(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 802 153**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04W 36/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.09.2012 PCT/US2012/054870**

(87) Fecha y número de publicación internacional: **21.03.2013 WO13040039**

(96) Fecha de presentación y número de la solicitud europea: **12.09.2012 E 12762166 (2)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 2756699**

(54) Título: **Comunicación inalámbrica mediante reautentificación simultánea y configuración de conexión**

(30) Prioridad:

12.09.2011 US 201161533627 P
15.09.2011 US 201161535234 P
04.01.2012 US 201261583052 P
05.03.2012 US 201261606794 P
15.03.2012 US 201261611553 P
11.05.2012 US 201261645987 P
11.09.2012 US 201213610718

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.01.2021

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

CHERIAN, GEORGE;
HAWKES, PHILIP MICHAEL;
MALINEN, JOUNI;
ABRAHAM, SANTOSH PAUL;
PALANIGOUNDER, ANAND y
WENTINK, MAARTEN MENZO

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Comunicación inalámbrica mediante reautentificación simultánea y configuración de conexión

CAMPO DE LA DIVULGACIÓN

[0001] La presente divulgación se refiere, en general, a las comunicaciones inalámbricas y, de forma más específica, a procesos de autentificación en comunicaciones inalámbricas.

ANTECEDENTES

[0002] Los avances en la tecnología han dado como resultado dispositivos informáticos más pequeños y más potentes. Por ejemplo, existe actualmente una variedad de dispositivos informáticos personales portátiles, incluyendo dispositivos informáticos inalámbricos, tales como teléfonos inalámbricos portátiles, asistentes digitales personales (PDA) y dispositivos de radiolocalización que son pequeños, ligeros y fáciles de transportar por los usuarios. Más específicamente, los teléfonos inalámbricos portátiles, tales como teléfonos móviles y teléfonos de protocolo de Internet (IP), pueden comunicar paquetes de datos y voz a través de redes inalámbricas. Además, muchos de dichos teléfonos inalámbricos incluyen otros tipos de dispositivos que están incorporados en los mismos. Por ejemplo, un teléfono inalámbrico también puede incluir una cámara fotográfica digital, una cámara de vídeo digital, un grabador digital y un reproductor de ficheros de audio. Además, dichos teléfonos inalámbricos pueden procesar instrucciones ejecutables, incluyendo aplicaciones de software, tales como una aplicación de navegador web, que se pueden usar para acceder a Internet. En sí, estos teléfonos inalámbricos pueden incluir capacidades informáticas significativas.

[0003] Las redes de comunicación inalámbrica permiten a los dispositivos de comunicación transmitir y/o recibir información mientras se está en movimiento. Estas redes de comunicación inalámbrica pueden estar comunicativamente acopladas a otras redes públicas o privadas para permitir la transferencia de información hacia y desde el terminal de acceso móvil. Dichas redes de comunicación incluyen típicamente una pluralidad de puntos de acceso (AP) que proporcionan enlaces de comunicación inalámbrica a terminales de acceso (por ejemplo, dispositivos de comunicación móvil, teléfonos móviles, terminales de usuario inalámbricos). Los puntos de acceso pueden ser estacionarios (por ejemplo, fijados al suelo) o móviles (por ejemplo, montados en vehículos, satélites, etc.) y posicionados para proporcionar una amplia área de cobertura a medida que el terminal de acceso se mueva dentro del área de cobertura.

[0004] Los dispositivos portátiles pueden configurarse para comunicar datos a través de estas redes inalámbricas. Por ejemplo, muchos dispositivos están configurados para funcionar de acuerdo con una especificación del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 802.11 que permite el intercambio inalámbrico de datos a través de un punto de acceso. En algunos sistemas de comunicación, cuando un terminal de acceso móvil se conecta a una red de comunicación a través de un punto de acceso, realiza la autentificación de acceso a la red. Cada vez que un terminal de acceso móvil se conecta a un punto de acceso diferente, puede ser necesario repetir el proceso de autentificación. Sin embargo, repetir este proceso de autentificación puede introducir retardos significativos en el establecimiento.

[0005] Muchos dispositivos de comunicación están configurados para realizar un establecimiento de enlace tanto en una etapa inicial de conexión como en una o más etapas de reconexión. Las soluciones actuales adoptan la clave precompartida para la asignación de direcciones AP-IP después de la autentificación para proteger las asignaciones de direcciones IP.

[0006] Si bien la utilización de múltiples mensajes comunicados entre dos o más puntos de procesamiento de mensajes en el sistema permite el establecimiento de enlace, es altamente deseable reducir el número de mensajes comunicados mientras se mantiene el nivel de autentificación requerido de la comunicación.

[0007] La publicación de la solicitud de patente de los Estados Unidos US 2005/0130659 se refiere a un procedimiento para garantizar la continuidad de una sesión de comunicación cuando se traspasa un equipo de usuario de una primera red de comunicación a una segunda red de comunicación celular. El procedimiento incluye las etapas de realizar un procedimiento de autentificación para una sesión de datos por paquetes con la segunda red mientras aún está conectado a la primera red y simultáneamente realizar un procedimiento de establecimiento de sesión de datos por paquetes con la segunda red mientras todavía está conectado a la primera red.

BREVE EXPLICACIÓN

[0008] La presente invención se define como el objeto de las reivindicaciones independientes. Se definen modos de realización preferentes en las reivindicaciones dependientes.

[0009] Una ventaja particular proporcionada por al menos uno de los modos de realización divulgados es la capacidad de un dispositivo (por ejemplo, un terminal de acceso móvil) para llevar a cabo la reautentificación y el

establecimiento de enlace con otro dispositivo (por ejemplo, un punto de acceso) mediante la agrupación de una solicitud de reautentificación y un mensaje de capa superior como una solicitud de asociación, lo que reduce el número de mensajes intercambiados entre el dispositivo y el otro dispositivo, lo que permite una reautentificación y un establecimiento de enlace más rápidos.

[0010] Otros aspectos, ventajas y características de la presente divulgación resultarán evidentes después de revisar la solicitud completa, incluyendo las siguientes secciones: Breve descripción de los dibujos, Descripción detallada y Reivindicaciones.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0011]

La FIG. 1 es un diagrama del sistema que ilustra una red a modo de ejemplo que puede usarse en sistemas y procedimientos para realizar la reautentificación y el establecimiento de enlace de un dispositivo con otro dispositivo, de acuerdo con diversos modos de realización;

la FIG. 2 es un diagrama de bloques que ilustra un dispositivo de usuario a modo de ejemplo;

la FIG. 3 es un diagrama de flujo que ilustra mensajes asociados con un establecimiento de conexión;

la FIG. 4 es un diagrama de flujo que ilustra un modo de realización particular de la mensajería asociada con la reautentificación y el establecimiento de enlace cifrados con autentificación independiente usando una KCK y una KEK;

la FIG. 5 es un diagrama de flujo que ilustra un modo de realización particular de mensajería asociada con la reautentificación y el establecimiento de enlace con autentificación independiente usando una rMSK;

la FIG. 6 es un diagrama de flujo que ilustra un modo de realización particular de mensajería asociada con la reautentificación y el establecimiento de enlace con determinación de la capacidad de cifrado;

la FIG. 7 es un diagrama de flujo que ilustra otro modo de realización particular de mensajería asociada con la reautentificación y el establecimiento de enlace cifrados con autentificación combinada usando la KCK y la KEK;

la FIG. 8 es un diagrama de flujo que ilustra otro modo de realización particular de mensajería asociada con la reautentificación y el establecimiento de enlace cifrados con autentificación combinada usando la rMSK;

la FIG. 9 es un diagrama de flujo que ilustra un modo de realización particular de mensajería asociada con la reautentificación y el establecimiento de enlace donde un elemento de información de mensaje de descubrimiento de DHCP está protegido con integridad de mensaje;

la FIG. 10 es un diagrama de flujo que ilustra un modo de realización particular de la mensajería asociada con la reautentificación y el establecimiento de enlace donde se establece un Anonce junto con un mensaje "Instalar PTK, GTK, IGTK";

la FIG. 11 es un diagrama de flujo que ilustra un modo de realización particular de mensajería asociada con la reautentificación y el establecimiento de enlace cifrados usando un indicador de capacidad de establecimiento rápido del enlace inicial;

la FIG. 12 es un diagrama de flujo que ilustra la mensajería que se puede realizar durante un protocolo de reautentificación asociado con la reautentificación y el establecimiento de enlace;

la FIG. 13 ilustra una jerarquía de claves que puede usarse para un protocolo de reautentificación asociado con la reautentificación y el establecimiento de enlace;

la FIG. 14 es un diagrama de flujo que muestra un proceso a modo de ejemplo para generar y agrupar una solicitud de reautentificación y una solicitud de descubrimiento en una solicitud de asociación; y

la FIG. 15 es un diagrama de flujo que muestra un proceso a modo de ejemplo que funciona en una estación base para recibir y extraer una solicitud de reautentificación y un mensaje de capa superior de una solicitud de asociación enviada por una estación/terminal.

DESCRIPCIÓN DETALLADA

[0012] En la siguiente descripción, se hace referencia a los dibujos adjuntos, en los cuales se muestran, a modo de ilustración, modos de realización específicos en los que la divulgación puede ponerse en práctica. Los modos de realización pretenden describir aspectos de la divulgación con suficiente detalle para permitir que los expertos en la técnica practiquen la invención. Se pueden utilizar otros modos de realización y se pueden hacer cambios en los modos de realización divulgados sin apartarse del alcance de la divulgación. La siguiente descripción detallada no se debe tomar en un sentido limitativo y el alcance de la presente invención se define solamente por las reivindicaciones adjuntas.

[0013] Las características y los modos de realización descritos en el presente documento proporcionan dispositivos y procedimientos para un tiempo de establecimiento rápido durante un proceso de reautentificación de un establecimiento de conexión.

[0014] En las redes inalámbricas, tales como las redes 802.11 (WiFi) del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), un usuario móvil puede pasar de una red a otra. En algunos casos, las redes pueden ser gestionadas por una misma entidad o portadora de red.

[0015] Algunos ejemplos no limitativos de tales casos de uso son:

1. Paso por hotspots

   (A) Un usuario puede pasar por (varios, no superpuestos) hotspots de WiFi accesibles al público (por ejemplo, en cafeterías u otros lugares públicos). Mientras tiene conectividad, el terminal de usuario puede cargar y descargar información tal como mensajes de correo electrónico, mensajes de redes sociales, etc. Otro ejemplo son los pasajeros a bordo de un tren que puede pasar por múltiples estaciones de tren con puntos de acceso WiFi.

2. Tren

   (B) Un usuario puede estar a bordo de un tren en el que se proporciona un servicio WiFi a los clientes a través de un punto de acceso (AP) local. Este AP puede utilizar una red troncal inalámbrica basada en 802.11 para conectarse a la infraestructura al lado de las vías. Puede utilizarse una antena direccional para proporcionar una cobertura continua a lo largo de las vías.

3. Paso por estación de peaje/pesaje

   (C) Un vehículo en una carretera que pasa por una estación de peaje o una estación de pesaje puede ser capaz de conectarse a un AP en la estación de peaje o en la estación de pesaje. Mientras se pasa por el peaje (o se realiza el pesaje), puede proporcionarse información tal como la facturación al cliente de peajes o intercambio de información de carga.

[0016] Las aplicaciones habilitadoras para estas conexiones no superpuestas pero relacionadas pueden basarse en un conjunto de protocolos de internet (IP) estándar y confiar potencialmente en la tecnología inalámbrica subyacente para establecer un enlace seguro.

[0017] En algunos sistemas propuestos para el establecimiento de conexiones de IP, después de recibir una baliza, puede haber 16 intercambios de ida y vuelta (32 mensajes comunicados hacia y desde un terminal de acceso) para establecer un enlace seguro para el terminal de acceso.

[0018] En los sistemas propuestos analizados en el presente documento, se puede realizar un establecimiento de enlace rápido en el que el número de mensajes para establecer una conexión IP y un enlace seguro después de recibir la baliza se reducen a 1 intercambio de ida y vuelta (2 mensajes) respecto a los 16 intercambios de ida y vuelta (32 mensajes) anteriores. Se puede utilizar un protocolo de autentificación extensible/protocolo de reautentificación (EAP/ERP) como parte del establecimiento de enlace rápido.

[0019] La FIG. 1 es un diagrama del sistema que ilustra un ejemplo de una configuración de red inalámbrica para realizar la reautentificación y el establecimiento de enlace de uno o más terminales con un punto de acceso. La configuración de la red 100 de la FIG. 1 puede utilizarse para comunicar datos entre uno o más terminales y un punto de acceso. La configuración de la red 100 incluye un punto de acceso 102 acoplado a una red 104. El punto de acceso 102 puede estar configurado para proporcionar comunicaciones inalámbricas a diversos dispositivos de comunicación tales como dispositivos inalámbricos (que también pueden denominarse en el presente documento estaciones y terminales de acceso 106, 108, 110). Como ejemplo no limitativo, el punto de acceso 102 puede ser una estación base. Como ejemplos no limitativos, las estaciones/terminales 106, 108, 110 pueden ser un ordenador personal (PC), un ordenador portátil, una tableta, un teléfono móvil, un asistente digital personal (PDA), y/o cualquier dispositivo configurado para enviar y/o recibir datos de forma inalámbrica, o cualquier combinación de los mismos. La red 104 puede incluir una red de ordenadores distribuida, tal como una red de protocolo de control de transmisión/protocolo de Internet (TCP/IP).

[0020] El punto de acceso 102 puede estar configurado para proporcionar una variedad de servicios de comunicaciones inalámbricas, incluyendo, de forma no limitativa: servicios de fidelidad inalámbrica (WiFi), servicios de interoperabilidad mundial para acceso por microondas (WiMAX) y servicios de protocolo de inicio de sesión (SIP) inalámbricos. Las estaciones/terminales 106, 108, 110 pueden configurarse para comunicaciones inalámbricas (incluyendo, de forma no limitativa, comunicaciones de acuerdo con la familia de especificaciones 802.11, 802.11-2007 y 802.11x desarrollada por el Instituto de Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)). Además, las estaciones/terminales 106, 108, 110 pueden configurarse para enviar datos y recibir datos desde el punto de acceso 102. Como se describe con más detalle a continuación, al menos una de las estaciones 106, 108 y 110 puede participar en la reautentificación y el establecimiento de enlace utilizando una solicitud de reautentificación y un mensaje de capa superior agrupados como una solicitud de asociación.

[0021] La FIG. 2 es un diagrama de bloques que ilustra un dispositivo de comunicación 200. En un modo de realización particular, el dispositivo de comunicación 200 corresponde al punto de acceso 102. En otro modo de realización particular, el dispositivo de comunicación 200 corresponde a una o más de las estaciones 106, 108 y/o 110. Un procesador 210 (que también puede ser un procesador de señales digitales (DSP)) está acoplado a una memoria 232 para almacenar información tal como datos para procesamiento y transmisión e instrucciones 260 (por ejemplo, admitiendo la agrupación de una solicitud de reautentificación y un mensaje de capa superior como una solicitud de asociación) para la ejecución en el procesador 210.

