(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 621 990**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.09.2012 PCT/US2012/054879**

(87) Fecha y número de publicación internacional: **21.03.2013 WO13040046**

(96) Fecha de presentación y número de la solicitud europea: **12.09.2012 E 12766259 (1)**

(97) Fecha y número de publicación de la concesión europea: **11.01.2017 EP 2756696**

(54) Título: **Sistema y procedimientos para codificar intercambios con un conjunto de datos de clave efímera compartida**

(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 201213610738

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.07.2017

(73) Titular/es:

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

(72) Inventor/es:

HAWKES, PHILIP, MICHAEL y
CHERIAN, GEORGE

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Sistema y procedimientos para codificar intercambios con un conjunto de datos de clave efímera compartida

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

La presente solicitud reivindica la prioridad de la solicitud de patente provisional estadounidense de propiedad común Nº 61/533.627 (número de expediente de Qualcomm 113346P1) presentada el 12 de septiembre de 2011, la solicitud de patente provisional estadounidense Nº 61/535.234 (número de expediente de Qualcomm 113346P2) presentada el 15 de septiembre de 2011, la solicitud de patente provisional estadounidense Nº 61/583.052 (número de expediente de Qualcomm 113346P3) presentada el 4 de enero del 2012, la solicitud de patente provisional estadounidense Nº 61/606.794 (número de expediente de Qualcomm 121585P1) presentada el 5 de marzo del 2012 y la solicitud de patente provisional estadounidense Nº 61/645.987 (número de expediente de Qualcomm 121585P2) presentada el 11 de mayo del 2012 y la solicitud de patente provisional estadounidense Nº 61/611.553 (número de expediente de Qualcomm 121602P1) presentada el 15 de marzo de 2012. Además, el contenido de la solicitud no provisional con el número de expediente de Qualcomm 113.346, titulada: COMUNICACIÓN INALÁMBRICA USANDO CONFIGURACIÓN DE RE-AUTENTIFICACIÓN Y CONEXIÓN CONCURRENTE, presentada el 11 de septiembre de 2012, y la solicitud no provisional con número de expediente de Qualcomm 121585, titulada: SISTEMAS Y PROCEDIMIENTOS PARA REALIZAR LA CONFIGURACIÓN Y AUTENTIFICACIÓN DE ENLACES, presentada el 11 de septiembre de 2012, son relevantes para la presente solicitud.

CAMPO DE LA DIVULGACIÓN

Las presentes enseñanzas se refieren a sistemas y procedimientos para la codificación de los intercambios con un conjunto de datos de clave efímera compartida.

ANTECEDENTES

En aplicaciones de redes de Wi-Fi, las características de seguridad han evolucionado gradualmente para proporcionar herramientas de seguridad más robustas y mejor integradas. En la norma del EAP (protocolo de autentificación extensible) de 802.11i, promulgada por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), se puede utilizar una técnica de autentificación que incluye un mecanismo denominado "coloquio inicial de 4 vías". En el mecanismo del coloquio inicial de 4 vías, un dispositivo de cliente, como un ordenador portátil, un teléfono inteligente u otro dispositivo de cliente, denominado "estación" en general, negocia con un encaminador inalámbrico u otro dispositivo, en general denominado "punto de acceso", para establecer una sesión de red segura. Durante la sesión, la estación puede buscar una conexión a Internet u otras redes.

En el enfoque del coloquio inicial de 4 vías, la estación y el punto de acceso intercambian una serie de cuatro mensajes definidos, en base a los cuales puede llevarse a cabo una autentificación mutua. El punto de acceso puede interactuar con un servidor del servicio de usuario telefónico de autentificación remota (RADIUS) u otro servidor de autentificación, una plataforma o un servicio para establecer una serie de secretos compartidos y/o claves públicas y privadas, que son utilizados por la estación y el punto de acceso para ejecutar el procedimiento de coloquio inicial de 4 vías. Como parte del procedimiento de coloquio inicial de 4 vías, la estación y el punto de acceso pueden tener acceso a un secreto compartido, que puede incluir una clave maestra por pares (PMK). Los mensajes intercambiados entre la estación y el punto de acceso se pueden codificar usando conjuntos adicionales de claves públicas y privadas, incluyendo una clave transitoria por pares (PTK), que puede construirse usando la clave maestra por pares como un generador para posteriores capas de claves de cifrado.

