfaz diferente de la red IEEE 802.11. La STA puede usar la información adquirida durante un procedimiento de configuración de enlace entre la STA y el AP.

Resumen

Un objetivo de la invención es proporcionar una alternativa mejorada de las técnicas anteriores y de la técnica anterior.

Más específicamente, un objetivo de la invención es proporcionar una protección mejorada de la señalización WLCP entre el UE y la TWAG.

Estos y otros objetos de la invención se logran por medio de diferentes aspectos de la invención, como se define en las reivindicaciones independientes. Las realizaciones de la invención se caracterizan por las reivindicaciones dependientes.

De acuerdo con un primer aspecto de la invención, se proporciona un método para proteger el intercambio de mensajes WLCP entre una TWAG de una TWAN y un UE. El método comprende derivar, por medio de un Servidor AAA de una red EPC que está interconectada con la TWAN, y por el UE, una Clave de Sesión Maestra (MSK) y una MSK Extendida (EMSK), enviar, desde el Servidor AAA a un TWAP de la TWAN y a un AP del TWAN, la MSK o la clave derivada desde al menos la MSK, y derivar, por la TWAN o por el Servidor AAA, y por el UE, desde la MSK, la EMSK o la clave derivada desde al menos la MSK o la EMSK, una clave para proteger el intercambio de mensajes WLCP.

De acuerdo con un segundo aspecto de la invención, se proporciona un método para proteger el intercambio de mensajes WLCP entre una TWAG de una TWAN y un UE. El método se realiza en colaboración con uno o más nodos que forman una TWAN, como se describe a lo largo de esta descripción. El método comprende recibir, por un TWAP de la TWAN y por un AP de la TWAN desde un Servidor AAA de una red EPC que está interconectada con la TWAN, una MSK o una clave derivada de al menos la MSK, y utilizando una clave derivada de la MSK, la clave derivada de al menos la MSK, la EMSK, o una clave derivada de al menos la EMSK, para proteger el intercambio de mensajes WLCP .

De acuerdo con un tercer aspecto de la invención, se proporciona un método para proteger el intercambio de mensajes WLCP entre una TWAG de un TWAN y un UE. El método es realizado por un Servidor AAA de una red EPC que está interconectada con la TWAN. El método comprende derivar una MSK y una EMSK, enviar, a un TWAP de la TWAN y a un AP de la TWAN, la MSK o una clave derivada de al menos la MSK, y derivar de la MSK, la EMSK, o la clave derivada de al menos la MSK o la EMSK, una clave para proteger el intercambio de mensajes WLCP.

De acuerdo con un cuarto aspecto de la invención, se proporciona un método para proteger el intercambio de mensajes WLCP entre una TWAG de una TWAN y un UE. El método es realizado por el UE. El método comprende derivar una MSK y una EMSK, y derivar de la MSK, la EMSK, o la clave derivada de al menos la MSK o la EMSK, una clave para proteger el intercambio de mensajes WLCP.

De acuerdo con un quinto aspecto de la invención, se proporciona un programa de ordenador. El programa de ordenador comprende instrucciones ejecutables por ordenador para hacer que un dispositivo realice el método de acuerdo con uno de los aspectos primero, segundo, tercero o cuarto de la invención, cuando se ejecutan las instrucciones ejecutables por ordenador en una unidad de procesamiento comprendida en el dispositivo.

De acuerdo con un sexto aspecto de la invención, se proporciona un producto de programa de ordenador que comprende un medio de almacenamiento interpretable por ordenador. El medio de almacenamiento interpretable por ordenador dispone del programa de ordenador incorporado en el mismo, según al quinto aspecto de la invención.

De acuerdo con un séptimo aspecto de la invención, se proporciona un nodo TWAN. El nodo TWAN realiza una TWAG del TWAN y un TWAP del TWAN. El nodo TWAN comprende medios de procesamiento que sirven para recibir, desde un Servidor AAA de una red EPC que se interconecta con el TWAN, una MSK o una clave derivada de al menos la MSK, y usar una clave derivada de la MSK, la clave derivada de al menos la MSK, una EMSK, o una clave derivada de al menos la EMSK, para proteger el intercambio de mensajes WLCP. Opcionalmente, el nodo TWAN puede realizar además un AP del TWAN, y puede comprender un interfaz WLAN operativo para comunicarse con el UE.

De acuerdo con un octavo aspecto de la invención, se proporciona un Servidor AAA para una red EPC que está interconectada con un TWAN. El Servidor AAA comprende medios de procesamiento que sirven para derivar una MSK y una EMSK, enviar la MSK o una clave derivada de al menos la MSK a un TWAP del TWAN y un AP del TWAN, y derivar, de la MSK, la EMSK, o la clave derivada de al menos la MSK o la EMSK, una clave para proteger el intercambio de mensajes WLCP entre una TWAG del TWAN y un UE que se comunica con el AP.

De acuerdo con un noveno aspecto de la invención, se proporciona un UE. El UE comprende un interfaz WLAN que funciona para comunicarse con un AP de un TWAN y medios de procesamiento. Los medios de procesamiento sirven para derivar una MSK y una EMSK, y derivar de la MSK, la EMSK o la clave derivada de al menos la MSK o la EMSK, una clave para proteger el intercambio de mensajes WLCP con una TWAG del TWAN.

A lo largo de esta descripción, se supone que un TWAN 110 está interconectado, a veces denominado integrado en una red EPC como un acceso fiable no 3GPP a través del interfaz STa al Servidor 103 3GPP AAA y a través del interfaz S2a a la PDN GW 102, como se describe en la sección 16 de TS 23.402 y se ilustra en la figura 1.

La invención hace uso del entendimiento de que la protección puede proporcionarse como parte del propio protocolo WLCP, aliviando así la necesidad de un despliegue seguro, confiando en las direcciones MAC, o similares.

Las soluciones propuestas aprovechan el material de codificación existente, la MSK, la EMSK, o una clave derivada de al menos la MSK o la EMSK, para derivar un nuevo material de claves para proteger el intercambio de mensajes WLCP en la capa de aplicación entre la TWAG y el UE, lo que a lo largo de esta descripción también se conoce como clave WLCP.

De acuerdo con una realización de la invención, la MSK o la clave derivada de al menos la MSK se envía desde el TWAP o desde el AP a la TWAG, y la clave para proteger el intercambio de mensajes WLCP se deriva por la TWAG de la MSK o la clave derivada de al menos la MSK.

De acuerdo con otra realización de la invención, la clave para proteger el intercambio de mensajes WLCP se deriva del TWAP o del AP, y se envía posteriormente desde el TWAP o el AP, respectivamente, a la TWAG.

De acuerdo con una realización adicional de la invención, la clave para proteger el intercambio de mensajes WLCP es derivada por el Servidor AAA y por el UE de la EMSK o la clave derivada de al menos la EMSK. La clave para proteger el intercambio de mensajes WLCP se envía desde el Servidor AAA al TWAP, y posteriormente desde el TWAP a la TWAG.

De acuerdo con una realización de la invención, una clave AP es derivada por el TWAP y por el UE a partir de la MSK o la clave derivada de al menos la MSK, y enviada desde el TWAP al AP. Otras claves se derivan por el AP y por el UE desde la clave del AP para su uso por una capa 802.11 para proteger un enlace aéreo entre el AP y el UE.

De acuerdo con otra realización de la invención, una clave AP es derivada por el Servidor AAA y por el UE a partir de la MSK o la clave derivada de al menos la MSK, la clave AP es enviada desde el Servidor AAA al TWAP, y posteriormente enviada desde el TWAP al AP. Otras claves son derivadas por el AP y por el UE de la clave AP para su uso por una capa 802.11 para proteger un enlace aéreo entre el AP y el UE

De acuerdo con otra realización más de la invención la clave para proteger el intercambio de mensajes WLCP es derivada por el Servidor AAA de la MSK o la clave derivada de al menos la MSK, y una clave AP es derivada por el

Servidor AAA y por el UE de la MSK o la clave derivada de al menos la MSK. La clave para proteger el intercambio de mensajes WLCP y la clave AP se envían desde el Servidor AAA al TWAP. A continuación, la clave para proteger el intercambio de mensajes WLCP se envía desde el TWAP a la TWAG, y la clave AP se envía desde el TWAP al AP. Otras claves son derivadas por el AP y por el UE a partir de la clave del AP para su uso por una capa 802.11 para proteger un enlace aéreo entre el AP y el UE.

Aunque las ventajas de la invención se han descrito en algunos casos con referencia a las realizaciones del primer aspecto de la invención, el razonamiento correspondiente se aplica a las realizaciones de otros aspectos de la invención.

Otros objetivos, características y ventajas de la invención se harán evidentes al estudiar la siguiente descripción detallada, los dibujos y las reivindicaciones adjuntas. Los expertos en la materia apreciarán que se pueden combinar diferentes características de la invención para crear realizaciones distintas de las que se describen a continuación.

Breve descripción de los dibujos

Lo anterior, así como los objetivos, características y ventajas adicionales de la invención, se entenderán mejor a través de la siguiente descripción ilustrativa y no limitativa de las realizaciones de la invención, con referencia a los dibujos adjuntos, en los que:

La figura 1 muestra la arquitectura carente de la función tránsito para el acceso TWAN a una red EPC, de acuerdo con una realización de la invención.

La figura 2 muestra las unidades funcionales de un TWAN, de acuerdo con otra realización de la invención.

La figura 3 ilustra la unión inicial de un UE a un TWAN, como se conoce en la técnica.

La figura 4 ilustra la unión inicial de un UE a un TWAN, de acuerdo con una realización de la invención.

La figura 5 ilustra la unión inicial de un UE a un TWAN, de acuerdo con otra realización de la invención.

La figura 6 ilustra la derivación de la clave AP por TWAP, de acuerdo con una realización de la invención.

La figura 7 ilustra la derivación de la clave AP por el Servidor AAA, de acuerdo con otra realización de la invención.

La figura 8 ilustra la unión inicial de un UE a un TWAN, de acuerdo con una realización adicional de la invención.

La figura 9 muestra dispositivos, de acuerdo con las realizaciones de la invención.

Todas las figuras son esquemáticas, no necesariamente a escala, y en general solo muestran las partes que son necesarias para dilucidar la invención, en donde otras partes pueden omitirse o simplemente sugerirse.