[0022] Un controlador de visualización 226 puede estar acoplado al procesador 210 y a un dispositivo de visualización 228. También se puede acoplar un codificador/decodificador (CÓDEC) 234 al procesador 210. Como ejemplos no limitativos de dispositivos de interfaz de usuario, un altavoz 236 y un micrófono 238 pueden estar acoplados al CÓDEC 234. Un controlador inalámbrico 240 puede estar acoplado al procesador 210 y a una antena 242. En un ejemplo particular, el procesador 210, el controlador de visualización 226, la memoria 232, el CÓDEC 234 y el controlador inalámbrico 240 pueden estar incluidos en un dispositivo de sistema en paquete o sistema en chip 222. En un ejemplo particular, un dispositivo de entrada 230 y una fuente de alimentación 244 pueden estar acoplados al dispositivo de sistema en chip 222. Además, en un ejemplo particular, como se ilustra, el dispositivo de visualización 228, el dispositivo de entrada 230, el altavoz 236, el micrófono 238, la antena 242 y la fuente de alimentación 244 son externos al dispositivo de sistema en chip. Sin embargo, cada uno del dispositivo de visualización, el dispositivo de entrada, el altavoz, el micrófono, la antena inalámbrica y la fuente de alimentación se puede acoplar a un componente del dispositivo de sistema en chip 222, tal como una interfaz o un controlador.

[0023] La FIG. 3 es un diagrama de flujo que ilustra los mensajes que pueden comunicarse en un establecimiento de conexión convencional. Los mensajes mostrados entre una estación/terminal (STA) 302 y un punto de acceso (AP) 304 pueden incluir una sonda y solicitud de autentificación. Puede iniciarse un proceso de protocolo de autentificación extensible (EAP) sobre red de área local (LAN) (EAPOL) e incluir una fase de identificación, una fase de EAP protegido (PEAP) y un protocolo de autentificación por desafío mutuo de EAP-Microsoft (EAP-MSCHAPv2). Después del éxito de EAP, se puede establecer una clave EAPOL. De este modo, al menos 16 mensajes deben ser comunicados hacia y desde la estación/terminal 302 para establecer el establecimiento de enlace y la autentificación.

[0024] A diferencia del establecimiento convencional en la FIG. 3, en un modo de realización particular, el número de mensajes para establecer una conexión IP (después de la recepción de la baliza) se reduce a 2 mensajes (de 16 mensajes). El Protocolo de Reautentificación del Protocolo de Autentificación Extensible (EAP-RP) se puede utilizar como parte de la reautentificación como se describe más completamente a continuación con respecto a las FIGS. 12 y 13 y puede incluir las siguientes optimizaciones. La STA 302 puede realizar la autentificación EAP completa una vez, y seguir usando la reautentificación rápida de EAP-RP para un rápido establecimiento inicial de enlace a partir de entonces.

[0025] Una clave de sesión principal raíz (rMSK) es generada por la estación/terminal 302 antes de enviar una solicitud de asociación sin obtener un desafío desde la red. La estación (STA) 302 genera una clave transitoria de pares (PTK) a partir de la rMSK e incluye una clave de confirmación de clave (KCK), una clave de cifrado de clave (KEK) y una clave transitoria (TK).

[0026] La solicitud de asociación es enviada por la STA 302 y agrupa una solicitud de reautentificación de EAP (o una solicitud de reautorización de EAP) con un descubrimiento con confirmación rápida de protocolo de configuración dinámica de host (DHCP) y un Snonce (por ejemplo, Snonce es recogido por la STA 302, es decir, nonce de estación). El mensaje agrupado puede incluirse como uno o más elementos de información (IE). La solicitud de reautentificación de EAP es autentificada por el servidor de autentificación (servidor Aut.) 308 utilizando una clave de integridad de raíz (rIK). El descubrimiento con confirmación rápida de DHCP y Snonce se protegen mediante la clave de sesión principal de reautentificación (rMSK) o la clave transitoria de pares (PTK) obtenida de la rMSK. El descubrimiento con confirmación rápida de DHCP puede estar cifrado y haberse codificado mediante MIC (Código de integridad del mensaje) o no estar cifrado sino codificado mediante MIC. Aunque algunos de los ejemplos del presente documento pueden utilizar una solicitud de descubrimiento (por ejemplo, descubrimiento con confirmación rápida) para ilustrar un concepto de reautentificación, debe entenderse que cualquier mensaje

utilizado en una capa superior (de una pila de protocolos) para asignar la dirección IP puede ser utilizado en su lugar.

[0027] En un modo de realización particular, la STA 302 realiza una reautorización o una reautentificación usando el EAP-RP. Después de la reautorización o la reautentificación, la STA 302 puede generar el mensaje de capa superior y la solicitud de asociación. La STA 302 puede agrupar el mensaje de la capa superior (u otros mensajes) en la solicitud de asociación y transmitir la solicitud de asociación al AP 304.

[0028] Si se cifra el mensaje de DHCP, el AP 304 puede retener los mensajes de descubrimiento con confirmación rápida de DHCP y Snonce hasta que la solicitud de reautentificación de EAP es validada por el servidor de autentificación 308. Para validar el mensaje de DHCP, el AP 304 espera hasta que recibe una rMSK del servidor de autentificación 308 y obtiene la clave transitoria de pares (PTK). Basándose en la rMSK obtenida del servidor de autentificación 308, el AP 304 obtiene la PTK que se utiliza para la codificación mediante MIC (Código de Integridad de Mensaje) así como para descifrar el mensaje de DHCP.

[0029] Si el mensaje de DHCP no está cifrado, el AP 304 puede reenviar el descubrimiento con confirmación rápida de DHCP a un servidor de DHCP con la expectativa de que en la mayoría de los casos el mensaje provino de un dispositivo correcto (pero conservar los mensajes Snonce hasta que la solicitud de reautentificación de EAP sea validada por el servidor de autentificación 308). Aunque se puede recibir un acuse de recibo de DHCP en el AP 304 del servidor de DHCP basado en el descubrimiento con confirmación rápida de DHCP enviado por el AP 304, el AP 304 retiene el acuse de recibo de DHCP hasta que el AP 304 verifique el mensaje de descubrimiento de DHCP basado en la rMSK obtenida del servidor de autentificación 308 y obtiene la PTK.

[0030] El AP 304 envía entonces el acuse de recibo de DHCP + una GTK/IGTK protegida con la PTK. En otras palabras, el acuse de recibo de DHCP está cifrado y la integridad del mensaje está protegida.

[0031] La invención incluye una o más de las siguientes etapas en un proceso para el establecimiento de enlace y la autentificación.

[0032] En primer lugar, un usuario obtiene la STA 302 y realiza una autentificación EAP completa como parte de un establecimiento inicial con una red específica (por ejemplo, una red WiFi específica). La autentificación EAP completa se mantiene durante un periodo de autentificación específico, tal como, por ejemplo, un año.

[0033] En segundo lugar, durante el periodo de autentificación, el usuario pasa por (varios, no superpuestos) hotspots de WiFi accesibles públicamente (por ejemplo, en cafeterías y otros lugares públicos). En otras palabras, esta etapa puede realizarse varias veces y con múltiples AP 304 que forman parte de la red de establecimiento durante el periodo de autentificación. La STA 302 realizará un establecimiento rápido de enlace inicial (FILS) con la red utilizando EAP-RP. La agrupación del EAP-RP con el Descubrimiento Rápido de DHCP utilizando el mensaje de solicitud de asociación reduce la señalización para la solicitud de asociación a una ida y vuelta, como se explica más detalladamente a continuación. Durante el periodo de autentificación, la STA 302 de usuario puede continuar realizando el EAP-RP para el establecimiento rápido de enlace inicial (FILS) cuando se conecta con la red.

[0034] En tercer lugar, cuando se acerque el final del periodo de autentificación, el usuario puede recibir una advertencia para realizar de nuevo un "acoplamiento completo" a la red, dentro de un periodo determinado de tiempo (por ejemplo, 2 semanas). Durante este periodo, el usuario seguirá siendo capaz de utilizar la autentificación rápida basada en la autentificación de EAP completa anterior hasta que expire o se realice un acoplamiento completo. La notificación de acoplamiento completo puede originarse desde la red o puede configurarse localmente en la STA 302.

[0035] En cuarto lugar, si el usuario no realiza el acoplamiento completo, después de un año, la red fallará el EAP-RP e iniciará la autentificación EAP completa durante otro año como se describe resumidamente en la etapa 1.

[0036] Las FIGS. 4-11 ilustran varios escenarios diferentes para realizar el establecimiento de enlace y la autentificación de dos mensajes.

[0037] La FIG. 4 es un diagrama de flujo que ilustra un primer ejemplo de realización de un establecimiento de enlace y la autentificación para una estación cliente. En las etapas 0a y 0b, mientras está comunicativamente acoplada a un primer punto de acceso (API) 304A, la STA 302 puede realizar la autentificación EAP completa. Al moverse (etapa 1) más cerca de un segundo punto de acceso (AP2) 304B, y detectar su baliza (etapa 2), la estación/terminal 302 puede intentar reautentificarse por medio del segundo punto de acceso AP2 304B. En este proceso, el AP2 304B transmite una baliza/sonda que incluye un indicador de capacidad para el establecimiento rápido de enlace inicial (FILS). El indicador de capacidad puede indicar la capacidad de manejar una solicitud de asociación con descubrimiento rápido de DHCP y EAP-RP agrupados. En la etapa 3, la estación/terminal 302 genera unas claves de sesión principal de reautentificación (rMSK) (véase la FIG. 13) usando EAP-RP antes de enviar la solicitud de asociación, donde:

rMSK = KDF (K, S);

K = rRK;

y

S = etiqueta rMSK | "\0" | SEQ | longitud.

[0038] La STA 302 agrupa los uno o más mensajes como elementos de información (IE) (o parámetros/carga útil) de una solicitud de asociación (Etapa 3). Por ejemplo, tal solicitud de asociación puede incluir: 1) Mensaje de iniciación de la reautentificación de EAP (integridad de mensaje usando rIK); 2) mensaje de descubrimiento con confirmación rápida de DHCP (cifrado e integridad de mensajes con KCK/KEK); y/o 3) Clave EAPOL (Snonce, Anonce) (integridad del mensaje usando KCK). La clave EAPOL puede configurarse como una trama completa o subconjunto. El Anonce (es decir, el nonce del punto de acceso) puede ser seleccionado por la STA 302 y enviado al punto de acceso AP2 304B. El AP2 304B puede garantizar que la STA 302 está usando un Anonce enviado en los últimos segundos/milisegundos (por ejemplo, un Anonce reciente obtenido de la baliza para el AP2), por ejemplo. El AP2 304B retiene el mensaje de DHCP y de clave EAPOL hasta que recibe una clave de sesión principal raíz (rMSK) del servidor de autentificación 308 a través de un mensaje de acuse de recibo de reautentificación (por ejemplo, un mensaje de finalización/reautorización de EAP). El AP2 304B genera una PTK a partir de la rMSK. El AP2 304B realiza un intercambio de Código de Integridad de Mensaje (MIC) para los mensajes DHCP y de clave EAPOL y descifra el DHCP. El AP2 304B utiliza la rMSK para obtener KCK/KEK para proteger un acuse de recibo de DHCP y un mensaje de clave EAPOL antes de enviarlo a la STA 302. El mensaje de inicio de reautentificación de EAP, el mensaje de finalización/reautentificación de EAP, o una combinación de los mismos, pueden ser mensajes de autentificación. La clave EAPOL, la GTK y un mensaje de confirmación de clave pueden ser mensajes de establecimiento de comunicación de 4 vías. Los mensajes de autentificación y los mensajes de establecimiento de comunicación de 4 vías pueden transmitirse simultáneamente al AP2 304B desde la STA 302.

[0039] En un modo de realización particular, el AP2 304B aloja un proxy de protocolo de configuración dinámica de host (DHCP) en nombre de la STA 302. El proxy DHCP y la STA 302 intercambian señales de dirección IP utilizando elementos de información (por ejemplo, elementos de información en la solicitud de asociación o una respuesta de asociación).

[0040] En diversos ejemplos, el Anonce puede ser enviado por el AP2 304B ya sea usando la baliza para permitir las estaciones que utilizan escaneo pasivo, o en un mensaje de respuesta de sonda cuando se usa el escaneo activo. Cuando el Anonce es enviado por el AP2 304B usando la baliza, el Anonce se puede cambiar en cada baliza, o en múltiples balizas. La STA 302 puede incluir el Anonce captado por la estación 302 en el mensaje de Solicitud de Asociación enviado desde la STA 302 al AP2 304B.

[0041] La FIG. 5 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros modos de realización del establecimiento de enlace y autentificación. Este proceso puede denominarse Opción 1a. Los procesos realizados en la FIG. 5 son similares a los realizados en la FIG. 4 (Opción 1), excepto porque se utiliza la rMSK (en lugar de la KCK/KEK de la PTK) para autentificar los mensajes de descubrimiento de DHCP y de clave EAPOL encapsulados en el mensaje de solicitud de asociación.

[0042] La FIG. 6 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros modos de realización del establecimiento de enlace y autentificación. Este proceso puede denominarse Opción 1b. Los procesos realizados en la FIG. 6 son similares a los realizados en la FIG. 4 (Opción 1) excepto por las siguientes diferencias posibles. En la etapa 2 mostrada en la FIG. 6, el AP2 304B puede anunciar la capacidad de que la solicitud de DHCP puede cifrarse. En la etapa 4 mostrada en la FIG. 6, la estación/terminal 302 puede decidir si el mensaje de DHCP debe estar cifrado o no. Varios factores pueden ser tomados en consideración por la STA 302, tales como, por ejemplo, si la solicitud de descubrimiento de DHCP contiene cualquier información privada, etc. Si la estación/terminal decide cifrar la solicitud de descubrimiento de DHCP, entonces el AP 304B puede retener el mensaje (como se muestra en las FIGS. 4 y 5).

[0043] Si la estación/terminal decide no cifrar la solicitud de descubrimiento de DHCP, se pueden realizar las siguientes etapas. En la etapa 4 mostrada en la FIG. 6, el elemento de información (IE) o el parámetro de solicitud de descubrimiento de DHCP solo está protegido para la integridad del mensaje. Basándose en la etapa 4, el AP2 304B envía el descubrimiento con confirmación rápida de DHCP (etapa 6) sin esperar una respuesta para una solicitud de inicio de reautentificación de EAP (etapa 9). Este proceso hace que la asignación de direcciones IP tenga lugar en paralelo con el procedimiento de reautentificación de EAP. En la etapa 7a mostrada en la FIG. 6, el punto de acceso retiene el acuse de recibo de DHCP que provenía del servidor de DHCP hasta la etapa 10b, en la que se ha validado el descubrimiento de DHCP. Si la integridad del mensaje falla, entonces el AP2 304B inicia un procedimiento para eliminar la dirección IP asignada mediante el acuse de recibo de DHCP.