Sin embargo, en los modos de realización existentes del coloquio inicial de 4 vías, un atacante que es capaz de interceptar y decodificar con éxito la clave maestra por pares puede entonces ser capaz de utilizar esa clave de nivel superior para generar y posiblemente interceptar y decodificar el tráfico entre el punto de acceso y una o más estaciones, generando o deduciendo las respectivas claves transitorias por pares u otra información de cifrado, porque una vez que se establece una clave maestra por pares, las claves de sesión adicionales obtenidas a partir de esa clave maestra por pares siguen siendo válidas y funcionan durante tanto tiempo como siga siendo válida la clave maestra por pares original. Como resultado, un atacante con éxito que captura la clave maestra por pares puede ser capaz de descifrar los flujos entre el punto de acceso y una o más estaciones cualesquiera que se comuniquen con el punto de acceso durante la vida útil efectiva de la clave maestra por pares.

El artículo XP031072092, de FANG-CHUN KUO ET AL: "Estudios de comparación entre mecanismos de intercambio de claves pre-compartidas y públicas para seguridad de capas de transporte" divulga que la DHE_PSK, que utiliza el intercambio de claves pre-compartida y efímeras de Diffie-Hellman, puede proporcionar confidencialidad directa perfecta, PFS, para asegurarse de que se genere una clave privada DH nueva para cada coloquio inicial.

El artículo XP010158990, de KRAWCZYK H: "SKEME: un mecanismo de intercambio de claves seguro y versátil para Internet", divulga el protocolo SKEME que proporciona confidencialidad directa perfecta; se obtiene una clave de sesión para las partes mediante el intercambio de Diffie-Hellman; pueden utilizarse claves compartidas a largo

plazo (como una clave maestra instalada manualmente).

RESUMEN

La presente invención se define mediante la materia objeto de las reivindicaciones adjuntas. En la siguiente descripción, el término "modo de realización" ha de interpretarse como un ejemplo, mientras que el alcance de la protección se define solamente mediante la materia objeto de las reivindicaciones adjuntas.

Se divulgan el aparato y el procedimiento para proporcionar confidencialidad directa perfecta en las sesiones de red de Wi-Fi. La confidencialidad directa perfecta (PFS) es un enfoque de la seguridad. La PFS puede referirse a una propiedad de una obtención de clave, de tal manera que si un secreto principal es expuesto por un atacante, entonces el atacante no puede determinar claves pasadas o futuras obtenidas del secreto principal.

Cuando un dispositivo de un cliente está realizando un coloquio inicial de 4 vías con un punto de acceso (AP), se genera una clave maestra por pares (PMK) y se obtienen claves adicionales, tales como una clave transitoria por pares (PTK), a partir de la PMK. La PTK sigue siendo válida durante el tiempo en que la PMK siga siendo válida; de este modo, sin seguridad añadida (por ejemplo, la PFS), un atacante puede obtener la PTK de una PMK comprometida para decodificar las transmisiones entre el dispositivo de cliente y el AP durante un tiempo de vida efectivo de la PMK comprometida. En lugar de depender de claves obtenidas que pueden permanecer válidas durante el tiempo en que la PMK pueda seguir siendo válida, las técnicas descritas proporcionan una seguridad mejorada mediante la implementación de la PFS en el coloquio inicial de 4 vías.

Cuando el dispositivo de cliente realiza el coloquio inicial de 4 vías con el AP, el AP puede generar y transmitir un mensaje ocasional de punto de acceso (ocasional-A) al dispositivo de cliente. El dispositivo de cliente puede obtener una PMK y generar un mensaje ocasional de estación (ocasional-S). El cliente puede obtener una PTK, una clave de confirmación de clave (KCK) y una clave de cifrado de clave (KEK) en base a la PMK, la información ocasional-A, la ocasional-S y/u otra información.

Para implementar la PFS en el coloquio inicial de 4 vías, el dispositivo de cliente puede transmitir una solicitud de asociación que puede incluir una clave pública efímera de Diffie-Hellman (SDHEPubKey) de estación (STA) al AP. El AP obtiene la PMK y obtiene la PTK a partir de la PMK.

Para implementar la PFS en el coloquio inicial de 4 vías, el AP puede obtener una clave de Diffie-Hellman efímera compartida (SharedDHEKey) a partir de la SDHEPubKey y una clave privada efímera de Diffie-Hellman de punto de acceso (ADHEPrivKey), que es conocida por el punto de acceso. La SDHEPubKey y la ADHEPrivKey pueden ser pre-generados por el dispositivo de cliente y el AP antes de implicarse en el coloquio inicial de 4 vías, respectivamente. Por otra parte, el AP puede obtener una clave transitoria por pares de confidencialidad directa perfecta (PFS-PTK), una clave de confirmación de clave de confidencialidad directa perfecta (PFS-KCK) y una clave de cifrado de clave de confidencialidad directa perfecta (PFS-KEK), en base a la SharedDHEKey y la PTK. El AP puede transmitir una clave pública efímera de Diffie-Hellman de punto de acceso (ADHEPubKey) al dispositivo de cliente. El dispositivo de cliente puede obtener la SharedDHEKey en base a una clave privada efímera de Diffie-Hellman de estación (SDHEPrivKey), que es conocida por el dispositivo de cliente, y la ADHEPubKey. La ADHEPubKey y la SDHEPrivKey pueden ser pre-generadas por el AP y el dispositivo de cliente antes de implicarse en el coloquio inicial de 4 vías, respectivamente. El dispositivo de cliente puede obtener la PFS-PTK, la PFS-KCK y la PFS-KEK en base a la PTK y la SharedDHEKey.