Descripción detallada

La invención se describirá ahora con más detalle en este documento de aquí en adelante con referencia a los dibujos adjuntos, en los que se muestran ciertas realizaciones de la invención. Sin embargo, esta invención puede realizarse de muchas formas diferentes y no debe interpretarse como limitada a las realizaciones establecidas en el presente documento. Más bien, estas realizaciones se proporcionan a modo de ejemplo para que esta descripción sea exhaustiva y completa y transmita completamente el alcance de la invención a los expertos en la materia.

El flujo de llamadas mostrado en la figura 3 ilustra cómo un UE 101 se conecta a un TWAN 110, negocia el uso del Modo de Conexión Múltiple (MCM) y establece una Conexión PDN. La figura 3 se vuelve a producir a partir de TS 23.402 (rev 12.3.0), sección 16.2 (Figura 16.2.1-1), con algunas partes simplificadas para mayor claridad y la autenticación (bloque 4 en la figura 3) expandida en etapas individuales. Téngase en cuenta que la etapa 14 se puede realizar después del bloque 4, es decir, arranca mediante una autenticación satisfactoria, o se puede realizar durante el bloque 4, por ejemplo, mediante una autenticación adicional como se describe en la solicitud de cambio C4-140308, "STa Authentication for Trusted WLAN access", 3GPP TSG CT4 Reunión # 64, Guangzhou, República Popular China, 20-24 de enero de 2014. Las etapas detalladas de la autenticación, como se muestra en el bloque 4 de la figura 3, también se pueden encontrar en TS 33.402, sección 6.2 (rev 12.3.0). Más específicamente, las etapas que se muestran en el bloque 4 de la figura 3 corresponden a las etapas 2-5 y 10-24 de la figura 6.2-1 en TS 33.402. Una vez finalizado el procedimiento que se muestra en la figura 3, el UE 101 puede establecer conexiones PDN adicionales ejecutando nuevamente las etapas en el bloque 17 de la figura 3, por ejemplo, para un APN diferente.

El método de autenticación EAP actual utilizado por un TWAN 110 para autenticar mutuamente el UE 101 y la red EPC, y para derivar claves para la protección en el enlace aéreo 802.11, es EAP-AKA', que se especifica en RFC 5448 ("Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')"). El principio básico en todos los métodos EAP actuales para la autenticación basada en SIM, es decir, EAP-SIM, EAP-AKA y EAP-AKA', es similar: una MSK se genera tanto en el UE como en el Servidor AAA, y se proporciona desde el Servidor AAA al AP WLAN. El UE y el AP luego ejecutan el acuse de recibo de cuatro vías

(bloque 15 en la figura 3) para derivar material de claves de la MSK para la protección de enlace aéreo 802.11. Téngase en cuenta que el AP 111 es una posible entidad en la WLAN AN que puede realizar las acciones descritas en esta descripción, y se apreciará que otras entidades de la WLAN AN pueden realizar las mismas tareas.

La MSK, así como la MSK Extendida (EMSK), se generan a partir de CK 'e IK', como se conoce en la técnica (véase, por ejemplo, TS 33.402, sección 6.2, y RFC 5448). Más específicamente, CK 'e IK' son generadas por el Servidor de Abonado Doméstico (HSS) 104 y se proporcionan al Servidor 103 AAA, como parte del vector de autenticación (bloque 7 de la figura 3), e independientemente por la aplicación del Módulo de Identidad del Abonado Universal (USIM) en el UE 101. La aplicación USIM se proporciona normalmente en una Tarjeta de Circuito Integrado Universal (UICC), la llamada tarjeta SIM.

A continuación, se describen realizaciones de la invención con referencia a la figura 4, que ilustra un flujo de llamadas para la autenticación EAP, incluida la derivación de la clave (estado de la técnica) para la protección en el enlace aéreo 802.11 y la derivación de la clave propuesta para la protección WLCP.

De acuerdo con las especificaciones actuales de 3GPP, y mostradas en el bloque 4 de la figura 4, se realiza el procedimiento EAP-AKA' entre el UE 101 y el Servidor 103 AAA para derivar la MSK y la EMSK der acuerdo con RFC 5448 en el UE 101 (etapa 10 en la figura 4) y el Servidor 103 AAA (etapa 8 en la figura 4) (véase 3GPP TS 33.402, sección 6.2, etapas 12 y 15, respectivamente). En la etapa 15 de la figura 4, la MSK se proporciona desde el Servidor 103 AAA al TWAP 113 y al AP 111. Téngase en cuenta que, a lo largo de la presente descripción, el material de claves derivado de al menos la MSK puede ser proporcionado desde el Servidor 103 AAA al TWAP 113 y al AP 111 en lugar de la propia MSK. Por ejemplo, el material de codificación puede ser la propia MSK, es decir, clave = MSK, se puede obtener mediante truncamiento, por ejemplo, utilizando solo los Bits Menos Significativos, clave = LSBs (MSK,32), puede ser obtenida por medio de una función de derivación de clave (KDF), por ejemplo, clave = KDF (MSK), puede ser un subconjunto en el sentido más estricto de la palabra, por ejemplo, los bits número 3, 27, 43, 53, 54, ... , de la MSK, o similar.

Téngase en cuenta que los mensajes EAP enviados entre el Servidor 103 AAA y el UE 101 están típicamente encapsulados y transportados por otro protocolo. Entre el Servidor 103 AAA y la TWAN 110, es decir, entre el Servidor 103 AAA y el TWAP 113, así como entre el TWAP 113 y el AP 111, Diámetro o RADIOUS son frecuentemente utilizados, mientras que EAPoL (EAP sobre LANs) se utiliza normalmente entre el AP 111 y el UE 101. Dichos protocolos de proveedor también pueden transportar otros elementos de información. Por ejemplo, la información del cargo se puede intercambiar entre el Servidor 103 AAA y el TWAP 113 y/o el AP 111. La MSK, o una clave derivada de al menos la MSK, se envía desde el Servidor 103 AAA al TWAP 113 y/o al AP 111 en el nivel de protocolo del portador, Así, en la etapa 15, la MSK, no se incluye en el elemento de información EAP-Satisfactorio pero en su lugar se incluye en el(los) otro(s) elemento(s) de información. Obsérvese también que la MSK no se envía al UE 101 en la etapa 16 sino que la deriva el UE 101 en la etapa 10.

Durante el acuse de recibo de cuatro vías, bloque 23 en la figura 4, el UE 101 y el AP 111 derivan claves de la MSK que son utilizadas por la capa 802.11 para proteger el enlace aéreo.

Las realizaciones de la invención utilizan la MSK, la EMSK, o una clave derivada de al menos la MSK o de la EMSK, para derivar también una clave WLCP, también denominada clave de sesión WLCP, para proteger la señalización WLCP entre la TWAG 112 y el UE 101.

De acuerdo con una primera realización, mostrada en el bloque 18 en la figura 4, la MSK, o el material de clave derivado de al menos la MSK se proporciona a la TWAG 112 en la etapa 19 o en la 20, respectivamente. Por ejemplo, el material de codificación puede ser la propia MSK, obtenida por truncamiento o mediante una KDF, o un subconjunto de la MSK.

La MSK, o el material de clave derivado de al menos la MSK, puede enviarse desde el TWAP 113 a la TWAG 112 en la etapa 19. Opcionalmente, la etapa 19 se puede combinar con la etapa 17. Alternativamente, la MSK, o el material de codificación derivado de al menos la MSK, puede enviarse desde el AP 111 a la TWAG 112 en la etapa 20. Por ejemplo, el centro distribuidor de radio del AP 111 puede estar controlado por un nodo central, el Controlador de Acceso (AC) (no ilustrado en las figuras), y el AP 111 y el AC se comunican a través del protocolo de Control y Aprovisionamiento de Puntos de Acceso Inalámbrico (CAPWAP). Si el AC y la TWAG 112 están situados conjuntamente, la MSK puede enviarse a la TWAG 112 a través de CAPWAP.

En las etapas 21 y 22, el UE 101 y la TWAG 112 derivan de forma independiente una clave que se puede usar para proteger el tráfico WLCP. Esta clave, llamada clave WLCP, se deriva de la MSK o del material de clave derivado de al menos la MSK, obtenido por la TWAG 112 en la etapa 19 o 20. Dado que la MSK se deriva de un funcionamiento EAP-AKA, EAP-AKA' o EAP-SIM, el material de codificación derivado y la clave WLCP serán nuevos. Por lo tanto, los tipos de repetición de ataques se ven obstaculizados. El material de codificación puede estar vinculado a un identificador asociado con la TWAG 112, como se conoce en la técnica, para mitigar el riesgo de que una TWAG suplante a otra TWAG hacia el UE 101.

Una segunda realización, que se ilustra en la figura 5, es similar a la primera realización pero difiere de la primera realización en esa etapa 19, la derivación de la clave WLCP, no la realiza la TWAG 112 sino el TWAP 113 o por el

AP 111. En este caso, la clave WLCP se envía a la TWAG 112 en la etapa 20, si la ha generado el TWAP 113, o en la etapa 21, si la ha generado el AP 111.

La clave WLCP puede derivarse utilizando una KDF, por ejemplo, clave WLCP = KDF (MSK, parámetro (s) de entrada). En lugar de la MSK, se puede usar material de clave derivado de al menos la MSK. Los parámetros de entrada pueden ser cualquier información disponible para las entidades que deriven la clave única WLCP. Por ejemplo, un identificador de TWAG se puede usar como parámetro de entrada tal como la dirección IP TWAG (suministrada al UE 101 en el EAP) o la dirección TWAG MAC, que se puede descubrir por medio de Protocolo de Resolución de Direcciones (ARP)/Descubrimiento de Vecinos (ND).

Común a ambas realizaciones es que la TWAG 112 y el UE 101 pueden derivar otras claves, por ejemplo, para la protección de encriptación e integridad. Los mensajes de WLCP se protegen luego utilizando la (s) clave (s) adicional (es) derivada (s) por ejemplo, la solicitud de conexión PDN y los mensajes de Respuesta en las etapas 26 y 29.

Existen múltiples maneras en que las claves derivadas pueden ser utilizadas para proteger el tráfico WLCP. Un ejemplo es usar Seguridad de la Capa de Transporte de Datagramas (DTLS) con una combinación de cifrado de clave pre compartida. En este caso, la clave pre compartida estaría relacionada con la clave WLCP. Una alternativa es Integrar la seguridad en el propio protocolo WLCP. Esto se puede hacer, por ejemplo, incluyendo un número secuencial en cada mensaje WCLP, usando la clave WLCP para calcular un código de Autenticación de Mensajes (MAC) para cada mensaje, y a continuación, agregar el MAC al mensaje antes de transmitirlo. El receptor puede verificar que el MAC es correcto tras la recepción.