[0044] La FIG. 7 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros modos de realización del establecimiento de enlace y autentificación. Este proceso puede denominarse Opción 2. Los procesos realizados en la FIG. 7 son similares a los realizados en la FIG. 4 (Opción 1) excepto por las siguientes diferencias posibles. En lugar de autentificar el mensaje de DHCP y el mensaje de clave de EAPOL de forma independiente, la carga útil combinada que incluye la reautentificación de EAP, el descubrimiento de DHCP y la clave de EAPOL puede autentificarse utilizando KCK/KEK. El AP2 304B extrae el mensaje de inicio de reautentificación de EAP y lo reenvía al servidor de autentificación 308 sin validar el mensaje completo, que se autentificó utilizando KCK/KEK. El punto de acceso 304 autentifica el mensaje completo después de recibir la rMSK del servidor de autentificación 308.

[0045] La FIG. 8 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros modos de realización del establecimiento de enlace y autentificación. Este proceso puede denominarse Opción 2a. Los procesos realizados en la FIG. 8 son similares a los realizados en la FIG. 5 (Opción 1a) excepto por las siguientes posibles diferencias. En lugar de autentificar el mensaje de DHCP y el mensaje de clave de EAPOL de forma independiente, la carga útil combinada que incluye la reautentificación de EAP, el descubrimiento de DHCP y la clave de EAPOL pueden autentificarse utilizando la rMSK. El AP 304B extrae el mensaje de inicio de reautentificación de EAP y lo reenvía al servidor de autentificación 308 sin validar el mensaje completo, que se autentificó utilizando la rMSK. El AP2 304B autentifica el mensaje completo después de recibir la rMSK del servidor de autentificación 308. El mensaje de descubrimiento de DHCP (etapa 9) se puede enviar antes de la etapa 5. En este caso, la dirección IP asignada se omite si la autentificación no tiene éxito.

[0046] La FIG. 9 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros modos de realización del establecimiento de enlace y autentificación. Este proceso puede denominarse Opción 2b. Los procesos realizados en la FIG. 9 son similares a los realizados en la FIG. 4 excepto por las siguientes posibles diferencias. En la etapa 2, el punto de acceso puede anunciar la capacidad de que la solicitud de DHCP puede cifrarse. En la etapa 4, la STA 302 decide si el mensaje de DHCP debe cifrarse o no. Varios factores pueden ser tomados en consideración por la STA 302, tales como, por ejemplo, si la solicitud de descubrimiento de DHCP contiene cualquier información privada, etc. Si la STA 302 decide cifrar la solicitud de descubrimiento de DHCP, entonces el AP2 304B mantendrá el mensaje como se ha descrito anteriormente en la opción 2 y en la opción 2a. Si la STA 302 decide no cifrar la solicitud de descubrimiento de DHCP, entonces se pueden realizar las siguientes etapas. En la etapa 4, el IE de mensaje de descubrimiento de DHCP solo está protegido para la integridad del mensaje. Basándose en la etapa 4, el punto de acceso 304 envía el descubrimiento con confirmación rápida de DHCP (etapa 6) sin esperar respuesta para la solicitud de inicio de reautentificación de EAP (etapa 9). Este proceso hace que la asignación de direcciones IP tenga lugar en paralelo con el procedimiento de reautentificación de EAP. En la etapa 7a, el AP2 304B retiene el acuse de recibo de DHCP que provenía del servidor de DHCP hasta la etapa 10b, en la que se ha validado el descubrimiento de DHCP. Si falla la integridad del mensaje, entonces el AP2 304B inicia un procedimiento para eliminar la dirección IP asignada mediante el mensaje de acuse de recibo de DHCP.

[0047] La FIG. 10 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros modos de realización del establecimiento de enlace y autentificación. Este proceso puede denominarse Opción 3. Los procesos realizados en la FIG. 10 son similares a los realizados en las FIGS. 4 y 5 (Opciones 1 y 1a) excepto por las siguientes posibles diferencias. El Anonce se puede enviar en la respuesta de asociación junto con un mensaje "Instalar PTK, GTK, IGTK". Las etapas 9 y 11 de la FIG. 10 puede realizarse en paralelo con las etapas 5-7 como se describe en la opción 1b y la opción 2b.

[0048] Una opción 4 también se puede obtener a partir de las opciones 1 y 2, excepto por las siguientes diferencias posibles. En lugar de un solo mensaje en la etapa 4 (es decir, la solicitud de asociación), la solicitud de asociación puede dividirse como el mensaje 1 (M1), que encapsula el mensaje de descubrimiento de DHCP y el mensaje 2 (M2), que encapsula el mensaje de inicio de reautentificación de EAP y el Snonce. El punto de acceso 304 no actuará sobre el mensaje de descubrimiento de DHCP hasta que reciba la clave de EAPOL. Los dos mensajes (M1 y M2) pueden estar separados por un periodo SIFS. Esta opción 4 puede tener la ventaja de que la estructura de EAPOL puede ser reutilizada.

[0049] La FIG. 11 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros modos de realización del establecimiento de enlace y autentificación. Este proceso puede denominarse Opción 5. Los procesos realizados en la FIG. 11 son similares a los realizados en la FIG. 4 (Opciones 1) excepto por las siguientes posibles diferencias. El punto de acceso 304 transmite la respuesta de baliza/sonda, que incluye el indicador de capacidad de establecimiento rápido de enlace inicial (FILS) para la asignación simultánea de dirección IP y/o EAP-RP. En este escenario, el temporizador de asignación de la dirección IP asignada por el AP2 304B no ha expirado. La estación/terminal 302 usa la dirección IP asignada por el AP1 304A en una solicitud de DHCP enviada al AP2 304B para confirmar si puede continuar usando esa dirección IP. Si la dirección IP ha expirado, entonces el servidor de DHCP 306 envía un DHCP-NAK.

[0050] La FIG. 12 es un diagrama de flujo que ilustra la mensajería que puede realizarse durante un protocolo de reautentificación. La primera vez que la STA 302 se conecta a una red, realiza un intercambio de EAP completa

con el servidor de autentificación 308. Como resultado, una clave de sesión principal (MSK) se distribuye al autentificador de EAP. La clave de sesión principal (MSK) es entonces utilizada por el autentificador y la STA 302 para establecer claves de sesión transitorias (TSK) según sea necesario. En el momento del intercambio inicial de EAP, la STA 302 y el servidor de autentificación 308 también obtienen una EMSK, que se utiliza para obtener una clave raíz de reautentificación (rRK). Más específicamente, una clave raíz de reautentificación (rRK) puede obtenerse a partir de la MSK ampliada (EMSK) o de una clave raíz específica del dominio (DSRK), que se obtiene a partir de la EMSK. La clave raíz de reautentificación (rRK) puede estar solamente disponible para la STA 302 y el servidor de autentificación 308 y en general no se distribuye a ninguna otra entidad. Además, una clave de integridad de reautentificación (rIK) puede obtenerse a partir de la clave raíz de reautentificación (rRK). La STA 302 y el servidor de autentificación 308 pueden usar la clave de integridad de reautentificación (rIK) para proporcionar una prueba de posesión mientras se realiza un intercambio de ERP. La clave de integridad de reautentificación (rIK) en general tampoco se distribuye a ninguna otra entidad y en general solo está disponible para la STA 302 y el servidor de autentificación 308.

[0051] Se definen dos nuevos códigos de EAP, Inicio de EAP y Finalización de EAP con el fin de la reautentificación de EAP. Cuando la STA 302 solicita un EAP-RP, realiza el intercambio de EAP-RP mostrado en la ventana inferior de la FIG. 12.

[0052] La FIG. 13 ilustra una jerarquía de claves que puede usarse para un protocolo de reautentificación. La clave de sesión principal (MSK) se puede obtener a partir de una clave raíz y una clave principal de pares (PMK) se puede obtener a partir de la clave de sesión principal (MSK). La MSK ampliada (EMSK) puede obtenerse a partir de la clave raíz. Para el intercambio de EAP-RP, se pueden obtener varias claves adicionales de la MSK ampliada (EMSK). Se pueden obtener DSRK1-DSRKn. Cada una de las claves de clave raíz específica del dominio (DSRK) puede incluir la rRK. A partir de la clave raíz de reautentificación (rRK), se pueden obtener la clave de integridad de reautentificación (rIK) y las claves de sesión principal de reautentificación (rMSK1 ... rMSKn). Cada una de las rMSK puede incluir una clave principal de pares (PMK). Se puede obtener a partir de la PMK una clave transitoria de pares (PTK), que puede incluir una clave de confirmación de clave de EAPOL (KCK), una clave de cifrado de clave EAPOL (KEK) y una clave transitoria (TK).

[0053] La FIG. 14 es un diagrama de flujo que muestra un proceso 1400 a modo de ejemplo que funciona en una estación/terminal para generar y agrupar una solicitud de reautentificación y un mensaje de la capa superior (por ejemplo, solicitud de descubrimiento) en una solicitud de asociación. El bloque de funcionamiento 1402 indica que se recibe desde el punto de acceso una baliza que incluye un número aleatorio o nonce (por ejemplo, Anonce). En el bloque de funcionamiento 1404, el terminal genera una solicitud de reautentificación con un protocolo de autentificación extensible a partir de una clave de cifrado utilizando el número aleatorio o nonce. En el bloque de funcionamiento 1406, el terminal genera un mensaje de capa superior. Por ejemplo, dicho mensaje de capa superior puede ser una solicitud de descubrimiento, una solicitud de descubrimiento con confirmación rápida de protocolo de configuración dinámica de host (DHCP) y/o un mensaje de asignación de dirección de protocolo de internet (IP).

[0054] El bloque de funcionamiento 1408 indica que, en algunos modos de realización, el terminal puede generar una clave de sesión principal de reautentificación (rMSK) que responde a los resultados de un proceso de autentificación anterior. El bloque de funcionamiento 1410 indica que en algunos modos de realización el terminal puede generar una clave transitoria de pares (PTK) a partir de la rMSK, el número aleatorio (Anonce) y/o un número aleatorio generado localmente (Snonce).

[0055] El bloque de funcionamiento 1412 indica que en algunos modos de realización el terminal puede cifrar el mensaje de la capa superior con la rMSK. El bloque de funcionamiento 1414 indica que en algunos modos de realización el terminal puede cifrar el mensaje de capa superior con la PTK o una combinación de la KCK y la KEK. En otros modos de realización, el mensaje de la capa superior puede no estar cifrado.

[0056] El bloque de funcionamiento 1416 indica que en algunos modos de realización el terminal puede generar la solicitud de asociación como un primer mensaje que encapsula un mensaje de descubrimiento de DHCP, un segundo mensaje que encapsula un mensaje de inicio de reautentificación de EAPOL.

[0057] El bloque de funcionamiento 1418 indica que el terminal agrupa el mensaje de la capa superior y la solicitud reautentificación como una solicitud de asociación. El bloque de funcionamiento 1420 indica que en algunos modos de realización el terminal puede transmitir el primer mensaje y el segundo mensaje por separado.

[0058] La FIG. 15 es un diagrama de flujo que muestra un proceso 1500 a modo de ejemplo que funciona en una estación base para recibir y extraer una solicitud de reautentificación y un mensaje de la capa superior de una solicitud de asociación enviada por una estación/terminal. El bloque de funcionamiento 1502 indica que en algunos modos de realización el punto de acceso puede generar un número aleatorio y transmitir una baliza que incluye el número aleatorio.

[0059] El bloque de funcionamiento 1504 indica que el punto de acceso recibe desde un terminal una solicitud de asociación que incluye un mensaje de capa superior (por ejemplo, solicitud de descubrimiento) y una solicitud de reautentificación agrupados. El bloque de funcionamiento 1506 indica que el punto de acceso extrae el mensaje de capa superior de la solicitud de asociación y lo reenvía a un servidor de configuración. El bloque de funcionamiento 1508 indica que el punto de acceso extrae la solicitud de reautentificación de la solicitud de asociación y la reenvía a un servidor de autentificación.

[0060] El bloque de funcionamiento 1510 indica que en algunos modos de realización el punto de acceso puede recibir una clave de cifrado del servidor de autentificación. El bloque de funcionamiento 1512 indica que en algunos modos de realización el punto de acceso puede generar una PTK a partir de la clave de cifrado, el número aleatorio y un número aleatorio recibido desde el terminal. El bloque operativo 1514 indica que, en algunos modos de realización, el punto de acceso puede verificar el mensaje de la capa superior con una combinación de la KCK y la KEK dentro de la PTK, que incluye la KCK y la KEK.

[0061] Conjuntamente con los modos de realización descritos, un primer aparato puede incluir medios para generar, los medios para generar estando configurados para generar al menos una de una solicitud de reautorización o una solicitud de reautentificación con un protocolo de autentificación extensible, generar un mensaje de capa superior y agrupar el mensaje de capa superior y al menos una de la solicitud de reautorización o la solicitud de reautentificación como una solicitud de asociación. Por ejemplo, los medios para generar pueden incluir uno o más componentes (por ejemplo, un procesador) de la estación 106, la estación 108 o la estación 110, el DSP 210, las instrucciones 260, uno o más componentes (por ejemplo, un procesador) de la STA 302, uno o más dispositivos configurados para generar una solicitud de reautentificación y/o una solicitud de reautorización, generar un mensaje de capa superior y agrupar el mensaje de capa superior y la solicitud de reautentificación y/o la solicitud de reautorización, o una combinación de los mismos. El aparato también puede incluir medios para transmitir la solicitud de asociación a un punto de acceso. Por ejemplo, los medios para transmitir pueden incluir uno o más componentes (por ejemplo, un transmisor) de la estación 106, la estación 108 o la estación 110, la antena 242, el controlador inalámbrico 240, uno o más componentes (por ejemplo, un transmisor) de la STA 302, uno o más dispositivos configurados para transmitir una solicitud de asociación, o una combinación de los mismos.

[0062] Un segundo aparato puede incluir medios para recibir una solicitud de asociación desde un terminal. La solicitud de asociación incluye un mensaje de capa superior y al menos una de una solicitud de reautorización o una solicitud de reautentificación agrupados. Por ejemplo, los medios para recibir pueden incluir uno o más componentes (por ejemplo, un receptor) del punto de acceso 102, la antena 242, el controlador inalámbrico 240, el punto de acceso 304, uno o más dispositivos configurados para recibir una solicitud de asociación, o una combinación de los mismos. El segundo aparato también puede incluir medios para extraer, los medios para extraer estando configurados para extraer el mensaje de capa superior de la solicitud de asociación y reenviar el mensaje de capa superior a un servidor de configuración. Los medios para extraer se configuran, además, para extraer al menos una de la solicitud de reautorización o la solicitud de reautentificación de la solicitud de asociación y reenviar la solicitud de reautentificación a un servidor de autentificación. Por ejemplo, los medios para extraer pueden incluir uno o más componentes (por ejemplo, un procesador) del punto de acceso 102, el DSP 210, las instrucciones 260, uno o más componentes del punto de acceso 304, uno o más dispositivos configurados para extraer elementos de información de una solicitud de asociación, o una combinación de los mismos.