El AP y el dispositivo de cliente pueden borrar la ADHEPrivKey y la SDHEPrivKey después de obtener la SharedDHEKey, respectivamente. El dispositivo de cliente y el AP pueden descifrar las respectivas transmisiones recibidas en base a la PFS-KEK, la PFS-KCK, la SharedDHEKey y/u otra clave obtenida de la PMK.

En un modo de realización particular, se proporciona un procedimiento de acuerdo con la reivindicación independiente 1.

En otro modo de realización particular, se proporciona un aparato de acuerdo con la reivindicación independiente 9

Una ventaja particular proporcionada por al menos uno de los modos de realización divulgados es la capacidad de un primer dispositivo (por ejemplo, una estación móvil) para implementar la PFS con un segundo dispositivo (por ejemplo, un punto de acceso) en una red de Wi-Fi.

Otros aspectos, ventajas y características de la presente divulgación se harán evidentes después de la revisión de toda la solicitud, incluyendo las siguientes secciones: Breve descripción de los dibujos, Descripción detallada y las Reivindicaciones.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los dibujos adjuntos, que están incorporados en, y que forman una parte de, esta memoria descriptiva, ilustran

modos de realización de las presentes enseñanzas y, junto con la descripción, sirven para explicar los principios de las presentes enseñanzas. En las figuras:

La FIG. 1 ilustra una red general que se puede utilizar en sistemas y procedimientos para proporcionar confidencialidad directa perfecta en sesiones de red de Wi-Fi, de acuerdo con diversos modos de realización;

la FIG. 2 ilustra el hardware, el software y otros recursos que se pueden utilizar en un punto de acceso que puede ser configurado para utilizar los sistemas y procedimientos para proporcionar confidencialidad directa perfecta en las sesiones de red de Wi-Fi, de acuerdo con diversos modos de realización;

las FIGs. 3A y 3B ilustran una secuencia ejemplar de flujo de llamadas para ejecutar la configuración y el funcionamiento de una disposición de cifrado entre un punto de acceso y una estación, de acuerdo con diversos modos de realización de las presentes enseñanzas;

la FIG. 4 ilustra otra secuencia ejemplar de flujo de llamadas para ejecutar la configuración y el funcionamiento de una disposición de cifrado entre un punto de acceso y una estación, de acuerdo con diversos modos de realización de las presentes enseñanzas; y

la FIG. 5 ilustra hardware, software y otros recursos ejemplares que se pueden utilizar en la provisión de confidencialidad directa perfecta en las sesiones de red de Wi-Fi, de acuerdo con diversos modos de realización.

DESCRIPCIÓN DETALLADA

Los modos de realización de las presentes enseñanzas se refieren a sistemas y procedimientos para proporcionar confidencialidad directa perfecta en las sesiones de red de Wi-Fi. Más en particular, los modos de realización se refieren a las plataformas y las técnicas para la introducción de mecanismos para crear o permitir la confidencialidad directa perfecta (PFS) que se aplicará a las sesiones de Wi-Fi que utilicen el coloquio inicial de 4 vías para establecer comunicaciones entre un punto de acceso y una estación. El punto de acceso y la estación pueden llevar a cabo una operación de coloquio inicial de 4 vías, utilizando una clave maestra por pares, un servidor de autentificación, una verificación de integridad del mensaje (MIC) y otros procedimientos y recursos especificados por la norma 802.11i y/u otros protocolos. En los sistemas y procedimientos para proporcionar confidencialidad directa perfecta en las sesiones de red de Wi-Fi, el punto de acceso y la estación pueden aplicar capas adicionales de protección criptográfica, incluyendo la generación de un conjunto adicional de claves ad hoc que se insertan en la estructura de coloquio inicial de 4 vías. El conjunto adicional de claves ad hoc puede incluir un conjunto de datos de claves públicas y privadas que se genera utilizando cálculos de Diffie-Hellman (DH), que pueden ser o incluir la generación de pares de claves públicas y privadas, utilizando aritmética de campo finito, elíptica y/u otra aritmética. Las claves de Diffie-Hellman y la información relacionada se pueden generar en base a, o utilizando, generadores de números aleatorizados.