Además, también se puede añadir un cifrado. El(Los) algoritmo (s) a usar para el cifrado se puede(n) negociar durante el acuse de recibo DTLS, si se usa DTLS. Si la seguridad está incorporada en el propio protocolo WLCP, entonces se puede agregar un mecanismo para acordar qué algoritmo (s) a usar se puede (n) agregar al protocolo WLCP. Un ejemplo de tal mecanismo es que el UE 101 informe a la TWAG 112 sobre qué algoritmos soporta, y la TWAG 112 hace una elección basándose en esta información. Por ejemplo, la TWAG 112 puede devolver una lista de algoritmos que el UE 101 soporta al UE 101 en un mensaje de integridad protegida. El UE 101 puede entonces verificar que la lista no haya sido manipulada durante la transmisión. Otra alternativa más es que los algoritmos de cifrado estén pre configurados o definidos en la normalización.

Téngase en cuenta que las etapas en el bloque 18 de las figuras 4 y 5, configuración de la clave WLCP, se pueden realizar en cualquier momento cuando sea conocida la MSK por el TWAP 113 o el AP 111, pero antes de que comience el bloque 25. Por ejemplo, el bloque 18 se puede realizar después del acuse de recibo de cuatro vías en el bloque 23.

Cuando se realiza una re autenticación, el Servidor 103 AAA y el UE 101 re utilizan las claves derivadas durante la autenticación completa anterior para generar una nueva MSK. Como parte del proceso de re autenticación, la nueva MSK, o el material de claves derivado de al menos la MSK, también se suministra al TWAP 113 y al AP 111. El UE 101 y el AP 111 ejecutan entonces el acuse de recibo de cuatro vías para negociar nuevo material de clave para la protección del enlace aéreo 802.11. Después del proceso de re autenticación, las claves WLCP también pueden ser renovadas. Una forma de lograr esto es volver a ejecutar el bloque 18 descrito anteriormente con referencia a las figuras 4 y 5 en cada re autenticación. En este enfoque, y cuando la TWAG 112 realiza la etapa 22 en la figura 4, la TWAG 112 necesita ser informada por el TWAP 113 o por el AP 111 de que ha tenido lugar una re autenticación. Tal notificación incluiría la nueva MSK, o el material de clave derivado de al menos la MSK.

Otra forma es agregar un mecanismo de cambio de clave al protocolo WLCP. Se envía un nuevo mensaje WLCP de la TWAG 112 al UE 101 que indica cuándo cambiar a la nueva clave establecida durante la autenticación.

De acuerdo con el estado de la técnica, la MSK se proporciona al AP 111 en la etapa 15 de las figuras 4 y 5. La MSK se usará para el acuse de recibo de cuatro vías entre el UE 101 y el AP 111 en el bloque 23. Sin embargo, dado que el enlace entre el TWAP 113 y el AP 111 puede ser inseguro, y/o la MSK podría ser extraída de un AP comprometido, un competidor puede adquirir la clave y derivar la clave WLCP. Por lo tanto, puede ser ventajoso abstenerse de enviar la MSK al AP 111.

Por lo tanto, de acuerdo con una tercera realización, el TWAP 113 puede derivar una clave adicional, llamada clave AP, de la MSK, o material de claves derivado de al menos la MSK, que luego se envía al AP 111. Con el fin de realizar esto, la etapa 15 en las figuras 4 y 5 se divide en varias sub-etapas que se describen a continuación con referencia a la figura 6. Téngase en cuenta que el UE 101 puede derivar la clave AP en cualquier momento antes del acuse de recibo de cuatro vías (bloque 23 de las figuras 4 y 5).

En la etapa 15b que se muestra en la figura 6, después de que el TWAP 113 haya recibido la MSK o el material de claves derivado de al menos la MSK en la etapa 15a, deriva la clave AP. La clave AP se deriva de tal manera que también puede ser derivada por el UE 101 en la etapa 15c. En la etapa 15d, el TWAP 113 envía la clave AP al AP 111. En la etapa 23, en las figuras 4 y 5, durante el acuse de recibo de cuatro vías, el UE 101 y el AP 111 derivan las claves de la clave AP para su uso por la capa 802.11 para proteger el enlace aéreo.

De acuerdo con una cuarta realización, ilustrada en la figura 7, la clave AP puede derivarse de la MSK, o del material de claves derivado de al menos la MSK, en la etapa 15a por el Servidor 103 AAA en lugar del TWAP 113. En este caso, el Servidor 103 AAA envía la MSK, o el material de claves derivado de al menos la MSK, y la clave AP al TWAP 113 en la etapa 15b, y el TWAP 113 solo envía la clave AP al AP 111 en la etapa 15d. El UE 101 deriva la misma clave AP en la etapa 15c.

La clave AP puede derivarse utilizando una KDF, por ejemplo, clave AP = KDF (MSK, parámetro (s) de entrada). En lugar de la MSK, se puede usar el material de claves derivado de al menos la MSK. Los parámetros de entrada pueden ser cualquier información disponible para las entidades que derivan la clave AP y que hace que la clave AP derivada sea única. Por ejemplo, el Identificador del Conjunto de Servicios (SSID), el Identificador del Conjunto de Servicios Básicos (BSSID), o el Identificador del Conjunto de Servicios Extendido Homogéneo (HESSID), del AP se pueden utilizar como parámetros de entrada.

De acuerdo con una quinta realización, la clave WLCP y la clave AP pueden derivarse de la MSK, o del material de claves derivado de al menos la MSK, por el Servidor 103 AAA en la etapa 15a, de acuerdo con los mecanismos de derivación descritos para las realizaciones anteriores, en particular con referencia a la figura 7. El Servidor 103 AAA enviaría la clave AP y la clave WLCP al TWAP 113 en la etapa 15b, y el TWAP 113 envía la clave WLCP a la TWAG 112 y la clave AP al AP 111 en la etapa 15d. El UE 101 obtiene la clave WLCP y la clave AP de acuerdo con la etapa 15c.

De acuerdo con una sexta realización, la clave WLCP puede derivarse de la EMSK, o del material de claves derivado de al menos la EMSK, por el Servidor 103 AAA en la etapa 15a, de acuerdo con los mecanismos de derivación de claves descritos para realizaciones anteriores, en particular con referencia a las figuras 6 y 7. La EMSK es una clave similar a la MSK y la derivan el UE 101 y el Servidor 103 AAA al mismo tiempo que la MSK. Actualmente se utiliza para la movilidad basada en IP y se describe en 3GPP TS 33.402, sección 6.2. El Servidor 103 AAA enviaría entonces la clave WLCP y la MSK al TWAP 113 en la etapa 15b, y el TWAP 113 envía la clave WLCP a la TWAG 112 en la etapa 15d y la MSK al AP 111. El UE 101 deriva la clave WLCP correspondiente en la etapa 15c.

Con el fin de aclarar aún más la sexta realización, derivar la clave WLCP de la EMSK por el Servidor 103 AAA y por el UE 101 se describe con más detalle a continuación y se ilustra en la figura 8.

Con este fin, con referencia a las figuras 1 y 2, una TWAN 110 está interconectada con la red EPC como un acceso fiable no 3GPP a través del interfaz STa al 3GPP Servidor 103 AAA y a través del interfaz S2a al PDN GW 102, como se describe en la sección 16 de TS 23.402.

Además con referencia a la sección 16 de TS 23.402, hay tres modos de conexión para la TWAN (Modo de Conexión Unica, Modo de Conexión Múltiple y Modo de Conexión Unica Transparente), y la negociación del modo de conexión se lleva a cabo durante la autenticación de acceso EAP-AKA'.

En caso de que se haya negociado el Modo de Conexión Única o el Modo de Conexión Única Transparente durante la autenticación de acceso EAP-AKA, se utilizará la autenticación y el acuerdo de clave como se describe en la sección 6.2 de TS 33.402.

En caso de que el Modo de Conexión Múltiple fuera negociado durante la autenticación de acceso EAP-AKA', el WLCP se usa entre el UE 101 y la TWAG 112 para controlar, por ejemplo, la configuración y la interrupción, las conexiones PDN a través del acceso TWAN. En este caso, se utilizará la autenticación y el acuerdo de claves como se describe en la sección 6.2 de TS 33.402, con las siguientes excepciones y adiciones.

En primer lugar, se realizan las etapas 1-14 en la figura 8. Estas etapas corresponden a las etapas 1-22A descritas en la sección 6.2 de TS 33.402. Como resultado, el UE 101 y el Servidor AAA 103 están en posesión de la MSK y de la EMSK, derivadas de CK' e IK' de acuerdo con RFC 5448, por el Servidor 103 AAA en la etapa 8 e, independientemente, por el UE 101 en la etapa 10.

A continuación, en la etapa 15, el Servidor 103 AAA deriva la clave WLCP de la EMSK similar a lo que se describió anteriormente en este documento para obtener la clave WLCP de la MSK. Más específicamente, la clave WLCP se puede derivar de la MSK usando una KDF, por ejemplo, clave WLCP = KDF (EMSK, parámetro(s) de entrada). En lugar de la EMSK, se puede utilizar material de claves derivado de al menos la EMSK. Los parámetros de entrada pueden ser cualquier información disponible para las entidades que derivan la clave WLCP y que hace que la clave WLCP derivada sea única. Por ejemplo, se puede usar un identificador TWAG como parámetro de entrada, tal como la dirección IP TWAG (suministrada al UE en EAP) o la dirección MAC TWAG, que se puede descubrir a través de ARP/ND.

En la etapa 16, el Servidor 103 AAA envía el mensaje EAP-Satisfactorio al TWAP 113 en la TWAN 110, opcionalmente precedido por una Notificación EAP, como se explica en la etapa 19 descrita en la sección 6.2 de TS 33.402. El Servidor 103 AAA también incluye la MSK y la clave WLCP en el mensaje de protocolo AAA subyacente, es decir, no en el nivel EAP.