[0063] Uno o más de los modos de realización divulgados pueden implementarse en un sistema o un aparato, que puede incluir un dispositivo de comunicaciones, una unidad de datos de ubicación fija, una unidad de datos de ubicación móvil, un teléfono móvil, un teléfono celular, un ordenador, una tablet, un ordenador portátil o un ordenador de escritorio. Además, el sistema o el aparato puede incluir un descodificador, una unidad de entretenimiento, un dispositivo de navegación, un asistente digital personal (PDA), un monitor, un monitor de ordenador, un televisor, un sintonizador, una radio, una radio satelital, un reproductor de música, un reproductor de música digital, un reproductor de música portátil, un reproductor de vídeo, un reproductor de vídeo digital, un reproductor de disco de vídeo digital (DVD), un reproductor de vídeo digital portátil, cualquier otro dispositivo que almacene o recupere datos o instrucciones del ordenador, o una combinación de los mismos. Como otro ejemplo ilustrativo, no limitativo, el sistema o el aparato pueden incluir unidades remotas, como teléfonos móviles, unidades de sistemas de comunicación personal portátiles (PCS), unidades de datos portátiles como asistentes de datos personales, dispositivos habilitados para el sistema de posicionamiento global (GPS), dispositivos de navegación, unidades de datos de ubicación fija, como equipos de lectura de medidores, o cualquier otro dispositivo que almacene o recupere datos o instrucciones de ordenador, o cualquier combinación de los mismos. Aunque una o más de las FIGS. 1-15 ilustran sistemas, aparatos y/o procedimientos de acuerdo con las enseñanzas de la divulgación, la divulgación no se limita a estos sistemas, aparatos y/o procedimientos ilustrados. Los modos de realización de la divulgación pueden emplearse adecuadamente en cualquier dispositivo que incluya circuitos integrados incluyendo memoria, un procesador y circuitos en chip.

[0064] Debe entenderse que cualquier referencia a un elemento en el presente documento que use una designación tal como "primer", "segundo" y así sucesivamente no limita en general la cantidad ni el orden de esos elementos. En su lugar, estas designaciones se pueden usar en el presente documento como un procedimiento conveniente de diferenciación entre dos o más elementos o instancias de un elemento. Por tanto, una referencia

a un primer y a un segundo elemento no significa que se puedan emplear solamente dos elementos o que el primer elemento deba preceder al segundo elemento de alguna manera. Asimismo, a menos que se establezca de otro modo, un conjunto de elementos puede comprender uno o más elementos. Como se usa en el presente documento, el término “determinar” abarca una amplia variedad de acciones. Por ejemplo, "determinar" puede incluir calcular, computar, procesar, obtener, investigar, consultar (por ejemplo, consultar una tabla, una base de datos u otra estructura de datos), averiguar y similares. Además, "determinar" puede incluir recibir (por ejemplo, recibir información), acceder (por ejemplo, acceder a datos en una memoria) y similares. Además, "determinar" puede incluir resolver, seleccionar, elegir, establecer y similares. Además, un “ancho de canal”, como se usa en el presente documento, puede abarcar, o se puede denominar también como, un ancho de banda en determinados aspectos.

[0065] Como se usa en el presente documento, una frase que hace referencia a "al menos uno de" una lista de elementos se refiere a cualquier combinación de esos elementos, incluyendo miembros únicos. Por ejemplo, "al menos uno de: a, b o c" pretende abarcar: a, b, c, a-b, a-c, b-c y a-b-c.

[0066] En lo que antecede se han descrito diversos componentes, bloques, configuraciones, módulos, circuitos y etapas ilustrativos, en general, en términos de su funcionalidad. Que dicha funcionalidad se implemente como hardware o instrucciones ejecutables por procesador depende de la aplicación particular y de las restricciones de diseño impuestas al sistema global. Adicionalmente, las diversas operaciones de los procedimientos descritos anteriormente pueden ser realizadas por cualquier medio adecuado capaz de realizar las operaciones, tales como diversos componentes, circuitos y/o módulos de hardware y/o software. En general, unos medios funcionales correspondientes capaces de realizar las operaciones pueden realizar cualquier operación ilustrada en las FIG. 1-15. Los expertos en la técnica pueden implementar la funcionalidad descrita de distintas formas para cada aplicación en particular, pero no se debe interpretar que dichas decisiones de implementación suponen apartarse del alcance de la presente divulgación.

[0067] Los expertos en la técnica apreciarán, además, que los diversos bloques lógicos, configuraciones, módulos, circuitos y etapas de algoritmos ilustrativos descritos en relación con la presente divulgación pueden implementarse o realizarse con un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), una señal de matriz de puertas programables in situ (FPGA) u otro dispositivo de lógica programable (PLD), lógica de puertas discretas o transistores, componentes de hardware discretos (por ejemplo, hardware electrónico), software informático ejecutado por un procesador, o cualquier combinación de los mismos diseñada para desempeñar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador pero, de forma alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados disponible en el mercado. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo.

[0068] En uno o más aspectos, las funciones descritas se pueden implementar en hardware, software, firmware o en cualquier combinación de los mismos. Si se implementan en software, las funciones pueden almacenarse como una o más instrucciones o como código en un medio legible por ordenador. Los medios legibles por ordenador incluyen tanto medios de almacenamiento legibles por ordenador como medios de comunicación, incluyendo cualquier medio que facilita la transferencia de un programa informático de un lugar a otro. Un medio de almacenamiento puede ser cualquier medio disponible al que se puede acceder mediante un ordenador. A modo de ejemplo, y no de limitación, dichos medios de almacenamiento legibles por ordenador pueden incluir memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de solo lectura programable (PROM), PROM borrable (EPROM), PROM borrable eléctricamente (EEPROM), uno o más registros, un disco duro, un disco extraíble, una memoria de solo lectura de disco compacto (CD-ROM), otro tipo de dispositivo de almacenamiento en disco óptico, almacenamiento en disco magnético, dispositivos de almacenamiento magnético o cualquier otro medio que se pueda usar para almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que se puede acceder desde un ordenador. De forma alternativa, los medios legibles por ordenador (por ejemplo, un medio de almacenamiento) pueden estar integrados en el procesador. El procesador y el medio de almacenamiento pueden residir en un circuito integrado específico de la aplicación (ASIC). El ASIC puede residir en un dispositivo informático o en un terminal de usuario. Como alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un dispositivo informático o en un terminal de usuario.

[0069] Además, cualquier conexión recibe adecuadamente la denominación de medio legible por ordenador. Por ejemplo, si el software se transmite desde un sitio web, un servidor u otra fuente remota usando un cable coaxial, un cable de fibra óptica, un par trenzado, una línea de abonado digital (DSL) o unas tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, la DSL o las tecnologías inalámbricas, tales como infrarrojos, radio y microondas, están incluidos en la definición de medio. Los discos, como se usan en el presente documento, incluyen el disco compacto (CD), el disco láser, el disco óptico, el disco versátil digital (DVD), el disco flexible y el disco Blu-ray®, de los cuales los discos flexibles reproducen normalmente datos magnéticamente, mientras que los demás discos reproducen datos ópticamente

con láseres. Por tanto, en algunos aspectos, el medio legible por ordenador puede incluir un medio legible por ordenador no transitorio (por ejemplo, medios tangibles). Además, en algunos aspectos, el medio legible por ordenador puede incluir un medio legible por ordenador transitorio (por ejemplo, una señal). Las combinaciones de los anteriores también se deben incluir dentro del alcance de los medios legibles por ordenador.

[0070] Los procedimientos divulgados en el presente documento incluyen un o más etapas o acciones para lograr el procedimiento descrito. Las etapas y/o acciones de procedimiento se pueden intercambiar entre sí sin apartarse del alcance de las reivindicaciones. En otras palabras, a menos que se especifique un orden específico de etapas o acciones, el orden y/o el uso de etapas y/o acciones específicas se pueden modificar sin apartarse del alcance de las reivindicaciones.

[0071] Por lo tanto, determinados aspectos pueden comprender un producto de programa informático para realizar las operaciones presentadas en el presente documento. Por ejemplo, un producto de programa informático puede incluir un medio de almacenamiento legible por ordenador que tiene instrucciones almacenadas (y/o codificadas) en el mismo, siendo las instrucciones ejecutables por uno o más procesadores para realizar las operaciones descritas en el presente documento. Para determinados aspectos, el producto de programa informático puede incluir material de embalaje.

[0072] El software o las instrucciones también se pueden transmitir sobre un medio de transmisión. Por ejemplo, si el software se transmite desde un sitio web, un servidor u otra fuente remota usando un cable coaxial, un cable de fibra óptica, un par trenzado, una línea de abonado digital (DSL) o tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, la DSL o las tecnologías inalámbricas tales como infrarrojos, radio y microondas están incluidos en la definición de medio de transmisión.

[0073] Además, debería apreciarse que los módulos y/u otros medios adecuados para realizar los procedimientos y las técnicas descritos en el presente documento pueden descargarse y/u obtenerse de otra forma por un terminal de usuario y/o una estación base, según corresponda. De forma alternativa, se pueden proporcionar varios procedimientos descritos en el presente documento a través de medios de almacenamiento (por ejemplo, RAM, ROM, un medio de almacenamiento físico tal como un disco compacto (CD)). Además, se puede utilizar cualquier otra técnica adecuada para proporcionar los procedimientos y técnicas descritos en el presente documento.

[0074] La anterior descripción de los modos de realización divulgados se proporciona para permitir que cualquier experto en la técnica realice o use los modos de realización divulgados. Aunque lo anterior está dirigido a aspectos de la presente divulgación, se pueden concebir aspectos diferentes y adicionales de la divulgación sin apartarse del alcance básico de la misma, y el alcance de la misma está determinado por las reivindicaciones siguientes. Se pueden realizar diversas modificaciones, cambios y variaciones en la disposición, el funcionamiento y los detalles de los modos de realización descritos en el presente documento sin apartarse del alcance de la divulgación o las reivindicaciones.

REIVINDICACIONES

1. Un procedimiento de uso de un terminal para comunicaciones inalámbricas, comprendiendo el procedimiento:

derivar una clave de integridad de reautentificación, rIK, basada en realizar un intercambio de autentificación EAP completa inicial con un servidor de autentificación (308);

recibir, en un terminal móvil desde un punto de acceso, una indicación para admitir un establecimiento rápido de enlace inicial, FILS, incluido el procesamiento de una solicitud agrupada que incluye una solicitud de protocolo de reautentificación extensible, EAP-RP, y un mensaje de capa superior, en el que la indicación se incluye en una baliza o un mensaje de respuesta de sonda, en el que el mensaje de la capa superior comprende un mensaje de asignación de dirección de protocolo de Internet, IP, una solicitud de descubrimiento con confirmación rápida de protocolo de configuración de host dinámico, DHCP, una solicitud de descubrimiento o una combinación de los mismos; y

en respuesta a recibir la indicación:

generar (1404), en el terminal móvil, la solicitud EAP-RP utilizando la clave de integridad de reautentificación, rIK;

generar (1406), en el terminal móvil, el mensaje de la capa superior;

agrupar la solicitud de reautentificación EAP y el mensaje de la capa superior para generar (1418) la solicitud agrupada, en la que la solicitud agrupada se genera dentro de un período de autentificación después de que el terminal móvil realice dicho intercambio de autentificación EAP completa; y

transmitir una solicitud agrupada desde un terminal al punto de acceso.

2. El procedimiento según la reivindicación 1, en el que el mensaje de la capa superior se cifra (1412) antes de la transmisión de la solicitud agrupada al punto de acceso.

3. El procedimiento según la reivindicación 1, en el que el mensaje de la capa superior se incluye en la solicitud agrupada como un elemento de información de acuerdo con un estándar del Instituto de Ingenieros Eléctricos y Electrónicos, IEEE.

4. El procedimiento según la reivindicación 1, que comprende, además, recibir un mensaje de respuesta de dirección de protocolo de Internet, IP, en el que el mensaje de respuesta de dirección IP se incluye en una respuesta como un elemento de información de acuerdo con un estándar del Instituto de Ingenieros Eléctricos y Electrónicos, IEEE.

5. El procedimiento según la reivindicación 1, en el que la solicitud agrupada incluye un primer nonce previamente obtenido del punto de acceso.

6. El procedimiento según la reivindicación 5, en el que el primer nonce es verificable por el punto de acceso para determinar que el primer nonce fue emitido por el punto de acceso dentro de un período de tiempo particular.

7. El procedimiento según la reivindicación 5, en el que el primer nonce está incluido (1402) en una baliza o en un mensaje de respuesta de sonda.

8. El procedimiento según la reivindicación 1, que comprende, además, obtener la indicación de soporte de protocolo de reautentificación de protocolo de autentificación extensible, EAP-RP, desde el punto de acceso antes de la transmisión de la solicitud agrupada.

9. El procedimiento según la reivindicación 1, que comprende, además, obtener una indicación de soporte de cifrado de la dirección de protocolo de internet, IP, desde el punto de acceso antes de la transmisión de la solicitud agrupada.

10. El procedimiento según la reivindicación 1, en el que agrupar el mensaje de la capa superior y la solicitud de reautentificación de EAP como la solicitud agrupada incluye agrupar el mensaje de la capa superior y la solicitud EAP como elementos de información separados de acuerdo con un estándar del Instituto de Ingenieros Eléctricos y Electrónicos, IEEE.

11. El procedimiento según la reivindicación 1, en el que la solicitud agrupada incluye, además, al menos un mensaje de establecimiento de comunicación de cuatro vías, en el que el al menos un mensaje de establecimiento de comunicación de cuatro vías incluye un nonce de punto de acceso, Anonce, un nonce de

estación, Snonce, una clave temporal de grupo, GTK, un mensaje de confirmación de clave o una combinación de los mismos.

12. El procedimiento según la reivindicación 1, en el que la solicitud agrupada se genera dentro de un período de tiempo dado del terminal móvil que realiza una autentificación EAP completa, y en el que después del período de tiempo dado, el terminal móvil recibe una notificación para realizar la autentificación EAP completa.

13. El procedimiento según la reivindicación 12, que comprende, además:

generar, en el terminal móvil después del período de tiempo dado, una segunda solicitud agrupada; y recibir un mensaje que inicia la autentificación EAP completa desde el punto de acceso.

14. El procedimiento según la reivindicación 12, en el que el período de tiempo dado es de dos semanas.

15. El procedimiento según la reivindicación 1, en el que el mensaje de la capa superior está asociado con la asignación de una dirección de protocolo de internet, IP, al terminal móvil.

16. Un aparato, que comprende:

medios para derivar una clave de integridad de reautentificación, rIK, basada en realizar un intercambio de autentificación EAP completa inicial con un servidor de autentificación (308);

medios para recibir (242), desde un punto de acceso, una indicación de soporte del establecimiento rápido de enlace inicial, FILS, incluido el procesamiento de una solicitud agrupada que incluye una solicitud de protocolo de reautentificación extensible, EAP-RP, y un mensaje de capa superior, en el que la indicación se incluye en una baliza o en un mensaje de respuesta de sonda, en el que el mensaje de capa superior comprende un protocolo de Internet, IP, mensaje de asignación de dirección, una solicitud de descubrimiento con confirmación rápida de protocolo de configuración de host dinámico, DHCP, una solicitud de descubrimiento o una combinación de las mismas; y

medios para generar (260) la solicitud agrupada en un terminal móvil, los medios para generar configurados para, en respuesta a la indicación:

generar la solicitud EAP-RP utilizando la clave de integridad de reautentificación, rIK;

generar el mensaje de la capa superior; y

agrupar el mensaje de la capa superior y la solicitud EAP-RP para generar la solicitud agrupada, en el que la solicitud agrupada se genera dentro de un período de autentificación después de que el terminal móvil realice dicho intercambio de autentificación EAP completa; y

medios para transmitir (242) una solicitud agrupada desde un terminal móvil al punto de acceso.