Después de que las correspondientes claves compartidas de Diffie-Hellman están generadas y / o extraídas, tanto en el lado del punto de acceso como en el lado de la estación, la parte privada de esa clave compartida de Diffie-Hellman puede ser borrada o destruida, tanto por el punto de acceso como por las unidades de estación. Dado que esas claves privadas (por ejemplo, la ADHEPrivKey y la SDHEPrivKey) se han borrado o destruido, un atacante que captura los flujos de mensajes entre el punto de acceso y la estación no puede comprometer otros flujos antes o después de una sesión actual, incluso si el atacante consigue más adelante recuperar la clave maestra por pares utilizada durante la sesión actual. El atacante no puede comprometer otros flujos porque las sesiones independientes que están codificadas de acuerdo con los sistemas y procedimientos para proporcionar confidencialidad directa perfecta en las sesiones de red de Wi-Fi tendrán diferentes datos de claves de Diffie-Hellman, generadas por separado durante cada sesión, cuya decodificación requeriría la adquisición de otra información de claves privadas y públicas de Diffie-Hellman. De acuerdo con estos y otros aspectos, la seguridad de las sesiones de Wi-Fi se puede mejorar, y la confidencialidad directa perfecta (PFS) se puede incorporar en el esquema de seguridad del coloquio inicial de 4 vías.

En un modo de realización particular, un procedimiento incluye la generación de un secreto maestro compartido. El procedimiento también incluye la generación de un conjunto de datos de clave efímera compartida, para codificar los intercambios asociados a un punto de acceso y al menos una estación, donde el conjunto de datos de clave efímera compartida se basa en el contenido de un intercambio de coloquios iniciales, asociado con el punto de acceso y la al menos una estación, realizado para autentificar las comunicaciones asociadas con el punto de acceso y la al menos una estación. Se genera el conjunto de datos de clave efímera compartida, independiente del secreto principal compartido, y una duración de validez del conjunto de datos de clave efímera compartida es menor que una duración de validez del secreto maestro compartido. El procedimiento incluye además la codificación de al menos un mensaje en base, al menos, al secreto maestro compartido y al conjunto de datos de clave efímera compartida.

En otro modo de realización particular, un aparato incluye una interfaz de red inalámbrica con al menos una estación. El aparato también incluye un procesador configurado para comunicarse con la al menos una estación a través de una interfaz de red, estando el procesador configurado para generar un secreto maestro compartido y para

generar un conjunto de datos de clave efímera compartida para codificar los intercambios asociados con un sistema de punto de acceso y la al menos una estación. El conjunto de datos de clave efímera compartida se basa en el contenido de un intercambio de coloquios iniciales, asociado con el sistema del punto de acceso y al menos una estación, realizado para autentificar las comunicaciones asociadas con el sistema del punto de acceso y la al menos una estación. El conjunto de datos de clave efímera se genera de forma independiente del secreto maestro compartido, y una duración de validez del conjunto de datos de clave efímera compartida es menor que una duración de validez del secreto maestro compartido. El procesador está configurado además para codificar al menos un mensaje asociado con el sistema del punto de acceso y la al menos una estación, utilizando al menos el secreto maestro compartido y el conjunto de datos de clave efímera compartida.

Se hace referencia a los modos de realización ejemplares de las presentes enseñanzas, que se ilustran en los dibujos adjuntos. Siempre que sea posible, se utilizan los mismos números de referencia en toda la extensión de los dibujos, para referirse a las mismas partes o a partes similares.

La FIG. 1 ilustra una red global 100 en la que pueden funcionar los sistemas y procedimientos para proporcionar confidencialidad directa perfecta en las sesiones de red de Wi-Fi. Como se muestra, un punto de acceso 108 puede difundir una señal de red inalámbrica a un conjunto de estaciones 102 dentro de su alcance. El punto de acceso 108 puede incluir un encaminador inalámbrico y/u otro punto de acceso a la red y puede estar configurado para funcionar usando la norma inalámbrica Wi-Fi, especificada por la especificación 802.11b, 802.11g, 802.11n del IEEE y/u otras normas. Cuando funciona como un punto de acceso de Wi-Fi, el punto de acceso 108 puede, por ejemplo, funcionar en la banda de frecuencias de 2,4 GHz. Se apreciará sin embargo, que en otros modos de realización, se pueden utilizar otras normas, canales y/o frecuencias de acceso inalámbrico. Como se describe con más detalle a continuación, al menos uno de los conjuntos de estaciones 102 puede participar en un intercambio de datos 114 que implementa la confidencialidad directa perfecta (PFS) con el punto de acceso 108 mediante una red de Wi-Fi.