En la etapa 21, al recibir el mensaje EAP-Satisfactorio, la MSK y la clave WLCP, el TWAP 113 proporciona la clave WLCP a la TWAG 112 que se usará para proteger la señalización WLCP entre el UE 101 y la TWAG 112. La etapa también puede ocurrir después, o en paralelo con las etapas 17-19.

En la etapa 17, el TWAP 113 reenvía el mensaje EAP-Satisfactorio al autenticador en la WLAN AN, es decir, el AP 111, opcionalmente precedido por una Notificación EAP, tal como se explica en la sección 6.2 de TS 33.402 en relación con la etapa 19. El TWAP 113 también incluye la MSK en el mensaje del protocolo AAA subyacente, es decir, no en el nivel EAP. El AP 111 almacena el material de codificación que se utilizará en la comunicación con el UE 101 autenticado, tal como lo requiere la WLAN AN.

En la etapa 18, el AP 111 informa al UE 101 sobre la autenticación satisfactoria con el mensaje EAP-Satisfactorio.

En la etapa 19, el UE 101 deriva la clave WLCP de la EMSK de manera similar a como lo hizo el Servidor 103 AAA en la etapa 15. Esto puede suceder tan pronto como el proceso de autenticación se haya completado satisfactoriamente, es decir, después de recibir el EAP-Satisfactorio o después de recibir la Notificación EAP'AKA opcional en la etapa 12.

Ahora el intercambio EAP AKA' se ha completado satisfactoriamente, y el UE 101 y el AP 111 comparten el material de codificación derivado durante ese intercambio, y el UE 101 y el AP 111 pueden realizar el acuse de recibo de cuatro vías (bloque 22 en la figura 8).

En el caso de una re autenticación rápida, las realizaciones de la invención funcionan de acuerdo con la sección 6.3 de TS 33.402, con la excepción de que las nuevas claves se derivan de acuerdo con lo que se describe en el presente documento.

Opcionalmente, la señalización WLCP entre el UE 101 y la TWAG 112 utilizada para establecer las Conexiones PDC puede protegerse por medio de DTLS, usando una clave previamente compartida como se define en RFC 6347. La clave utilizada para DTLS es la clave WLCP, derivada por el UE 101 y el Servidor 103 AAA como se describe anteriormente en este documento. En este caso, el UE 101 establece una conexión DTLS con la TWAG 112 después de la autenticación satisfactoria en caso del Modo de Conexión Múltiple. El UE 101 y la TWAG 112 soportarán DTLS como se define en RFC 6347, y de acuerdo con el perfil dado en el Anexo E de TS 33.310.

Las realizaciones de la invención pueden realizarse en los dispositivos que, de acuerdo con las especificaciones de 3GPP, se denominan UE, AP, TWAP, TWAG, Servidor AAA, y similares, como se ilustra en las figuras. 1 y 2. Dichos dispositivos comprenden un interfaz de red y medios de procesamiento, como un procesador y una memoria que almacena instrucciones ejecutables, es decir, programas de ordenador, adaptados para realizar las realizaciones de los métodos descritos anteriormente en el presente documento. El interfaz de red puede comprender cualquier circuitería de interfaz conocida operativa para transmitir y recibir datos a través de una red de comunicaciones, por ejemplo, Ethernet, WLAN o una red 3GPP como el Sistema Global para Comunicaciones con Móviles (GSM), Sistema Universal de Telecomunicaciones con Móviles (UMTS), o Evolución a Largo Plazo (LTE). Los medios de procesamiento pueden comprender un circuito de procesamiento que incluya uno o más microprocesadores, microcontroladores, circuitos de hardware, o una combinación de los mismos. La memoria puede comprender tanto memoria no volátil, por ejemplo, memoria de solo lectura (ROM) y memoria flash, para almacenar el programa informático y los datos necesarios para el funcionamiento, y memoria volátil, por ejemplo, memoria de acceso aleatorio (RAM), para almacenar datos temporales.

Como ejemplo, una realización 910 del UE101 se muestra en la figura 9. El UE 910 comprende un interfaz WLAN 911, un procesador 912 y una memoria 913 que almacena instrucciones ejecutables 914 adaptadas para realizar realizaciones de los métodos descritos anteriormente en este documento. El UE 910 puede comprender interfaces de red adicionales para efectuar comunicaciones inalámbricas a través de una red 3GPP.

Como otro ejemplo, se muestra una realización 920 del Servidor 103 AAA en la figura 9. El Servidor AAA 920 comprende un interfaz de red 921, un procesador 922 y una memoria 923 que almacena las instrucciones ejecutables 924 adaptadas para realizar las realizaciones de los métodos descritos anteriormente en este documento.

Con respecto a la TWAN 110, se puede observar que las entidades funcionales mostradas en la figura 2, el TWAP 113, la TWAG 112, y el WLAN AN (que comprende al menos un AP 111), han sido definidas por 3GPP con el propósito de describir la funcionalidad requerida relacionada con el intercambio de mensajes entre la red EPC (que comprende el Servidor AAA 103), el TWAN 110 y el UE 101. Se apreciará que estas entidades pueden ser realizadas como unidades separadas, dispositivos, nodos o similares, o situados en el mismo lugar. Por ejemplo, en realización 930 de la TWAN 110 puede realizar todas las entidades funcionales, es decir, el TWAP 113, la TWAG 112, y al menos un AP 111, en un nodo único. Tal nodo TWAN 930 comprende un Interfaz WLAN 931, al menos un interfaz de red 935 adicional para comunicarse a través de los interfaces S2a y STa, un procesador 932 y una memoria 933 que almacena instrucciones ejecutables 934 adaptadas para realizar las realizaciones de los métodos descritos anteriormente.

Como alternativa, las entidades funcionales del TWAN 110 se pueden realizar como nodos separados. Por ejemplo, el TWAP 113 y la TWAG 112 se pueden realizar en un primer nodo TWAN 940 y el AP 111 se realiza en un segundo nodo 950. El primer nodo TWAN 940 comprende al menos un interfaz de red 941 para comunicarse con la red EPC (a través de los interfaces S2a y STa) y con el segundo nodo 950 TWAN, respectivamente, un procesador 942 y una memoria 943 que almacena instrucciones ejecutables 944 adaptadas para efectuar las realizaciones de los métodos descritos anteriormente en este documento. El AP 950 comprende un interfaz WLAN 951, un interfaz de red adicional 955 para comunicarse con el primer nodo TWAN 940, un procesador 952 y una memoria 953 que almacena instrucciones ejecutables 954 adaptadas para efectuar las realizaciones de los métodos descritos anteriormente. En este documento. Opcionalmente, el primer nodo TWAN 940 puede servir como un CA que controla uno o más APs 950, es decir, a través de CAPWAP.

Como otra alternativa adicional, el TWAP 113, la TWAG 112, y el AP 111, pueden realizarse como nodos separados, comprendiendo cada nodo un interfaz de red para comunicarse con los otros nodos y/o la red EPC, un procesador y una memoria que almacena instrucciones ejecutables adaptadas para efectuar las realizaciones de los métodos descritos anteriormente en este documento. El nodo que realiza el AP 111 comprende adicionalmente un interfaz WLAN.

Los expertos en la materia comprobarán que la invención no se limita de ninguna manera a las realizaciones descritas anteriormente. Por el contrario, son posibles muchas modificaciones y variaciones dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para proteger una Red de Area Local Inalámbrica, WLAN, el Protocolo de Control, WLCP, el intercambio de mensajes entre una Pasarela de Acceso WLAN Fiable, TWAG, (112) de una Red de Acceso WLAN Fiable, TWAN, (110) y un Equipo de Usuario , UE, (101) que comprende:

derivar, por medio de un Servidor (103) de Autenticación, Autorización y Contabilización, AAA, de una red de Núcleo de Paquetes Evolucionado, EPC, interconectada con el TWAN, y por medio del UE, una Clave de Sesión Maestra, MSK, y una MSK Extendida, EMSK,

enviar, desde el Servidor AAA a través de un Proxy AAA WLAN Fiable, TWAP, (113) de la TWAN a un Punto de Acceso, AP, (111) de la TWAN, la MSK, y

derivar, por medio del Servidor AAA y del UE, una clave de la EMSK para proteger el intercambio de mensajes WLCP.

2. El método de acuerdo con la reivindicación 1, que comprende además:

enviar, desde el Servidor (103) AAA a la TWAP (113) la clave para proteger el intercambio de mensajes WLCP, y

enviar, desde el TWAP (113) a la TWAG (112), la clave para proteger el intercambio de mensajes WLCP.

3. El método de acuerdo con las reivindicaciones 1 o 2, que comprende además:

derivar, por el TWAP (113) y por el UE (101), una clave AP de la MSK,

enviar, desde el TWAP (113) al AP (111), la clave AP, y

derivar, por el AP (111) y por el UE (101), claves procedentes de la clave AP para su uso por una capa 802.11 para proteger un enlace aéreo entre el AP (111) y el UE (101).

4. El método de acuerdo con cualquiera de las reivindicaciones 1 a 3, que comprende además:

derivar, por el Servidor AAA (103) y por el UE (101), una clave AP de la MSK,

enviar, desde el Servidor AAA (103) al TWAP (113), la clave AP,

enviar, desde el TWAP (113) al AP (111), la clave AP, y

derivar, por el AP (111) y por el UE (101), claves procedentes de la clave AP para su uso por una capa 802.11 para proteger un enlace aéreo entre el AP (111) y el UE (101).

5. Un método para proteger una Red de Area Local Inalámbrica, WLAN, el Protocolo de Control, WLCP, el intercambio de mensajes entre una Pasarela de Acceso WLAN Fiable, TWAG, (112) de una Red de Acceso WLAN Fiable, TWAN, (110) y un Equipo de Usuario , UE, (101) que comprende:

recibir, por medio de un Proxy TWAP, (113) de Autenticación, Autorización y Contabilización, AAA, de la TWAN y de un Punto de Acceso, AP, (111) de la TWAN, desde un Servidor AAA (103) de una red de Núcleo de Paquetes Evolucionado, EPC, interconectada con la TWAN, una Clave de Sesión Maestra, MSK, y

utilizar una clave derivada de la MSK Extendida, EMSK, para proteger el intercambio de mensajes WLCP.