17. El aparato según la reivindicación 16, en el que la solicitud agrupada incluye un primer nonce obtenido previamente del punto de acceso.

18. Un producto de programa informático que comprende instrucciones, que cuando se ejecutan en un ordenador, realizan un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 15.

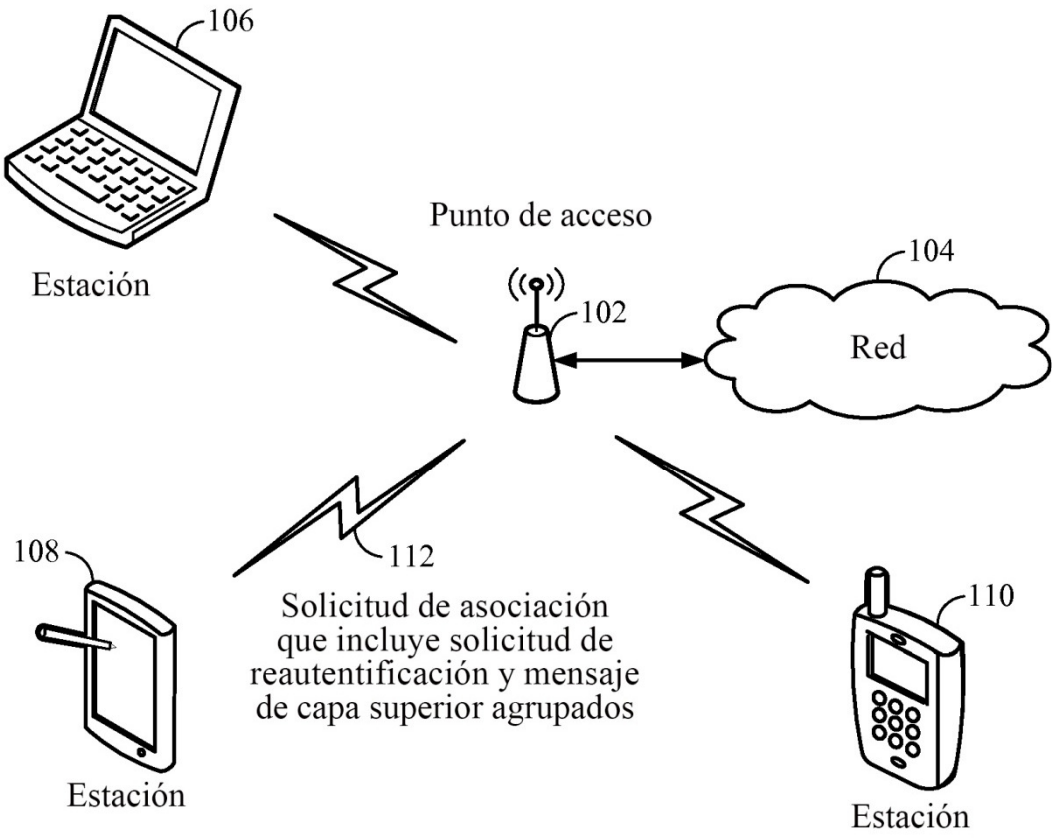
106
Estación
Punto de acceso
102
104
Red
112
Solicitud de asociación
que incluye solicitud de
reautentificación y mensaje
de capa superior agrupados
108
Estación
110
Estación

FIG. 1

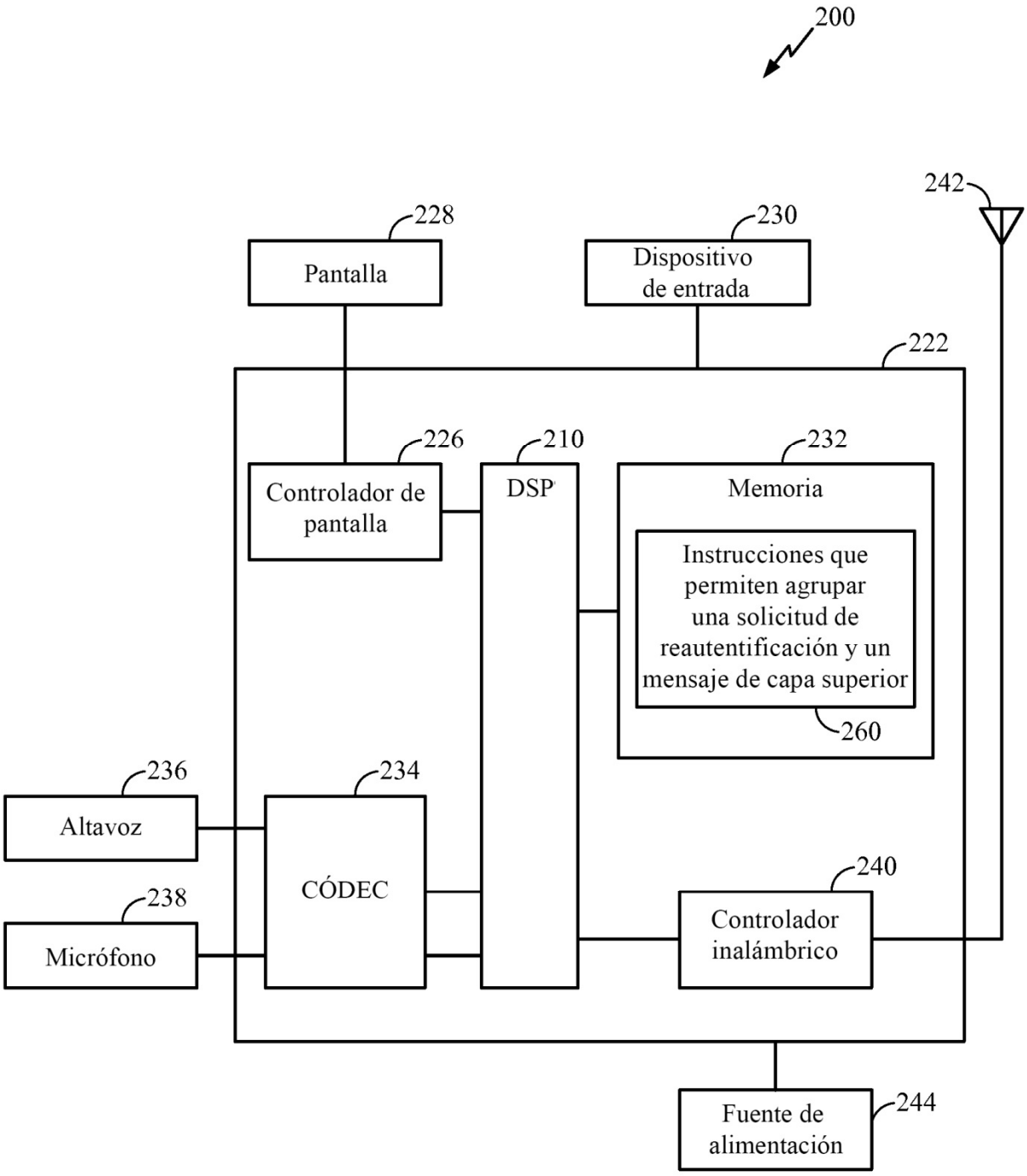
200
242
228
Pantalla
230
Dispositivo de entrada
222
226
Controlador de pantalla
210
DSP
232
Memoria
Instrucciones que permiten agrupar una solicitud de reautentificación y un mensaje de capa superior
260
236
Altavoz
234
CÓDEC
238
Micrófono
240
Controlador inalámbrico
Fuente de alimentación
244

FIG. 2

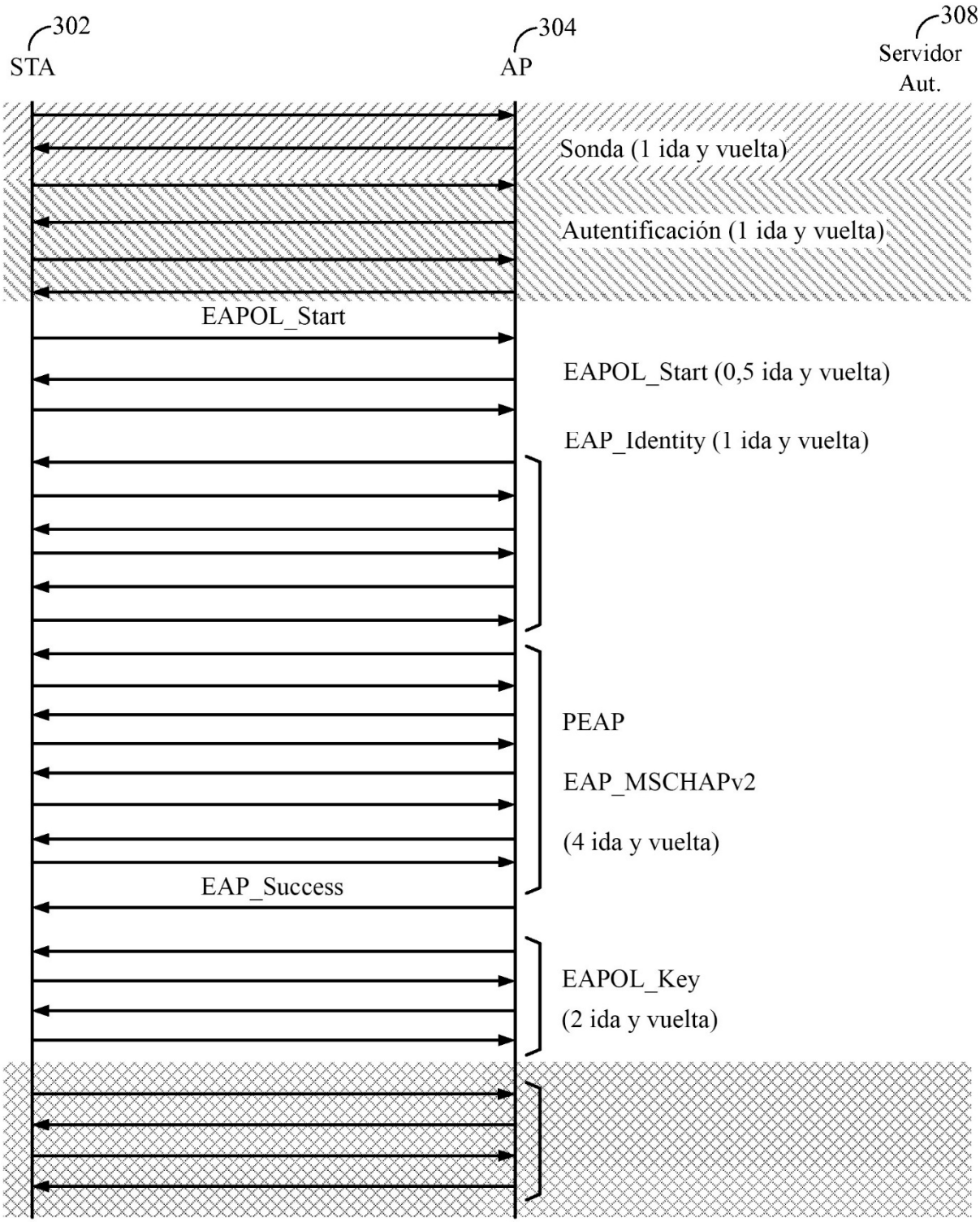
302
STA
304
AP
308
Servidor
Aut.
Sonda (1 ida y vuelta)
Autentificación (1 ida y vuelta)
EAPOL_Start
EAPOL_Start (0,5 ida y vuelta)
EAP_Identity (1 ida y vuelta)
PEAP
EAP_MSCHAPv2
(4 ida y vuelta)
EAP_Success
EAPOL_Key
(2 ida y vuelta)

FIG. 3

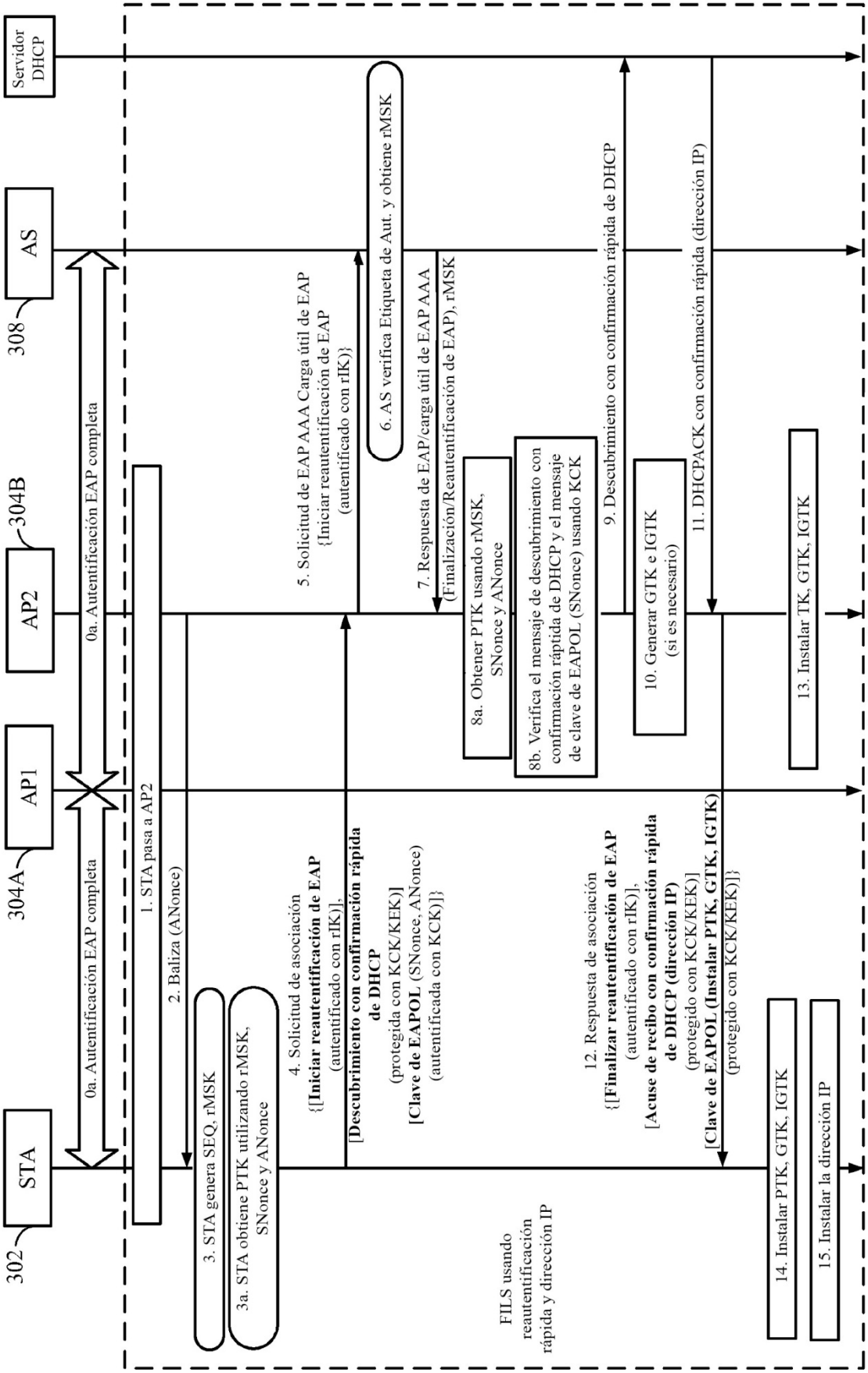

FIG. 4 (Opción 1)