Cada dispositivo o estación en el conjunto de estaciones 102 puede incluir cualquier dispositivo habilitado para red inalámbrica, tal como un teléfono inteligente equipado con Wi-Fi, un dispositivo de panel táctil y/u otro dispositivo o plataforma. Como se muestra en la FIG. 2, una estación individual 118 en el conjunto de estaciones 102 puede estar configurada con uno o más recursos de hardware, software y/u otros. Una estación 118 puede comprender una variedad de hardware, software y otros recursos, incluyendo un sistema operativo 112, una pantalla 110 que puede, por ejemplo, mostrar una interfaz gráfica de usuario (GUI) del sistema operativo 112, y una antena de radiofrecuencia 150 (o múltiples antenas). El sistema operativo 112 puede comprender un sistema operativo de dispositivos móviles, tal como el sistema operativo Android™ disponible en Google Inc., Mountain View, California, Estados Unidos, u otros. El sistema operativo 112, como se ha señalado, puede comprender una interfaz gráfica de usuario (GUI), así como la gestión de ficheros, la gestión de energía, las comunicaciones y/u otra lógica, servicios y/o recursos para hacer funcionar la estación 118. El sistema operativo 112 puede incluir instrucciones de ordenador 116. Las instrucciones de ordenador 116 pueden hacer que un procesador implemente la PFS para el intercambio de datos mediante una red de Wi-Fi. La estación 118 puede alojar aplicaciones, servicios, lógica y/u otra lógica, otros servicios y/u otros módulos, que se pueden utilizar para establecer conexiones con los puntos de acceso y/u otros canales. Una cualquiera, o más, del conjunto de estaciones 102 pueden conectarse al punto de acceso 108 a la vez. Como se muestra en la FIG. 2, el punto de acceso 108 puede emitir información de baliza 104 para el conjunto de estaciones 102. La información de baliza 104 puede incluir un elemento de información (IE) de identificación del conjunto de servicios (SSID), que indica el nombre, tipo de conexión, canales disponibles y otra información y servicios de red proporcionados por el punto de acceso 108 a cualquier estación dentro de su rango de conexión inalámbrica. La FIG. 3 ilustra una secuencia de llamada que se puede utilizar para establecer una conexión de acuerdo con la norma de Wi-Fi, con mejoras, características, ampliaciones y/o ventajas de acuerdo con los sistemas y procedimientos para proporcionar confidencialidad directa perfecta en las sesiones de red de Wi-Fi, incluyendo el suministro de confidencialidad directa perfecta (PFS) en sesiones de redes individuales. En términos generales, la secuencia de flujos de llamadas puede llevarse a cabo entre dos o más plataformas, sistemas, nodos, dispositivos y/u otro hardware, incluyendo, como se ilustra, la estación 120, el primer punto de acceso 122, el segundo punto de acceso 124, un servidor de autentificación 126 y un servidor del protocolo de configuración dinámica de anfitriones (DHCP) 128. Si bien se ilustran esas plataformas, sistemas, nodos, dispositivos y/o hardware individuales, se apreciará que, en otros modos de realización, pueden utilizarse plataformas de hardware, sistemas, nodos, dispositivos y/o hardware alternativos o adicionales. Como se muestra en 0002, una estación 120 puede acercarse y entrar al alcance inalámbrico de un primer punto de acceso 122 (etiquetado como API), tal como, por ejemplo, un encaminador inalámbrico de Wi-Fi y/u otro dispositivo, plataforma o sede de acceso. En 1002, la estación 120 puede desplazarse fuera de alcance del primer punto de acceso 122 y hacia el alcance inalámbrico del segundo punto de acceso 124 (etiquetado como AP2). El segundo punto de acceso 124 puede incluir asimismo un encaminador inalámbrico de Wi-Fi y/u otro dispositivo o sede de acceso. En 2002, el segundo punto de acceso 124 puede generar un mensaje ocasional de punto de acceso (ocasional-A), que puede incluir un mensaje de una sola vez, una secuencia, datos y/o un código para anunciar la presencia del segundo punto de acceso 124, y puede ser utilizado en la generación de códigos de clave. El mensaje ocasional de punto de acceso (ocasional-A) puede incluir un número y/u otros datos generados aleatoriamente o pseudo-aleatoriamente. El mensaje ocasional de punto de acceso (ocasional-A) se puede insertar en el mensaje de baliza difundido por el segundo punto de acceso 124.