6. Un método para proteger una Red de Area Local Inalámbrica, WLAN, el Protocolo de Control, WLCP, el intercambio de mensajes entre una Pasarela de Acceso WLAN Fiable, TWAG, (112) de una Red de Acceso WLAN Fiable, TWAN, (110) y un Equipo de Usuario , UE, (101) que comprende:

derivar, por medio de un Servidor AAA (103) de Autenticación, Autorización y Contabilización, de una red de Núcleo de Paquetes Evolucionado, EPC, interconectada con la TWAN, una Clave de Sesión Maestra, MSK, y una MSK Extendida, EMSK,

enviar desde el Servidor AAA (103) a través de un Proxy AAA WLAN Fiable, TWAP, (113) de la TWAN a un Punto de Acceso, AP, (111) de la TWAN, la MSK y

derivar, por medio del Servidor AAA (103), de la EMSK, una clave para proteger el intercambio de mensajes WLCP.

7. Un método para proteger una Red de Area Local Inalámbrica, WLAN, el Protocolo de Control, WLCP, el intercambio de mensajes entre una Pasarela de Acceso WLAN Fiable, TWAG, (112) de una Red de Acceso WLAN Fiable, TWAN, (110) y un Equipo de Usuario , UE, (101) que comprende:

derivar, por el UE (101), una Clave de Sesión Maestra, MSK, y una MSK extendida, EMSK, y

derivar, por el UE (101), de la EMSK, una clave para proteger el intercambio de mensajes WLCP.

8. Un programa de ordenador (914, 924, 934, 944, 954) que incluye instrucciones ejecutables por ordenador para hacer que un dispositivo realice el método de acuerdo con cualquiera de las reivindicaciones 1 a 7, cuando las instrucciones ejecutables por ordenador son ejecutadas en una unidad de procesamiento (912, 922, 932, 942, 952) comprendida en el dispositivo.

9. Un producto de programa informático que comprende medios de almacenamiento interpretables por ordenador (913, 923, 933, 943, 953), teniendo los medios de almacenamiento interpretables por ordenador el programa de ordenador (914, 924, 934, 944, 954) de acuerdo con la reivindicación 8 incorporada en los mismos.

10. Un nodo (930, 940, 950) de Red de Area Local Inalámbrica Fiable, WLAN, una Red de Acceso, TWAN, que forman una Pasarela de Acceso WLAN Fiable, TWAG, (112) de la TWAN (110) y un Proxy de Autenticación, Autorización y Contabilización AAA, Fiable, TWAP, (113) de la TWAN, comprendiendo el nodo TWAN medios de procesamiento (932-934, 942-944, 952-954) que sirven para:

recibir, desde un Servidor AAA (103) de una red de Núcleo de Paquetes Evolucionado, EPC, interconectada con la TWAN, una Clave de Sesión Maestra, MSK y

usar una clave derivada de una MSK extendida, EMSK, para proteger el intercambio de mensajes WLAN Protocolo de Control WLCP, con un Equipo de Usuario, UE, (101).

11. El nodo TWAN de acuerdo con la reivindicación 10, en el que los medios de procesamiento sirven además para:

recibir, desde el Servidor AAA (103), la clave para proteger el intercambio de mensajes WLCP con el UE (101).

12. El nodo TWAN (930, 950) de acuerdo con las reivindicaciones 10 u 11, que forma además un punto de acceso, AP, (111), comprendiendo además el nodo TWAN:

una Red de Area Local Inalámbrica, WLAN, interfaz (935, 955) que sirve para comunicarse con el UE (101).

13. Un Servidor de Autenticación, Autorización y Contabilización, AAA, (103; 920) para una red de Núcleo de Paquetes Evolucionado, EPC, interconectada con una Red de Acceso WLAN Fiable, TWAN, (110) comprendiendo el Servidor AAA medios de procesamiento (922-924) que sirven para:

derivar una Clave de Sesión Maestra, MSK y una MSK extendida, EMSK,

enviar la MSK a través de un Proxy AAA WLAN Fiable, TWAP, (113) de la TWAN a un punto de acceso, AP, (111) de la TWAN, y

derivar, de la EMSK, una clave para proteger el intercambio de mensajes de Protocolo de Control WLAN, WLCP, entre una Pasarela de Acceso WLAN Fiable, TWAG, (112) de la TWAN y un equipo de usuario, UE, (101).

14. El Servidor AAA de acuerdo con la reivindicación 13, en el que los medios de procesamiento sirven además para: enviar la clave para proteger el intercambio de mensajes WLCP al TWAP (113).

15. El Servidor AAA de acuerdo con la reivindicación 13 o 14, en el que los medios de procesamiento sirven además para:

derivar una clave AP de la MSK, y

enviar la clave AP al TWAP (113).

16. Un equipo de usuario, UE, que comprende:

un interfaz (101; 910) de Red de Area Local Inalámbrica, WLAN, (911) que sirve para comunicarse con un Punto de Acceso, AP, (111) de una Red de Acceso WLAN Fiable, TWAN, (110) y

medios de procesamiento (912-914) que sirven para:

derivar una Clave de Sesión Maestra, MSK y una MSK extendida, EMSK, y

derivar de la EMSK, una clave para proteger el intercambio de mensajes WLAN Protocolo de Control, WLCP, con una Pasarela de Acceso WLAN Fiable, TWAG, (112) de la TWAN.

17. El UE de acuerdo con la reivindicación 16, en el que los medios de procesamiento sirven además para:

derivar una clave AP la MSK, y

derivar claves de la clave AP para su uso por una capa 802.11 para proteger un enlace aéreo entre el AP (111) y el UE (101; 910).

Fig. 1

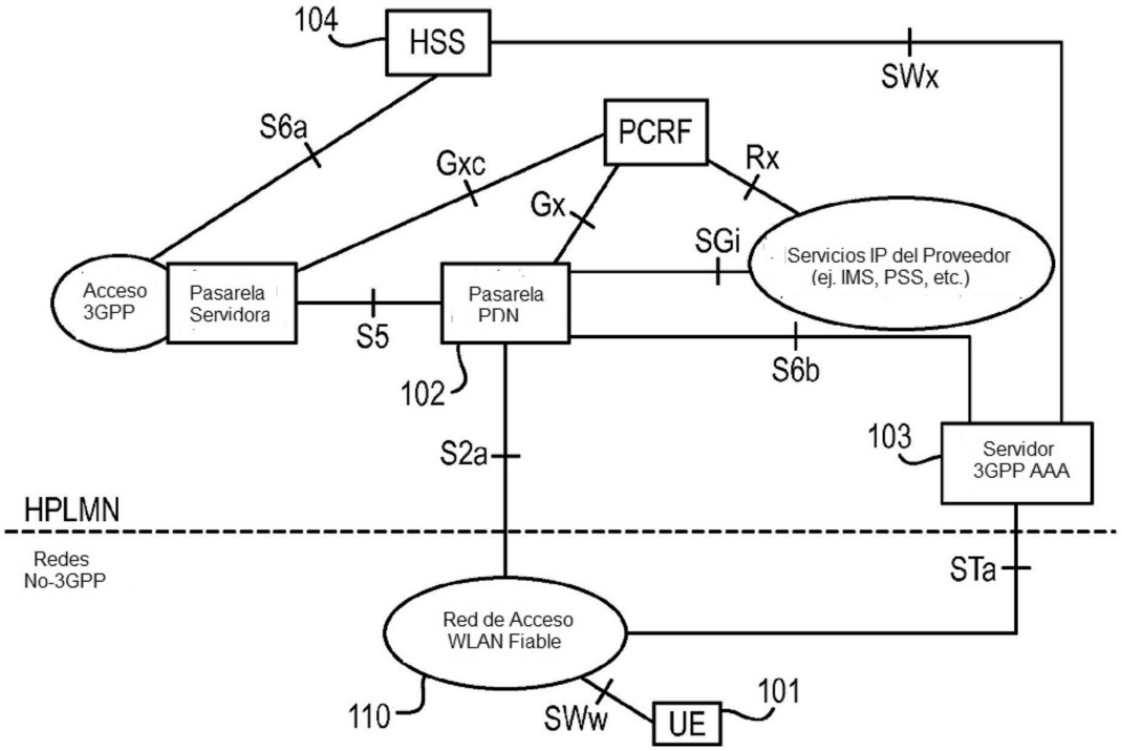

104
HSS
SWx
S6a
PCRF
Rx
Gxc
Gx
SGi
Servicios IP del Proveedor
(ej. IMS, PSS, etc.)
Acceso
3GPP
Pasarela
Servidora
Pasarela
PDN
S5
S6b
102
S2a
103
Servidor
3GPP AAA
HPLMN
Redes
No-3GPP
STa
Red de Acceso
WLAN Fiable
110
SWw
UE
101

Fig. 2

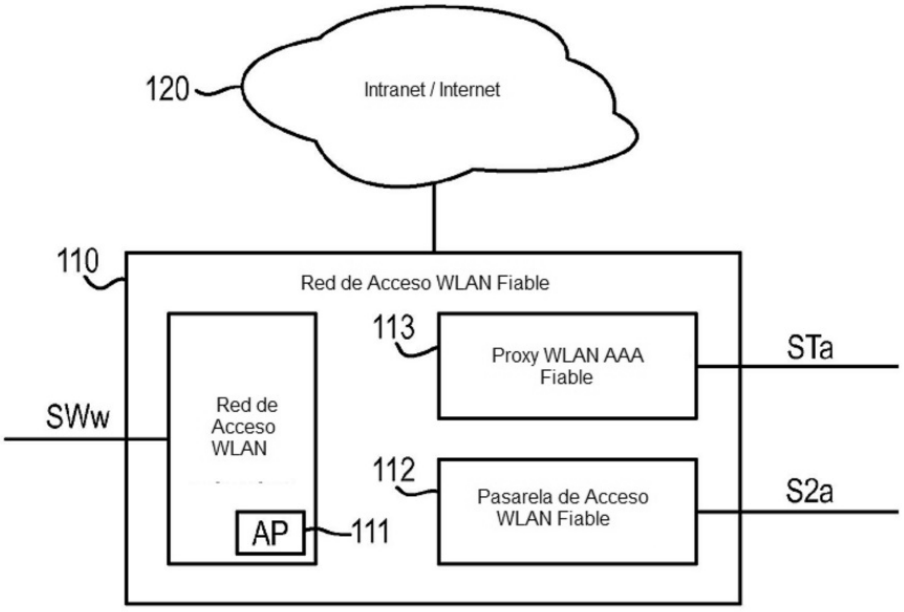

120
Intranet / Internet
110
Red de Acceso WLAN Fiable
113
Proxy WLAN AAA
Fiable
STa
SWw
Red de
Acceso
WLAN
112
Pasarela de Acceso
WLAN Fiable
S2a
AP
111