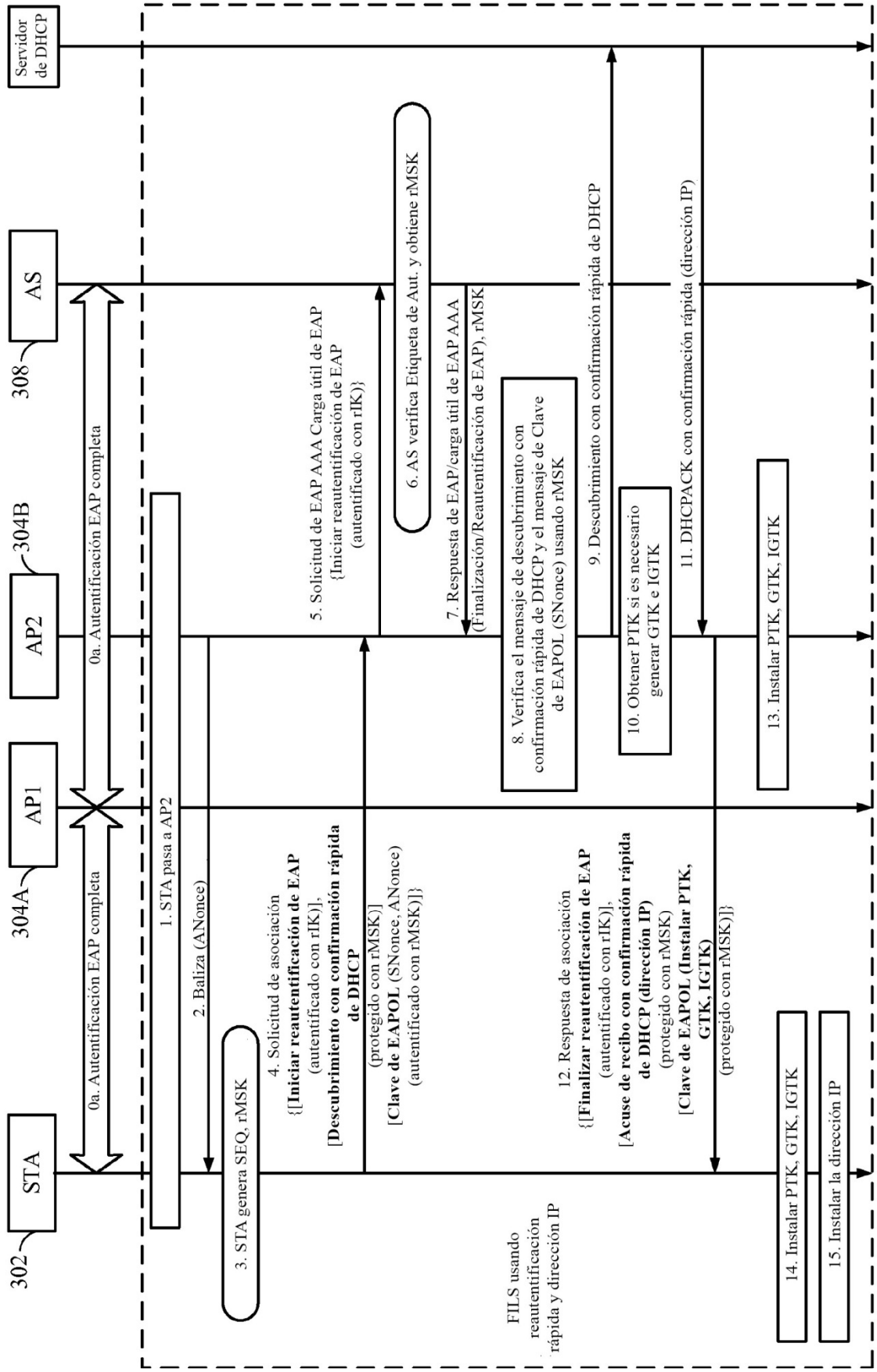

FIG. 5 (Opción 1a)

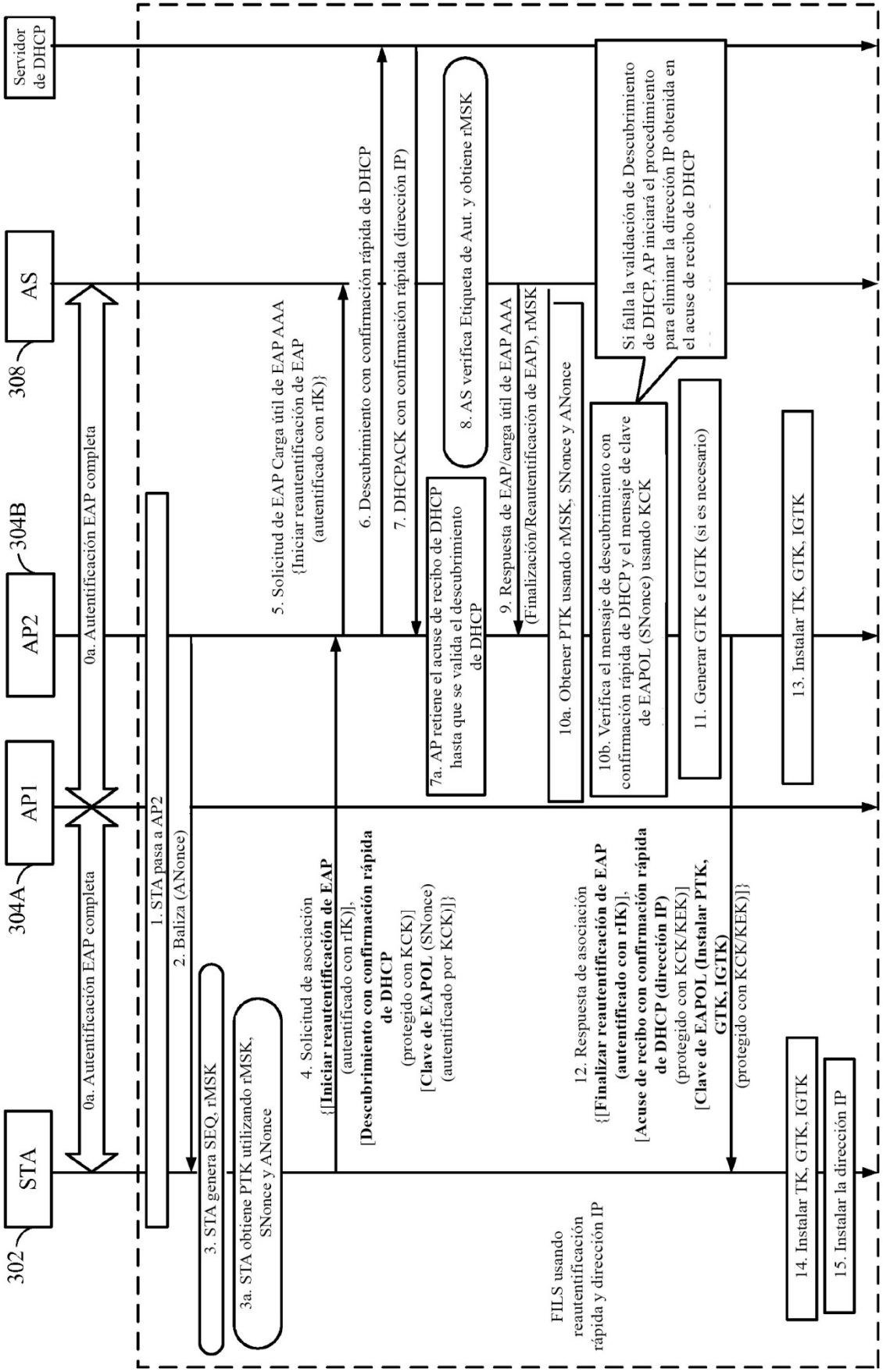

FIG. 6 (Opción 1b)

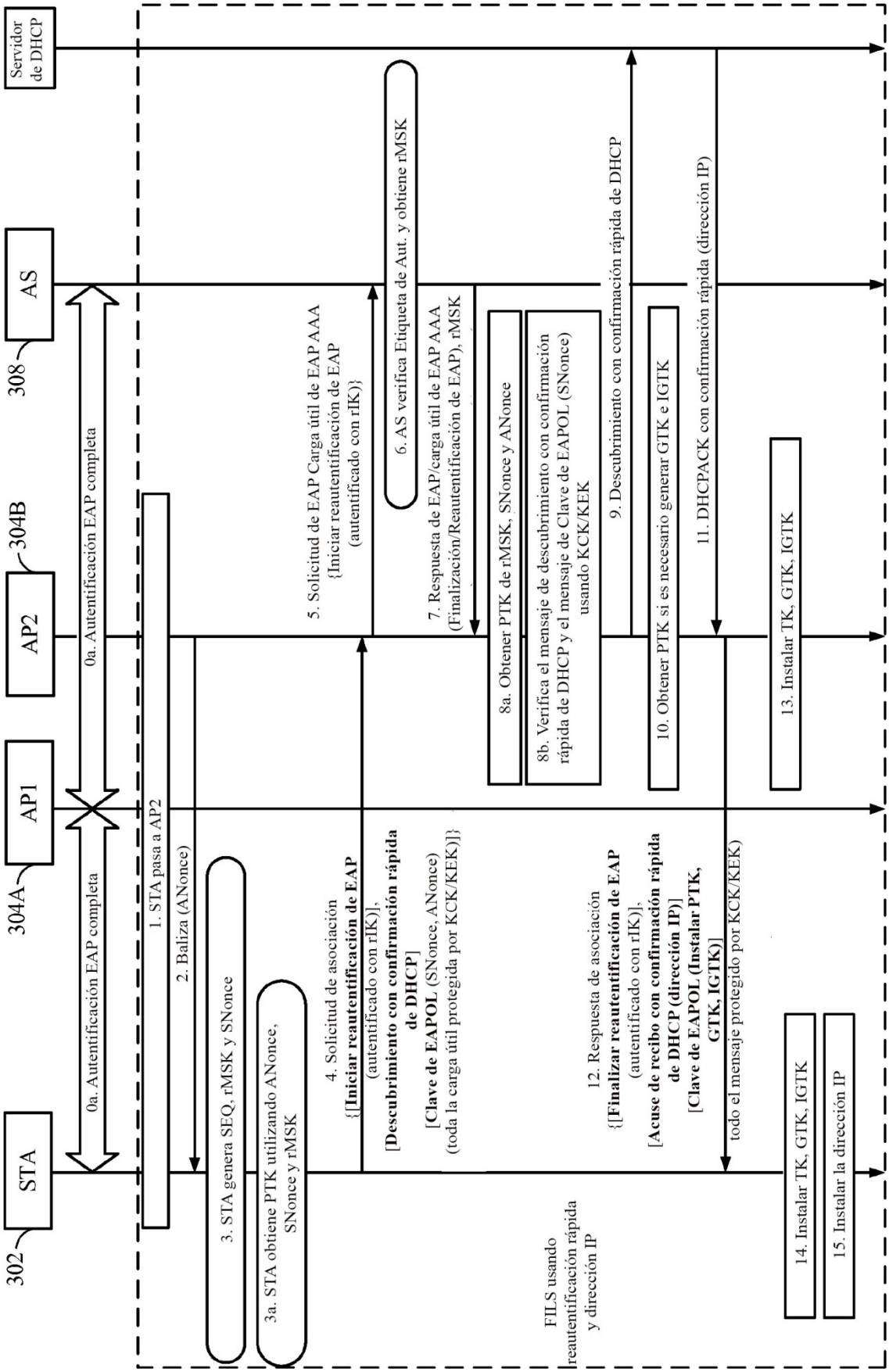

FIG. 7 (Opción 2)

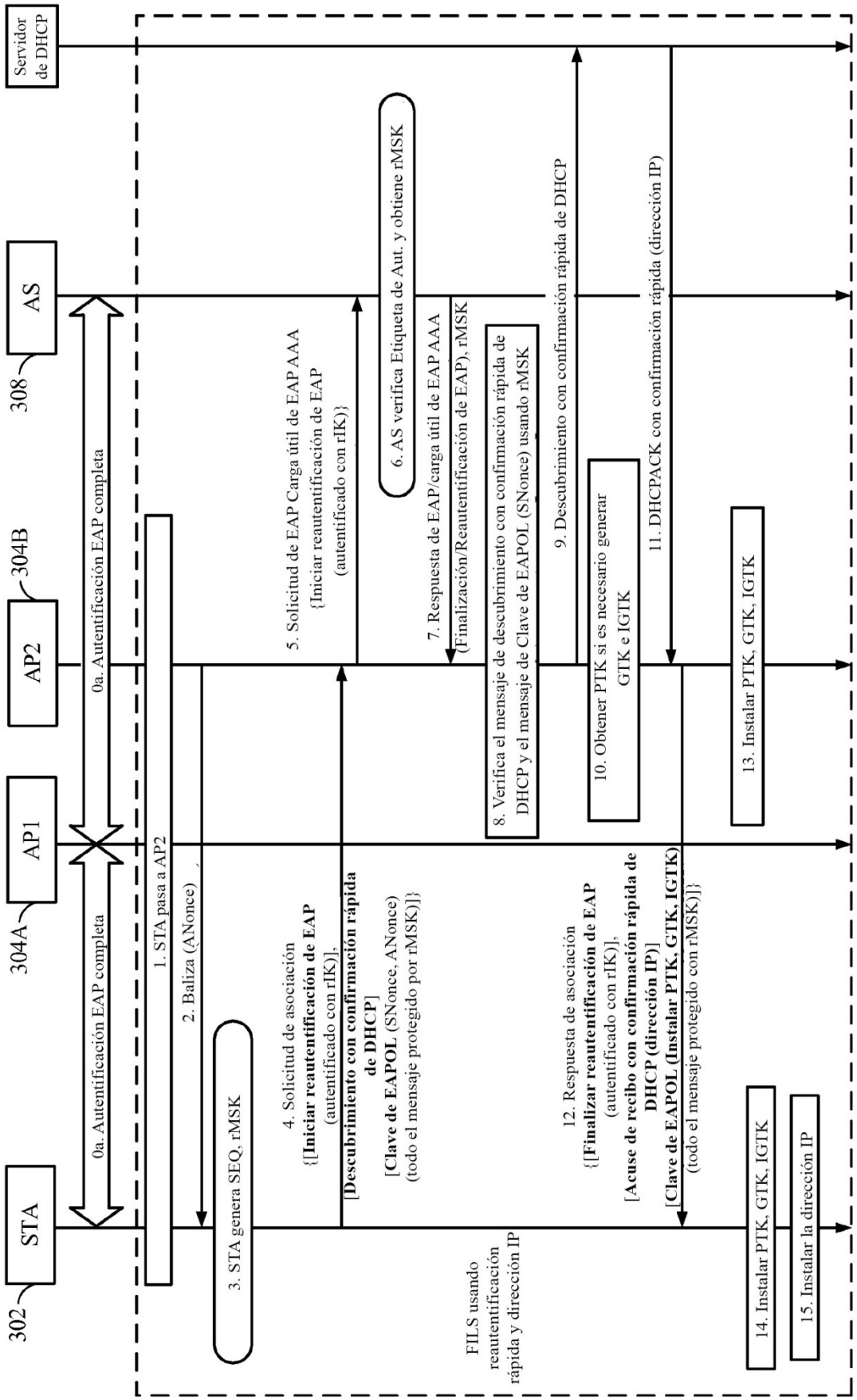

FIG. 8 (Opción 2a)