En 3002, la estación 120 puede obtener una clave maestra por pares (PMK), a utilizar para establecer una

comunicación segura con el segundo punto de acceso 124. Para obtener la PMK, la estación 120 puede generar información que incluye, por ejemplo, un mensaje de SEQ o datos, un mensaje de rMSK o datos y un mensaje ocasional de estación (ocasional-S) o datos. Si se utiliza una clave maestra por pares pre-establecida, la estación 120 puede recuperar esa clave maestra por pares. En 3004, el segundo punto de acceso 124 puede obtener información adicional que incluye, por ejemplo, una clave transitoria por pares (PTK), una clave de confirmación de clave (KCK) del protocolo de autentificación exhaustiva por LAN (EAPOL) y una clave de cifrado de clave (KEK) del EAPOL, utilizando la clave maestra por pares, un mensaje ocasional de punto de acceso (ocasional-A), un mensaje ocasional de estación (ocasional-S) y/u otra información.

En 4002, la estación 120 puede generar una solicitud de asociación (Sol. Asoc.) y transmitir esa solicitud al segundo punto de acceso 124. En relación con la solicitud, la estación 120 puede realizar cálculos para generar claves y datos relacionados adicionales, incluyendo una clave privada efímera de Diffie-Hellman (SDHEPrivKey) y una clave pública efímera de Diffie-Hellman (SDHEPubKey). La clave privada efímera de Diffie-Hellman de estación (SDHEPrivKey) y la clave pública efímera de Diffie-Hellman de estación (SDHEPubKey) pueden generarse usando enfoques criptográficos de Diffie-Hellman, que pueden incluir aritmética elíptica u otra aritmética.

Se puede observar que una de las estaciones 120, o ambas, y el segundo punto de acceso 124 pueden acceder, almacenar y/o pre-calcular los mismos datos de Diffie-Hellman y recuperar esos datos cuando sea necesario, lo cual puede reducir la carga de cálculo durante la ejecución del protocolo modificado de coloquio inicial de 4 vías. La clave pública efímera de Diffie-Hellman de estación (SDHEPubKey) se puede incorporar en los parámetros o campos de la solicitud de asociación (Sol. Asoc.) y puede enviarse al segundo punto de acceso 124. En 4004, el segundo punto de acceso 124 puede recibir la solicitud de asociación (Sol. Asoc.), pero puede desechar esa solicitud si el mensaje ocasional de punto de acceso (ocasional-A) no es actual, válido o nuevo.

En 5002, el segundo punto de acceso 124 puede transmitir una solicitud de AAA del EAP al servidor de autentificación 126. Como se ilustra, la solicitud de AAA del EAP puede incluir un determinado número de parámetros o campos, algunos de los cuales, o todos, pueden ser utilizados para autentificar la estación 120 y/o los datos o credenciales asociados con la estación 120. En 6002, el servidor de autentificación 126 puede verificar la etiqueta de autentificación (Etiqueta Aut.) y obtener la clave rMSK o datos. En 7002, el servidor de autentificación 126 puede transmitir una respuesta de AAA del EAP al segundo punto de acceso 124, respuesta que puede incluir una serie de parámetros o campos, como se ilustra. En 8002, el segundo punto de acceso 124 puede asignar la clave maestra por pares para igualar la rMSK devuelta en la respuesta de AAA del EAP. En otros modos de realización que utilizan una clave maestra por pares almacenada, el segundo punto de acceso 124, en cambio, puede recuperar la clave maestra por pares del almacenamiento.

En 9002, el segundo punto de acceso 124 puede obtener una clave transitoria por pares (PTK) a partir de la clave maestra por pares, el mensaje ocasional de estación (ocasional-S) y el mensaje ocasional de punto de acceso (ocasional-A). En 10002, el segundo punto de acceso 124 puede verificar el mensaje DHCP-Descubrir con Compromiso Rápido y el mensaje de EAPOL-Clave_F, utilizando datos de KCK y KEK y/u otra información. En 11002, el segundo punto de acceso 124 puede transmitir un mensaje DHCP-Descubrir con Compromiso Rápido () al servidor de DHCP 128. En 12002, el segundo punto de acceso 124 puede obtener una clave efímera de Diffie-Hellman compartida (SharedDHEKey) o ad hoc, a partir de la ADHEPivKey y la SDHEPubKey, y/u otra información o datos. En 12004, el segundo punto de acceso 124 puede obtener la clave por pares transitoria de confidencialidad directa perfecta (PFS-PTK), así como otra información o datos que incluyen una clave de confirmación de clave de confidencialidad directa perfecta (PFS-KCK) y una clave de cifrado de clave de confidencialidad directa perfecta del EAPOL (PFS-KEK), usando la clave transitoria por pares, la clave efímera de Diffie-Hellman compartida (SharedDHEKey) y/u otra información.