Fig. 3

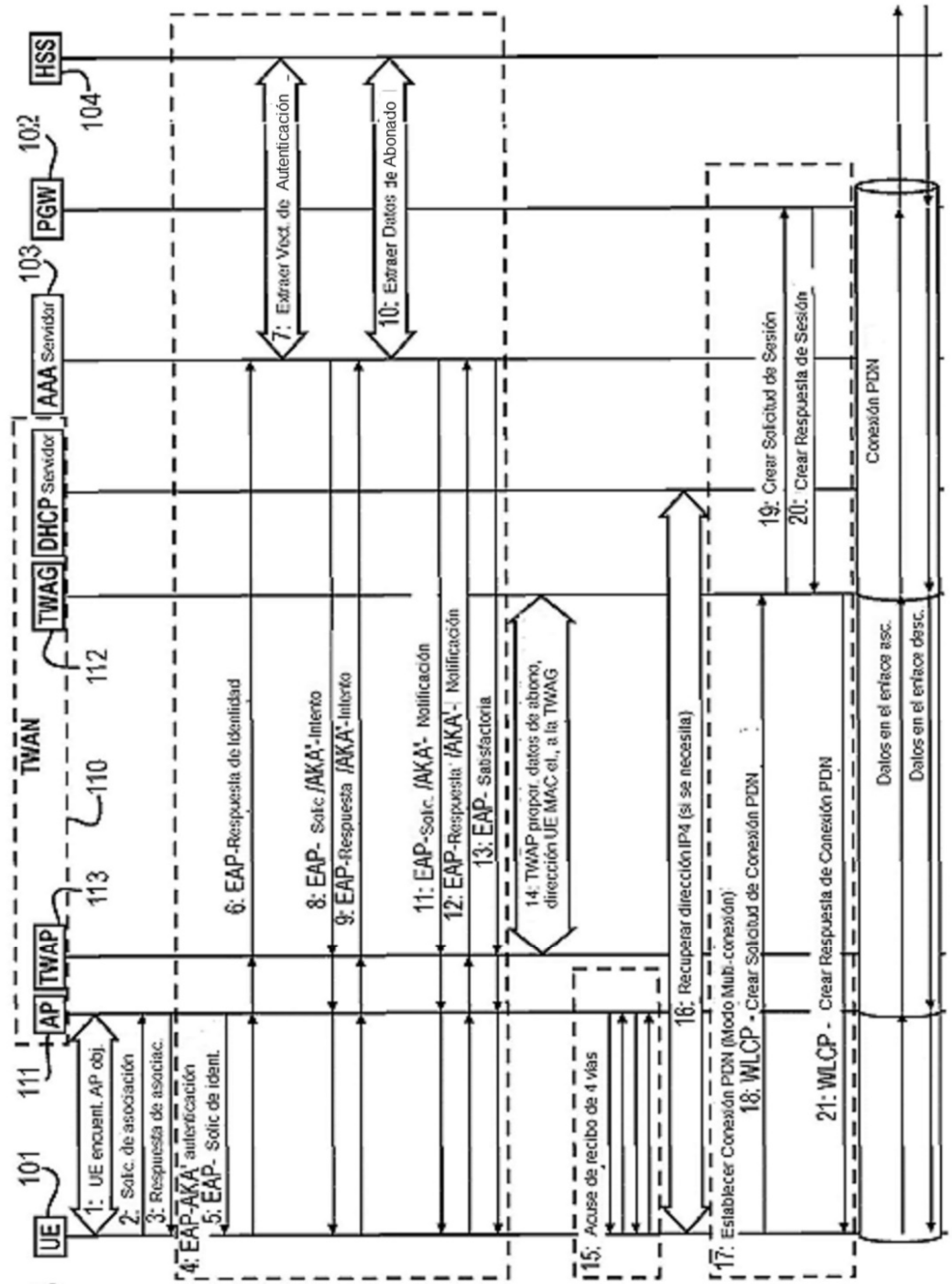

UE
101
AP
111
TWAP
113
TWAN
110
TWAG
112
DHCP Servidor
AAA Servidor
103
PGW
102
HSS
104
1: UE encuent. AP obj.
2: Solic. de asociación
3: Respuesta de asociac.
4: EAP-AKA' autenticación
5: EAP- Solic de ident.
6: EAP-Respuesta de Identidad
7: Extraer Vect. de Autenticación
8: EAP- Solic./AKA'-Intento
9: EAP-Respuesta /AKA'-Intento
10: Extraer Datos de Abonado
11: EAP-Solic. /AKA'- Notificación
12: EAP-Respuesta /AKA'- Notificación
13: EAP- Satisfactoria
14: TWAP propor. datos de abono, dirección UE MAC el., a la TWAG
15: Acuse de recibo de 4 vías
16: Recuperar dirección IP4 (si se necesita)
17: Establecer Conexión PDN (Modo Multi-conexión)
18: WLCP - Crear Solicitud de Conexión PDN
19: Crear Solicitud de Sesión
20: Crear Respuesta de Sesión
21: WLCP - Crear Respuesta de Conexión PDN
Conexión PDN
Datos en el enlace asc.
Datos en el enlace desc.

Fig. 4

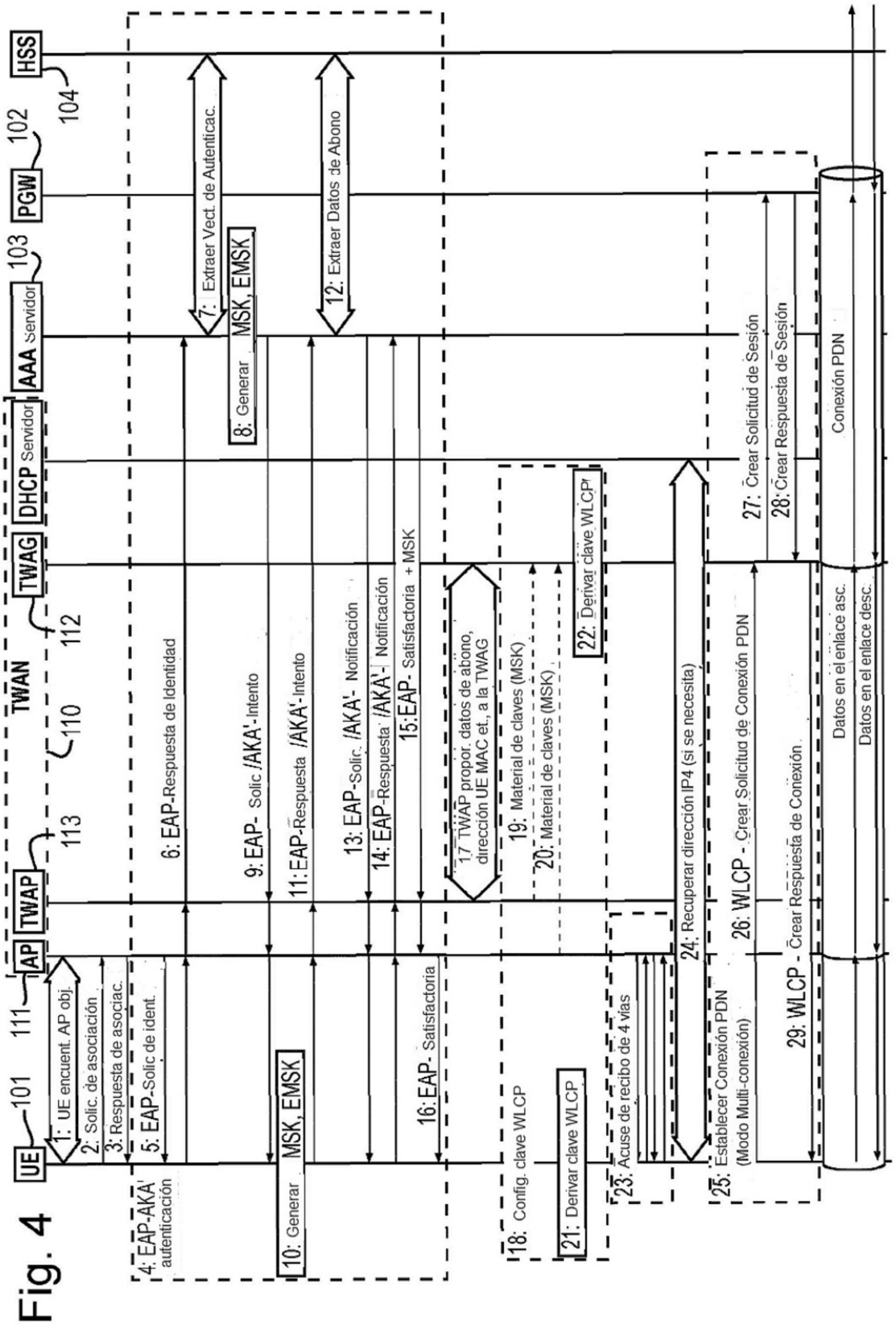

UE
101
AP
111
TWAP
113
TWAN
110
TWAG
112
DHCP Servidor
AAA Servidor
103
PGW
102
HSS
104
1: UE encuent. AP obj.
2: Solic. de asociación
3: Respuesta de asociac.
4: EAP-AKA' autenticación
5: EAP-Solic de ident.
6: EAP-Respuesta de Identidad
7: Extraer Vect. de Autenticac.
8: Generar MSK, EMSK
9: EAP- Solic /AKA'-Intento
10: Generar MSK, EMSK
11: EAP-Respuesta /AKA'-Intento
12: Extraer Datos de Abono
13: EAP-Solic. /AKA'- Notificación
14: EAP-Respuesta /AKA'- Notificación
15: EAP- Satisfactoria + MSK
16: EAP- Satisfactoria
17 TWAP propor. datos de abono, dirección UE MAC et., a la TWAG
18: Config. clave WLCP
19: Material de claves (MSK)
20: Material de claves (MSK)
21: Derivar clave WLCP
22: Derivar clave WLCP
23: Acuse de recibo de 4 vías
24: Recuperar dirección IP4 (si se necesita)
25: Establecer Conexión PDN (Modo Multi-conexión)
26: WLCP - Crear Solicitud de Conexión PDN
27: Crear Solicitud de Sesión
28: Crear Respuesta de Sesión
29: WLCP - Crear Respuesta de Conexión
Conexión PDN
Datos en el enlace asc.
Datos en el enlace desc.