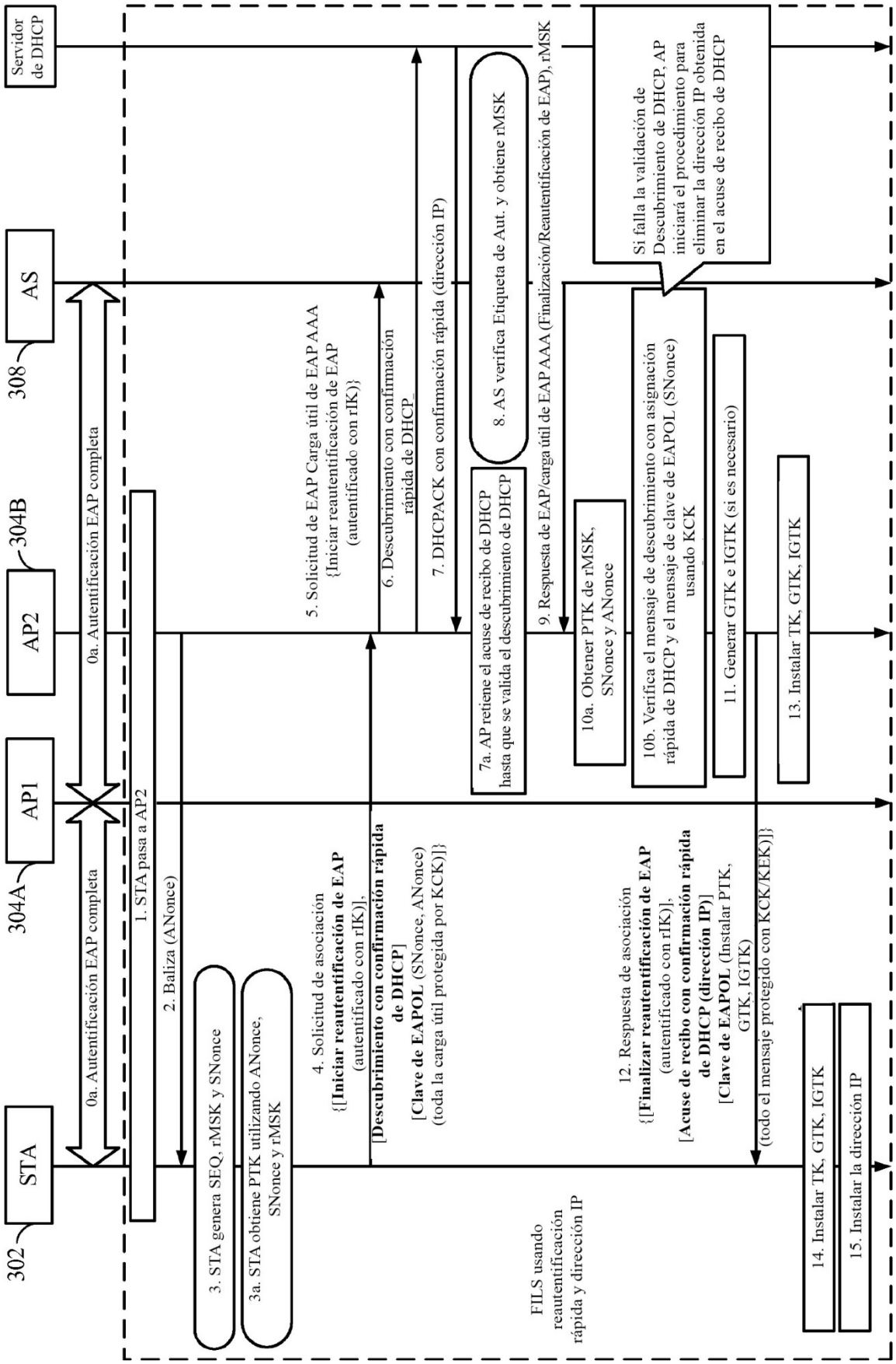

FIG. 9 (Opción 2b)

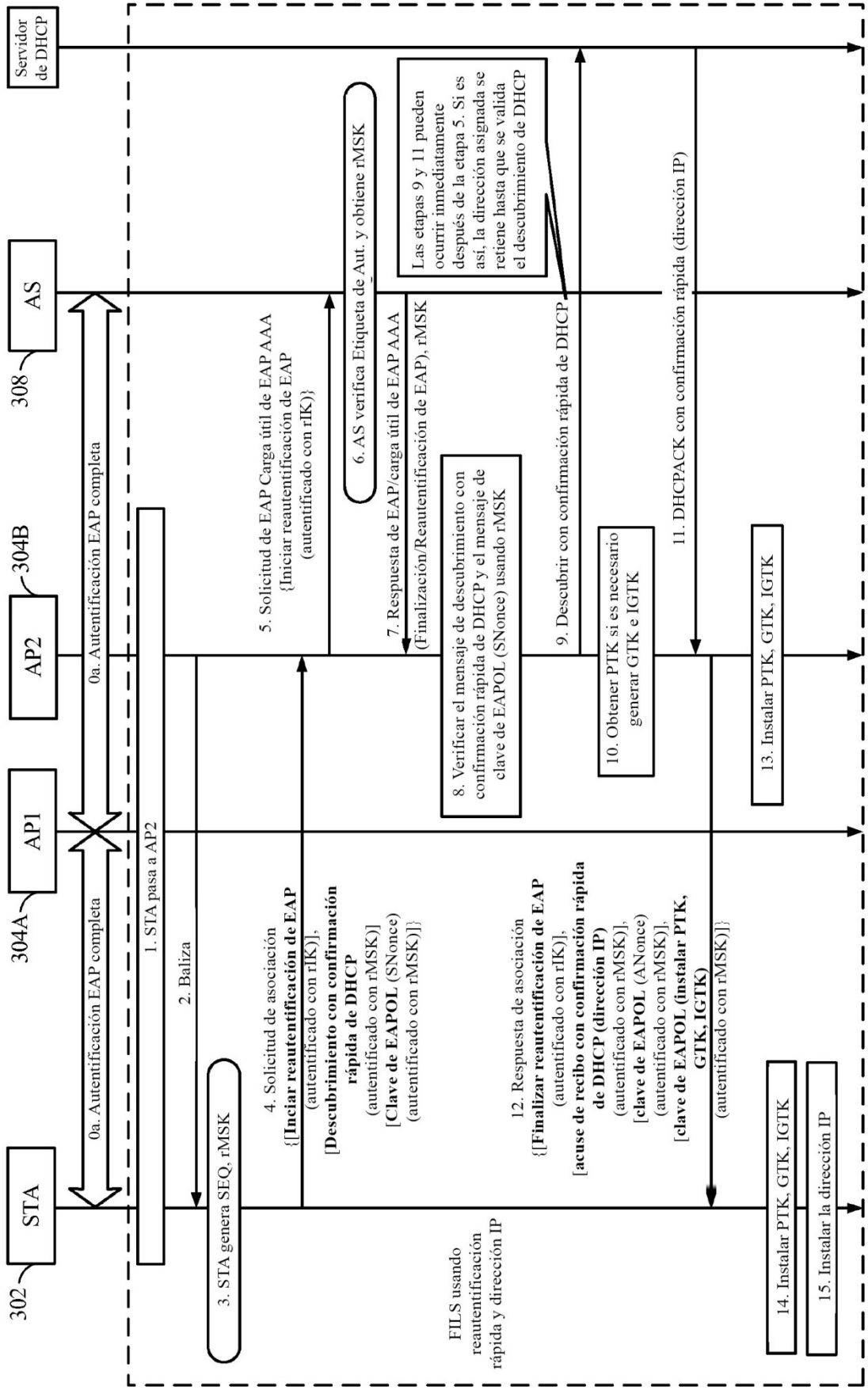

FIG. 10 (Opción 3)

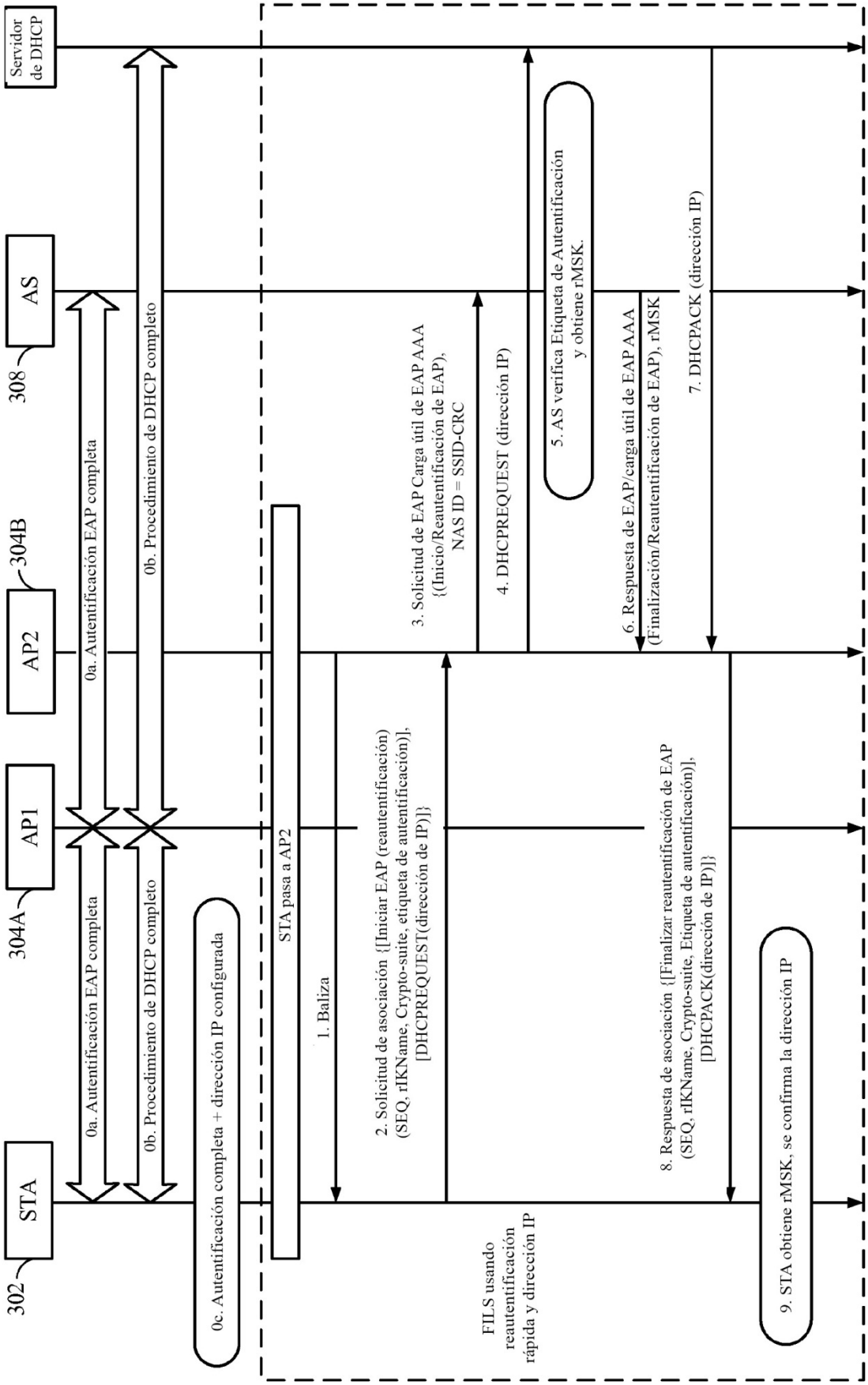

FIG. 11 (Opción 5)

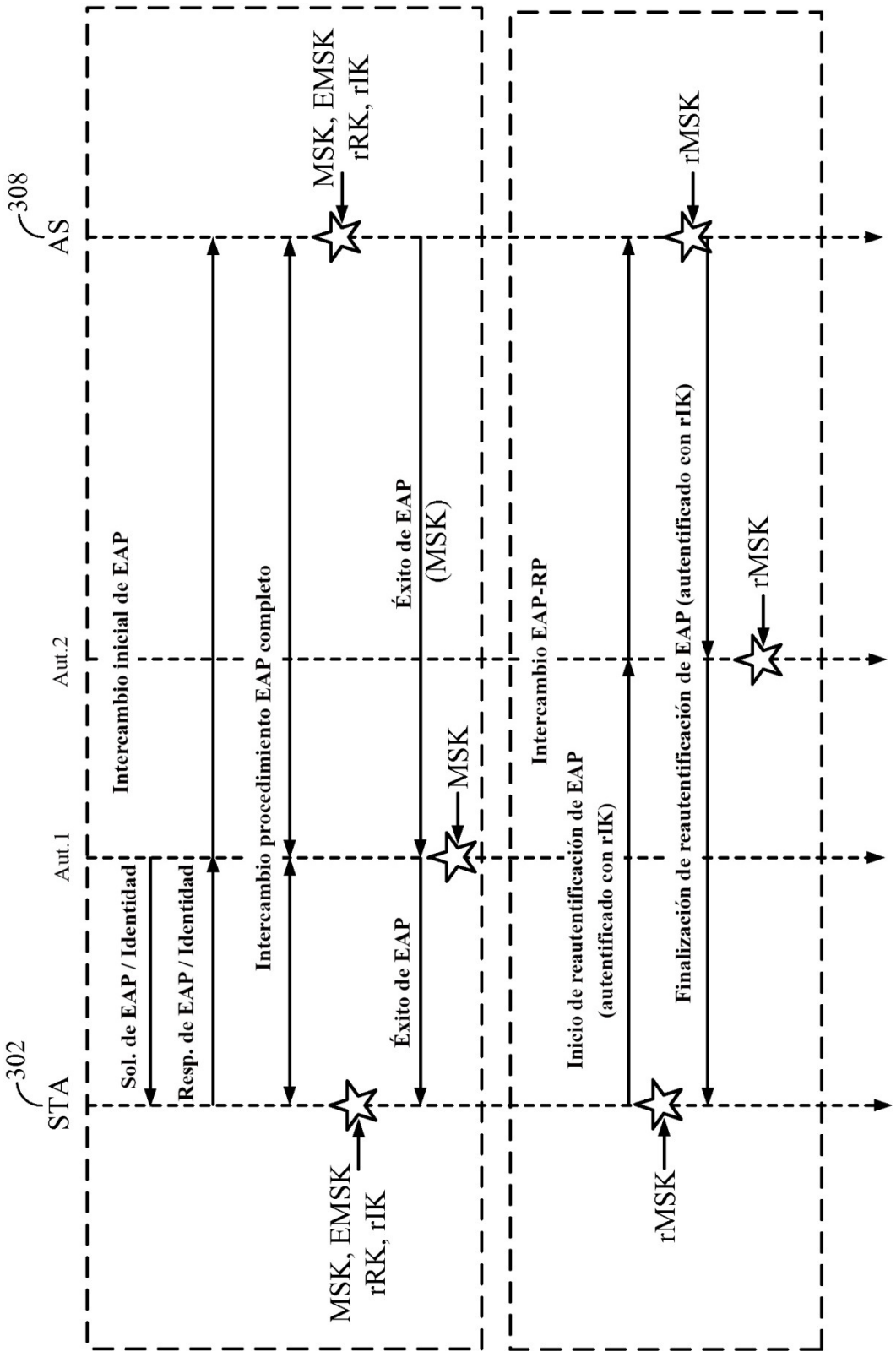
302
STA
Aut.1
Aut.2
308
AS
Intercambio inicial de EAP
Sol. de EAP / Identidad
Resp. de EAP / Identidad
Intercambio procedimiento EAP completo
MSK, EMSK
rRK, rIK
Éxito de EAP
MSK
Éxito de EAP
(MSK)
MSK, EMSK
rRK, rIK
Intercambio EAP-RP
Inicio de reautentificación de EAP
(autentificado con rIK)
rMSK
Finalización de reautentificación de EAP (autentificado con rIK)
rMSK
rMSK