En 13002, el segundo punto de acceso 124 puede generar una clave temporal de grupo (GTK) y una clave temporal de grupo de integridad (IGTK), según sea necesario. Cabe señalar que, después de generar la clave efímera de Diffie-Hellman compartida (SharedDHEKey) y/o en otros momentos, la estación 120 y el segundo punto de acceso 124 pueden, respectivamente, eliminar, desechar, sobrescribir y/o borrar o destruir de otra manera sus respectivas claves privadas efímeras de Diffie-Hellman (es decir, las correspondientes SDHEPrivKey y ADHEPrivKey). Eliminando, sobrescribiendo y/o borrando o destruyendo de otra manera las claves privadas efímeras de Diffie-Hellman que pertenecen a la estación 120 y al segundo punto de acceso 124, la estación 120 y el segundo punto de acceso 120 pueden asegurar que ningún atacante puede comprometer el tráfico de mensajes almacenados. Este es el caso incluso si el atacante obtiene la posesión de la clave maestra por pares y la clave transitoria por pares inalterada, ya que la clave efímera de Diffie-Hellman compartida (SharedDHEKey) seguiría siendo necesaria para descifrar ese tráfico, pero la clave efímera de Diffie-Hellman compartida (SharedDHEKey) es irrecuperable una vez que se borran las respectivas claves de Diffie-Hellman privadas (SDHEPrivKey y ADHEPrivKey). En 14002, el servidor del DHCP 128 puede generar un mensaje DHCP-Ack con Compromiso Rápido (dir. de IP) y transmitir ese mensaje al segundo punto de acceso 124. Ese mensaje puede incluir una dirección de IP asignada a la estación 120. Cabe señalar que, si bien 11.002 a 14.002 se ilustran como teniendo lugar en un cierto orden, esas etapas de procesamiento, mensajes, lógica de decisión y/u otras acciones, así como otros mostrados en las FIGs. 3A y 3B y en otras partes, pueden tener lugar en varias otras secuencias u órdenes, en función de la configuración de la estación 120 y del segundo punto de acceso 124 y/u otros factores.

En 15002, el segundo punto de acceso 124 puede formar una respuesta de asociación (Resp. Asoc.) con varios campos o componentes. Los diversos campos o componentes pueden incluir un mensaje relacionado con la autentificación del EAP, es decir, un mensaje de EAP-Fin o datos recibidos desde el servidor de autentificación en 7002. El mensaje de EAP-Fin o los datos pueden ser un mensaje de EAP-Fin Re-Aut o datos. La respuesta de asociación también puede incluir un mensaje relacionado con el DHCP con varias opciones que, como se ilustra, puede consistir en un mensaje DHCP-Ack con Compromiso Rápido o datos y/u otros mensajes o datos recibidos desde el servidor del DHCP en 14002. El AP2 puede aplicar el cifrado y/o protección de la integridad a estos mensajes o datos. El cifrado puede utilizar la KEK o la PFS-KEK, u otra clave obtenida de la PMK y la PTK y la SharedDHEKey. La protección de integridad puede utilizar la KCK o la PFS-KCK u otra clave obtenida de la PMK y/o la PTK y/o la SharedDHEKey. La respuesta de asociación puede incluir, además, un mensaje relacionado con un mensaje de clave de EAPOL que, como se ilustra, puede incluir opciones para el cifrado, la autentificación y/o la comprobación de la integridad utilizando la clave transitoria por pares de confidencialidad directa perfecta (PFS-PTK) y/u otras claves o datos. Este mensaje relacionado con la clave de EAPOL puede incluir la ADHEPubKey. Este mensaje relacionado con la clave de EAPOL puede incluir una comprobación de la integridad del mensaje (MIC), calculada sobre el mensaje o datos relacionados con la clave de EAPOL, utilizando la KCK. El AP2 122 puede calcular una comprobación de integridad de mensajes de confidencialidad directa perfecta (PFS-MIC) utilizando la PFS KCK y/u otros datos, mensajes o información. La PFS-MIC puede proporcionar protección de la integridad de la totalidad o de una parte de la combinación de la Sol. Asoc. 4002 y la Resp. Asoc. 15002. La parte protegida por integridad puede corresponder al mensaje o a los datos relacionados con la clave de EAPOL en la Resp. Asoc. 15002. La PFS-MIC puede transmitirse internamente a los mensajes o datos relacionados con la clave de EAPOL, EAP-Fin Re-Aut o DHCP. La PFS-MIC puede ser parte de la Resp. Asoc., pero fuera de los mensajes o datos relacionados con la clave de EAPOL, EAP-Fin Re-Aut o DHCP.

En 16002, la estación 120 puede verificar el mensaje EAP-Fin Re-Aut usando la rIK y/u otra información. En 17002, la estación 120 puede verificar la comprobación de integridad de mensajes (MIC) de clave de EAPOL utilizando la KCK. En 18002, la estación 120 puede generar una clave efímera de Diffie-Hellman compartida (SharedDHEKey) a partir de la SDHEPrivKey y la ADHEPubKey situadas en el mensaje de clave de EAPOL, como se genera o presenta en 15002, y/u otros datos o información. En 18004, la estación 120 puede obtener la PFS-PTK, la PFS-KCK y la información de la PFS-KEK usando la clave transitoria por pares y la clave efímera de Diffie-Hellman compartida (SharedDHEKey) y/u otros datos o información. En 18006, la estación 120 puede verificar la PFS-MIC utilizando la PFS-KCK y/u otros datos, mensajes o información.