Fig. 5

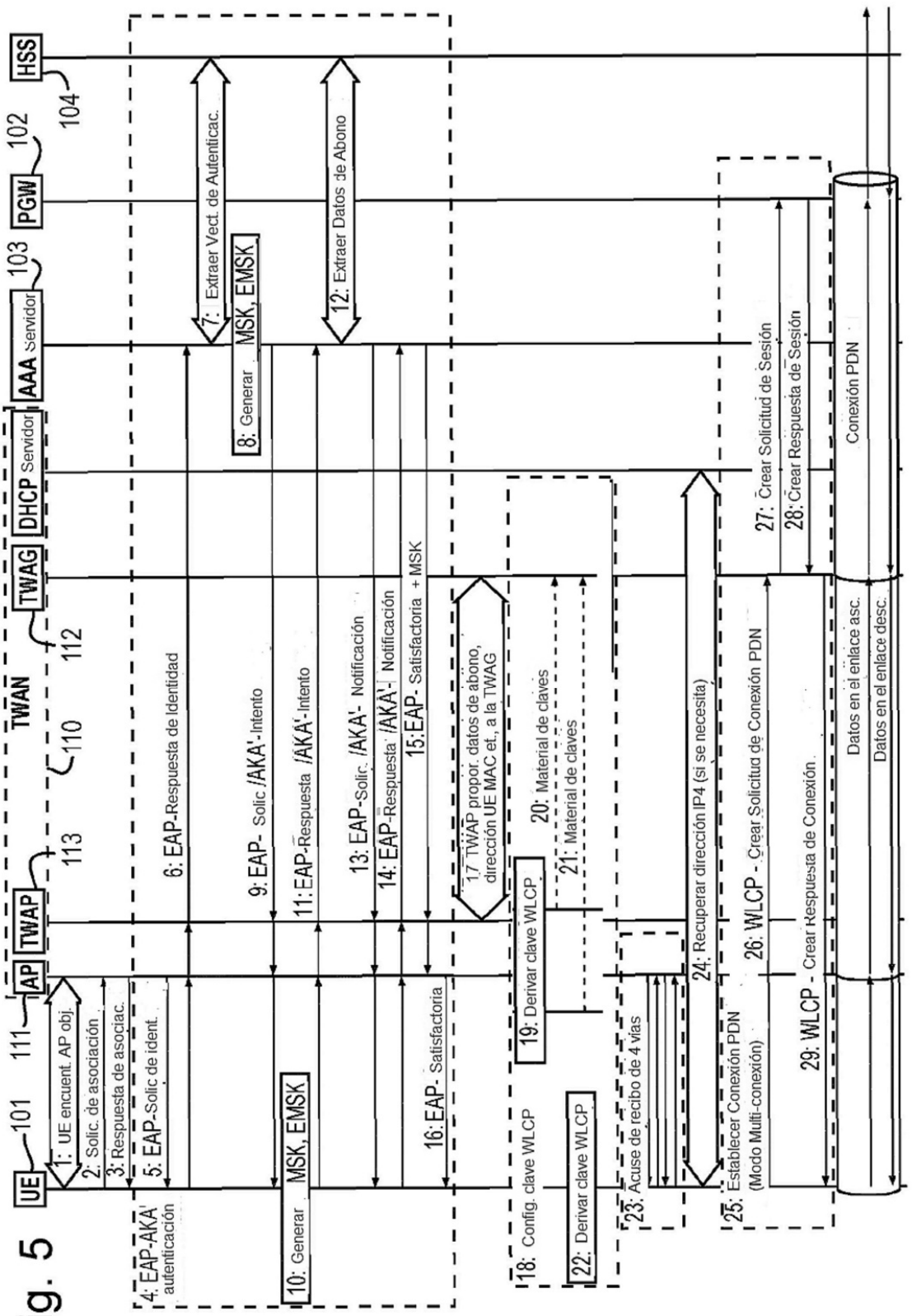

UE
101
AP
111
TWAP
113
TWAN
110
TWAG
112
DHCP Servidor
AAA Servidor
103
PGW
102
HSS
104
1: UE encuent. AP obj.
2: Solic. de asociación
3: Respuesta de asociac.
4: EAP-AKA' autenticación
5: EAP-Solic de ident.
6: EAP-Respuesta de Identidad
7: Extraer Vect. de Autenticac.
8: Generar MSK, EMSK
9: EAP- Solic./AKA'-Intento
10: Generar MSK, EMSK
11: EAP-Respuesta /AKA'-Intento
12: Extraer Datos de Abono
13: EAP-Solic. /AKA'- Notificación
14: EAP-Respuesta /AKA'- Notificación
15: EAP- Satisfactoria + MSK
16: EAP- Satisfactoria
17 TWAP propor. datos de abono, dirección UE MAC et., a la TWAG
18: Config. clave WLCP
19: Derivar clave WLCP
20: Material de claves
21: Material de claves
22: Derivar clave WLCP
23: Acuse de recibo de 4 vías
24: Recuperar dirección IP4 (si se necesita)
25: Establecer Conexión PDN (Modo Multi-conexión)
26: WLCP - Crear Solicitud de Conexión PDN
27: Crear Solicitud de Sesión
28: Crear Respuesta de Sesión
29: WLCP - Crear Respuesta de Conexión
Conexión PDN
Datos en el enlace asc.
Datos en el enlace desc.

Fig. 6

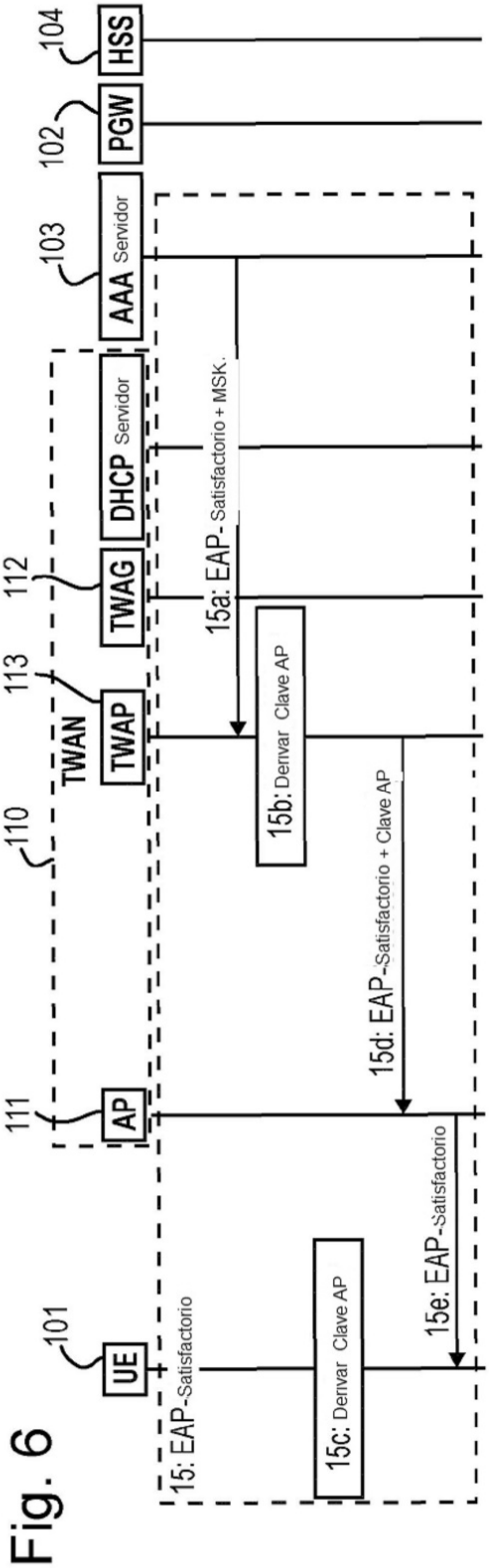

UE
101
AP
111
TWAP
TWAN
113
110
TWAG
112
DHCP Servidor
AAA Servidor
103
PGW
102
HSS
104
15: EAP-Satisfactorio
15a: EAP- Satisfactorio + MSK.
15b: Derivar Clave AP
15c: Derivar Clave AP
15d: EAP-Satisfactorio + Clave AP
15e: EAP-Satisfactorio

Fig. 7

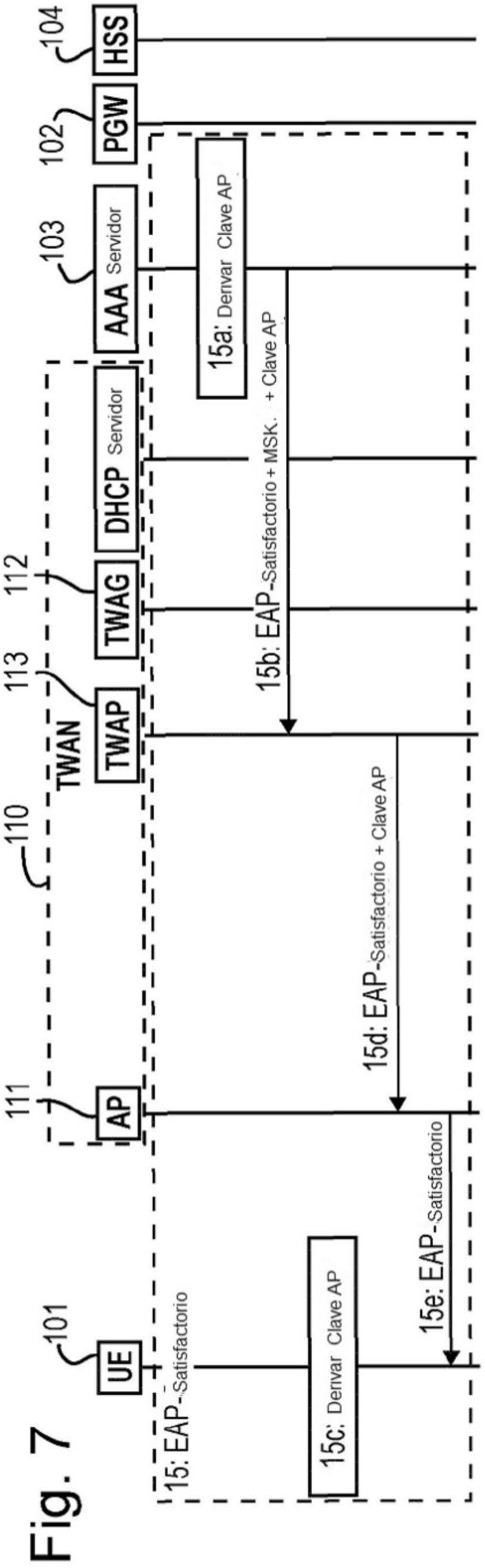

UE
101
AP
111
TWAP
TWAN
113
110
TWAG
112
DHCP Servidor
AAA Servidor
103
PGW
102
HSS
104
15: EAP-Satisfactorio
15a: Derivar Clave AP
15b: EAP-Satisfactorio + MSK. + Clave AP
15c: Derivar Clave AP
15d: EAP-Satisfactorio + Clave AP
15e: EAP-Satisfactorio