FIG. 12

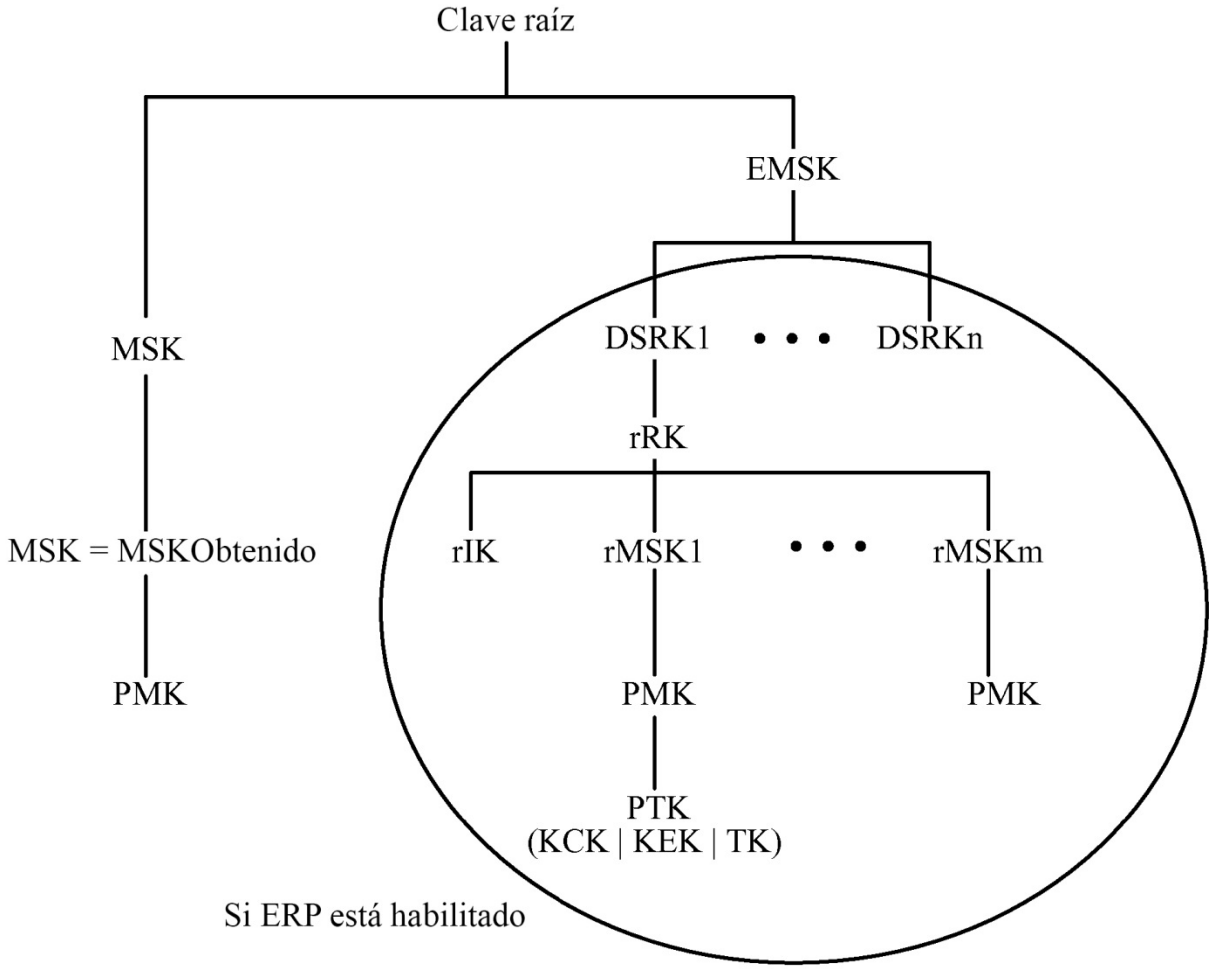
Clave raíz
EMSK
MSK
DSRK1
DSRKn
rRK
MSK = MSKObtenido
rIK
rMSK1
rMSKm
PMK
PMK
PMK
PTK
(KCK | KEK | TK)
Si ERP está habilitado

FIG. 13

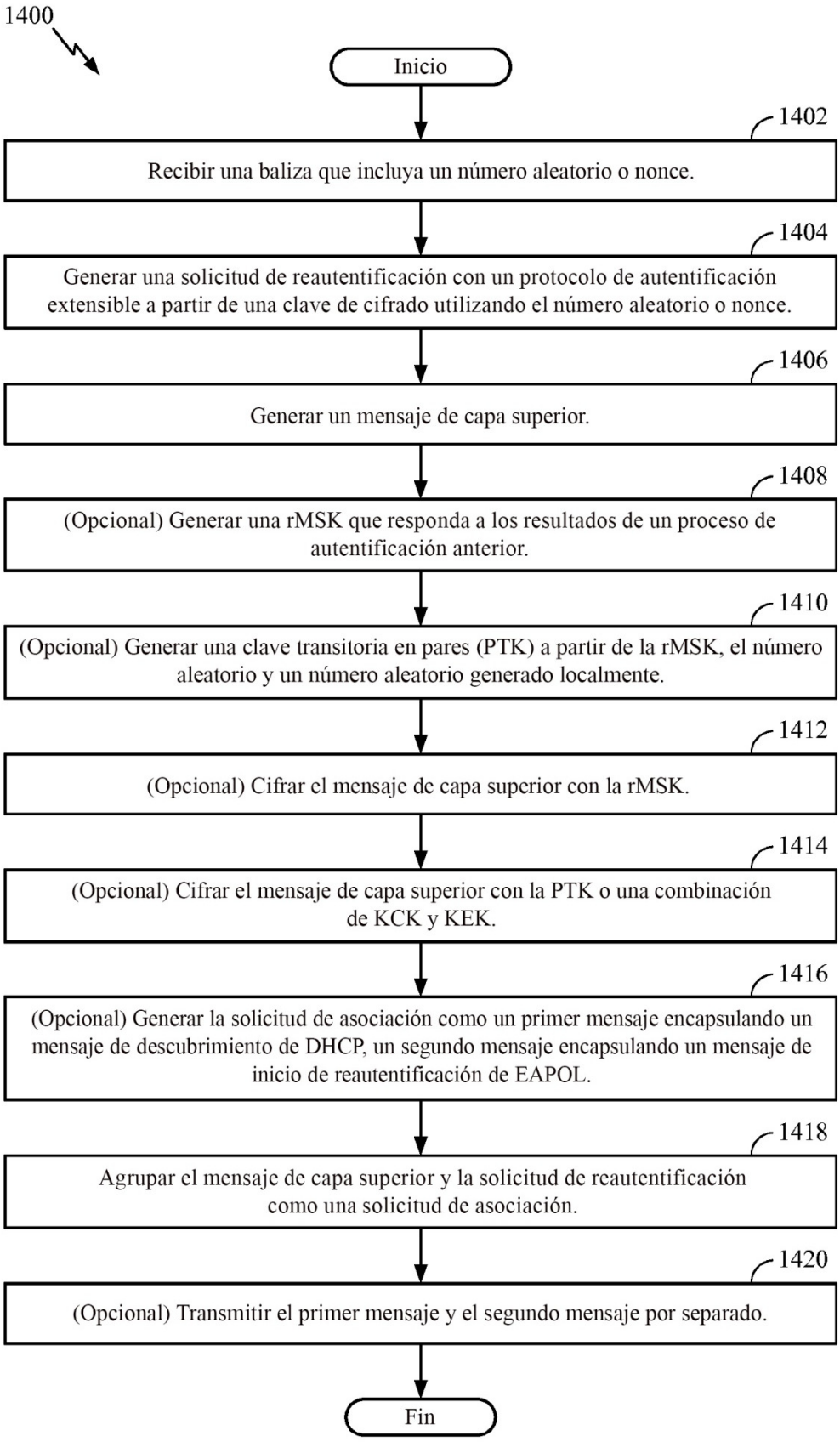
1400
Inicio
1402
Recibir una baliza que incluya un número aleatorio o nonce.
1404
Generar una solicitud de reautentificación con un protocolo de autentificación extensible a partir de una clave de cifrado utilizando el número aleatorio o nonce.
1406
Generar un mensaje de capa superior.
1408
(Opcional) Generar una rMSK que responda a los resultados de un proceso de autentificación anterior.
1410
(Opcional) Generar una clave transitoria en pares (PTK) a partir de la rMSK, el número aleatorio y un número aleatorio generado localmente.
1412
(Opcional) Cifrar el mensaje de capa superior con la rMSK.
1414
(Opcional) Cifrar el mensaje de capa superior con la PTK o una combinación de KCK y KEK.
1416
(Opcional) Generar la solicitud de asociación como un primer mensaje encapsulando un mensaje de descubrimiento de DHCP, un segundo mensaje encapsulando un mensaje de inicio de reautentificación de EAPOL.
1418
Agrupar el mensaje de capa superior y la solicitud de reautentificación como una solicitud de asociación.
1420
(Opcional) Transmitir el primer mensaje y el segundo mensaje por separado.
Fin

FIG. 14

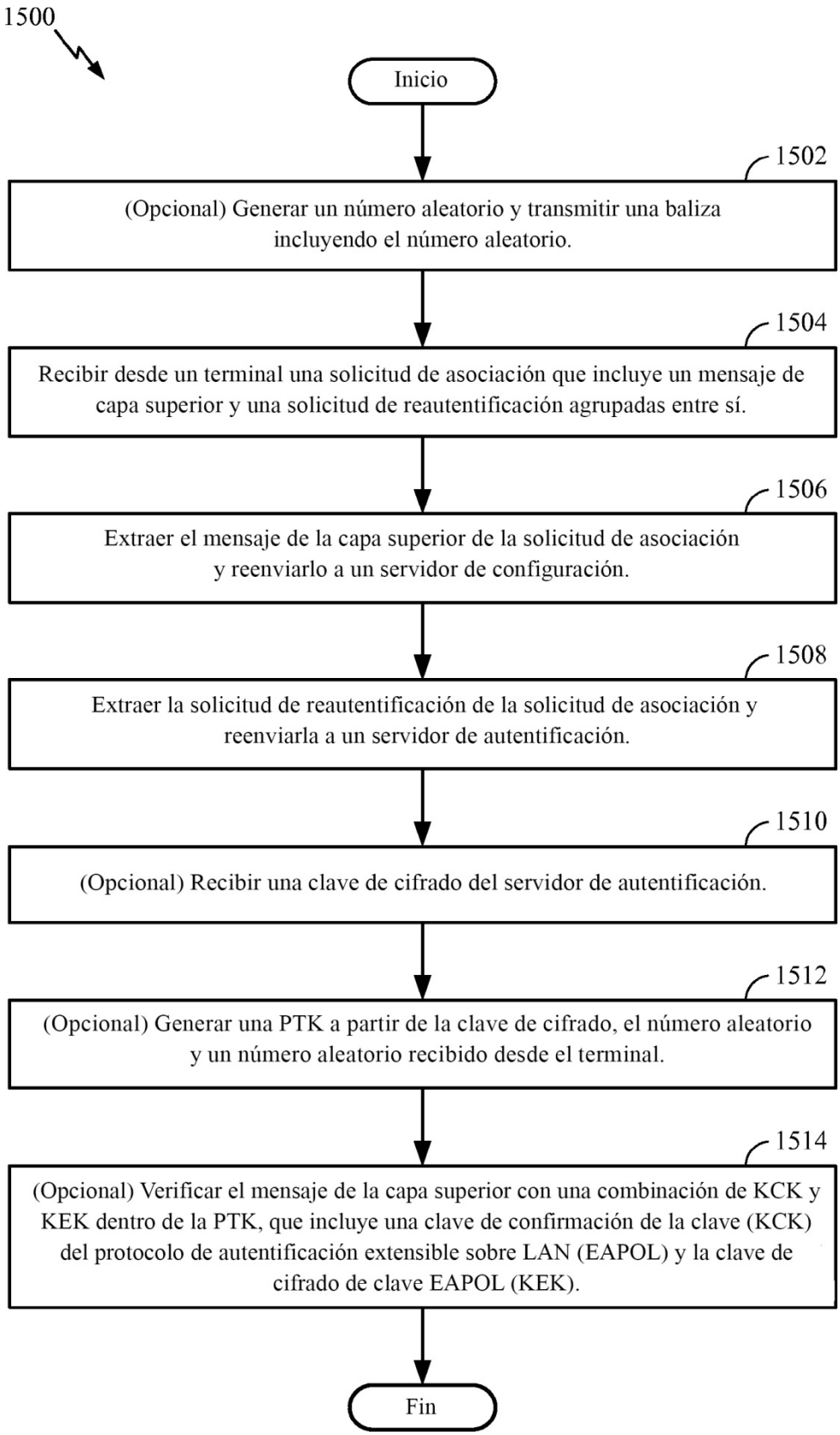
1500
Inicio
1502
(Opcional) Generar un número aleatorio y transmitir una baliza incluyendo el número aleatorio.
1504
Recibir desde un terminal una solicitud de asociación que incluye un mensaje de capa superior y una solicitud de reautentificación agrupadas entre sí.
1506
Extraer el mensaje de la capa superior de la solicitud de asociación y reenviarlo a un servidor de configuración.
1508
Extraer la solicitud de reautentificación de la solicitud de asociación y reenviarla a un servidor de autentificación.
1510
(Opcional) Recibir una clave de cifrado del servidor de autentificación.
1512
(Opcional) Generar una PTK a partir de la clave de cifrado, el número aleatorio y un número aleatorio recibido desde el terminal.
1514
(Opcional) Verificar el mensaje de la capa superior con una combinación de KCK y KEK dentro de la PTK, que incluye una clave de confirmación de la clave (KCK) del protocolo de autentificación extensible sobre LAN (EAPOL) y la clave de cifrado de clave EAPOL (KEK).
Fin

FIG. 15