Fig. 8

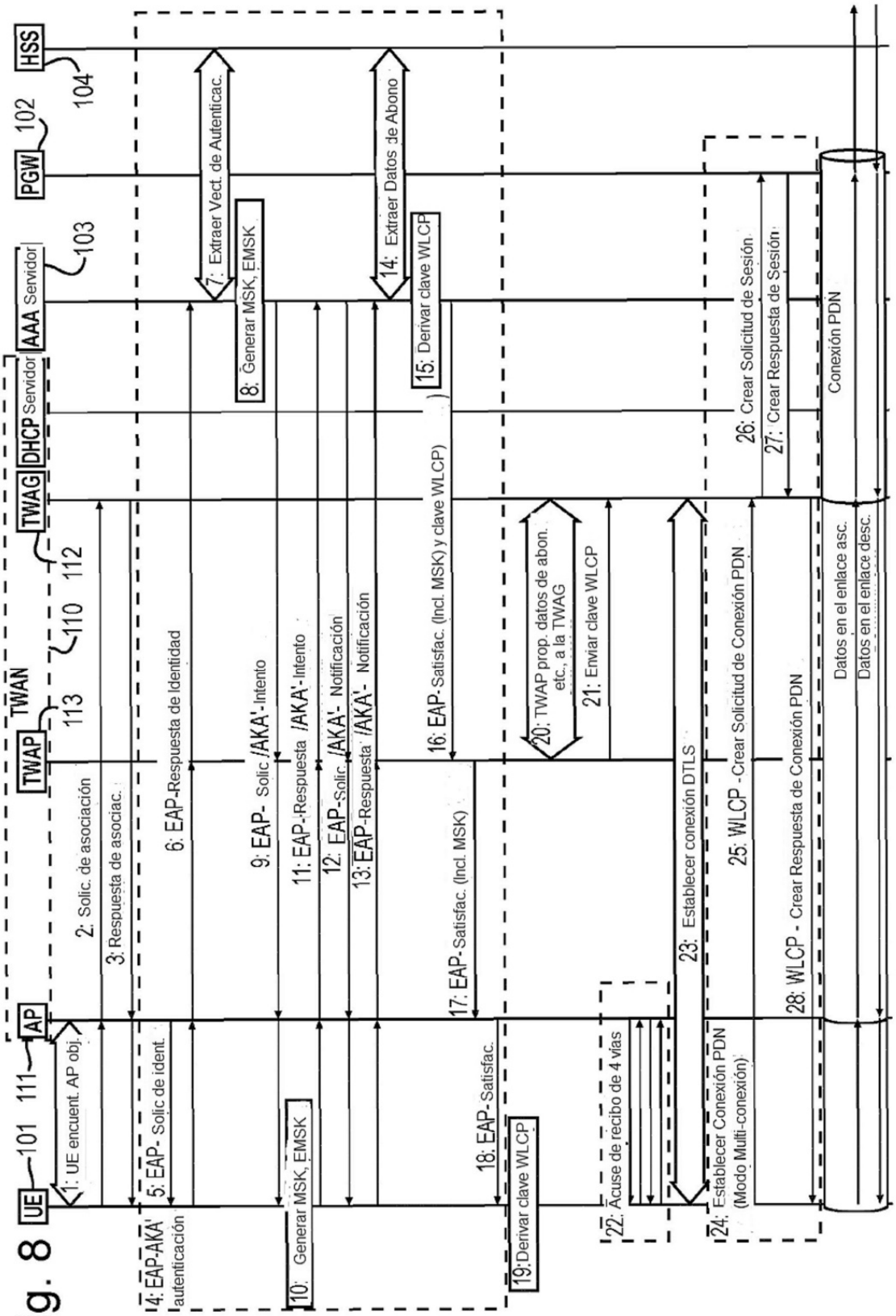
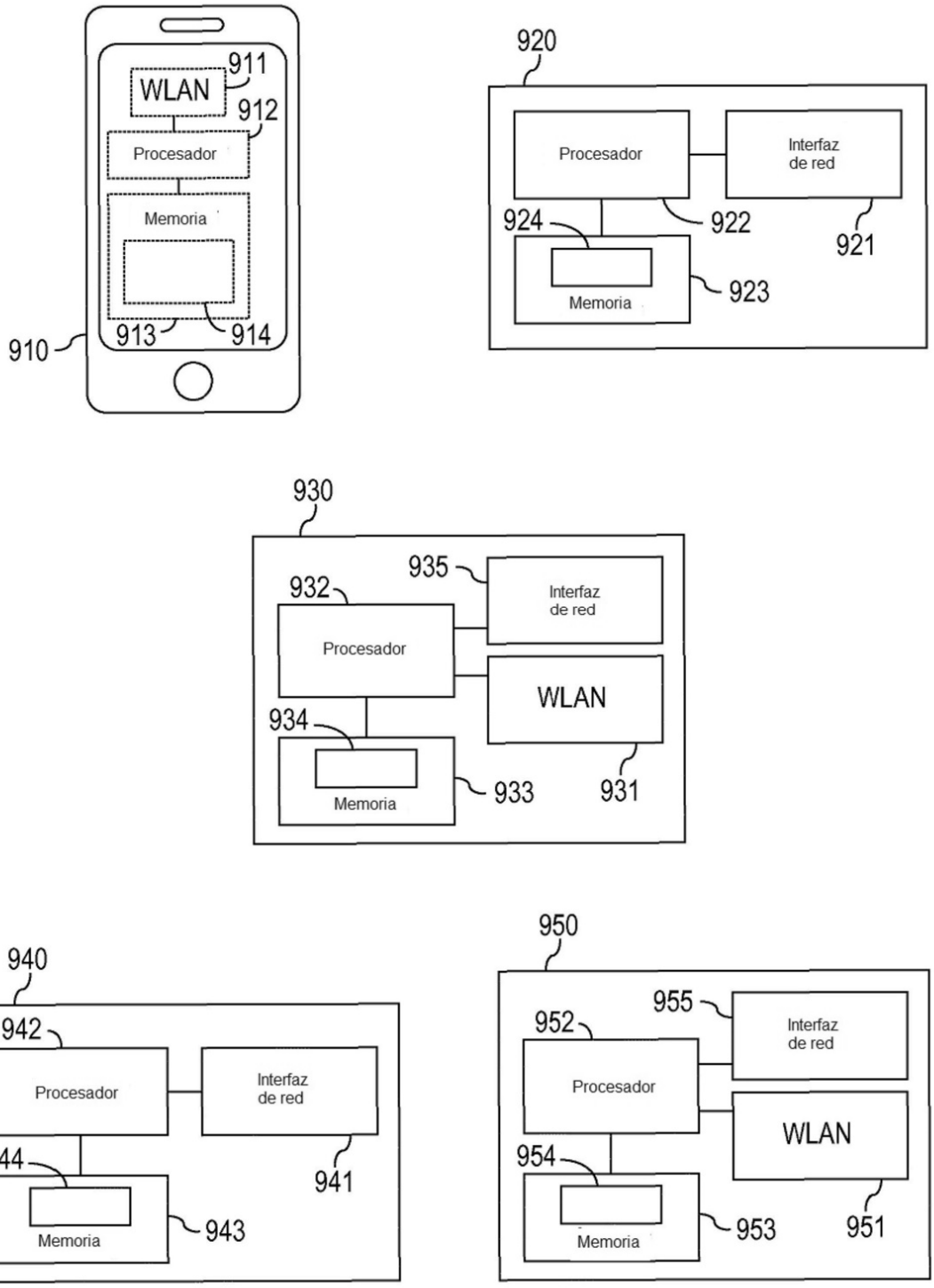

UE
101
111
AP
TWAP
TWAN
113
110
112
TWAG
DHCP Servidor
AAA Servidor
103
PGW
102
HSS
104
1: UE encuent. AP obj.
2: Solic. de asociación
3: Respuesta de asociac.
4: EAP-AKA' autenticación
5: EAP- Solic de ident.
6: EAP-Respuesta de Identidad
7: Extraer Vect. de Autenticac.
8: Generar MSK, EMSK
9: EAP- Solic /AKA'- Intento
10: Generar MSK, EMSK
11: EAP-Respuesta /AKA'- Intento
12: EAP-Solic. /AKA'- Notificación
13: EAP-Respuesta /AKA'- Notificación
14: Extraer Datos de Abono
15: Derivar clave WLCP
16: EAP-Satisfac. (Incl. MSK) y clave WLCP)
17: EAP-Satisfac. (Incl. MSK)
18: EAP-Satisfac.
19:Derivar clave WLCP
20: TWAP prop. datos de abon. etc., a la TWAG
21: Enviar clave WLCP
22: Acuse de recibo de 4 vías
23: Establecer conexión DTLS
24: Establecer Conexión PDN (Modo Multi-conexión)
25: WLCP -Crear Solicitud de Conexión PDN
26: Crear Solicitud de Sesión
27: Crear Respuesta de Sesión
28: WLCP - Crear Respuesta de Conexión PDN
Conexión PDN
Datos en el enlace asc.
Datos en el enlace desc.

Fig. 9


910
911
WLAN
912
Procesador
Memoria
913
914
920
Procesador
Interfaz de red
922
921
924
Memoria
923
930
935
Interfaz de red
932
Procesador
WLAN
934
Memoria
933
931
940
942
Procesador
Interfaz de red
941
944
Memoria
943
950
955
Interfaz de red
952
Procesador
WLAN
954
Memoria
953
951