En 19002, la estación 120 puede verificar y/o descifrar el mensaje de confirmación de DHCP. El descifrado puede utilizar la KEK o la PFS-KEK u otra clave obtenida de la PMK y/o la PTK y/o la SharedDHEKey. La verificación puede utilizar la KCK o la PFS-KCK u otra clave obtenida de la PMK y/o la PTK y/o la SharedDHEKey. En 20002, la estación 120 puede transmitir un mensaje de confirmación de autorización (Confirm-Aut) al segundo punto de acceso 124, incluyendo un conjunto de parámetros o campos, como se ilustra. El mensaje Confirm-Aut puede incluir un mensaje o datos relacionados con un mensaje de clave de EAPOL. Este mensaje o datos relacionados con una clave de EAPOL pueden incluir una comprobación de la integridad del mensaje (MIC), calculada sobre el mensaje o los datos relacionados con la clave de EAPOL, utilizando la KCK. Cuando se utiliza la confidencialidad directa perfecta (PFS) de acuerdo con las presentes enseñanzas, la verificación de la integridad del mensaje de confidencialidad directa perfecta (PFS-MIC) se puede incorporar en el mensaje de autorización (Confirm-Aut). La PFS-MIC se puede calcular utilizando la PFS KCK y/u otros datos, mensajes o información. La PFS-MIC puede proporcionar protección de integridad de la totalidad o una parte de la combinación de la Sol. Asoc. 4002 y la Resp. Asoc. 15002 y la Confirm-Aut 20002. La parte con integridad protegida puede corresponder al mensaje o los datos relacionados con la clave de EAPOL en la Confirm-Aut 20002. La PFS-MIC puede ser interna a los mensajes o datos relacionados con la clave de EAPOL, EAP-Fin Re-Aut o DHCP. La PFS-MIC puede ser parte de la Confirm-Aut, pero fuera de los mensajes o datos relacionados con la clave de EAPOL, EAP-Fin Re-Aut o DHCP.

En 21002, la estación 120 puede instalar claves o datos que incluyen la PFS-TK, la GTK y la IGTK. En 21004, la estación 120 puede instalar la dirección de IP (protocolo de Internet) generada por el protocolo de configuración dinámica de anfitriones (DHCP) 128 mediante el proceso de autentificación.

En 22002, el segundo punto de acceso 124 puede verificar la comprobación de integridad de mensaje (MIC) usando la clave de confirmación de clave (KCK). En 2302, el segundo punto de acceso 124 puede verificar la PFS-MIC utilizando los datos de la PFS-KCK y/u otros datos, mensajes o información. En 2402, el segundo punto de acceso 124 puede instalar claves o datos que incluyen la PFS-TK, la GTK y la IGTK. En 24004, el segundo punto de acceso 124 puede instalar la dirección de IP (Protocolo de Internet) para la estación 120. Después de 24004, la estación 120 puede acceder a Internet y/u otras redes públicas o privadas a través del segundo punto de acceso 124, utilizando la dirección de IP (protocolo de Internet) asignada. Puede observarse que mientras que el cifrado y el procesamiento relacionado mostrado en las FIGs. 3A y 3B ilustran los intercambios entre la estación 120 y el segundo punto de acceso 124 hacia el cual se está desplazando la estación 120, el mismo procesamiento, o uno similar, puede aplicarse entre la estación 120 y el primer punto de acceso 122, la estación 120 y un tercer punto de acceso (no mostrado) y/u otras configuraciones de red.

Puede igualmente observarse que después de la finalización del proceso de autentificación mejorada ilustrado en la FIG. 2, la sesión llevada a cabo entre la estación 120 y el segundo punto de acceso 124 está protegida por la clave maestra por pares (PMK), la clave transitoria por pares (PTK) y/u otras características de seguridad del protocolo de autentificación extensible (EAP), incluyendo el coloquio inicial de 4 vías. Sin embargo, de acuerdo con los aspectos de las presentes enseñanzas, la adición de características relacionadas con la confidencialidad directa perfecta (PFS) y el uso de conjuntos de claves públicas / privadas en base a los generadores de Diffie-Hellman permiten una mayor seguridad en comparación con un protocolo de coloquio inicial de 4 vías "raso". De acuerdo con los aspectos de las presentes enseñanzas, un atacante que captura y almacena los flujos de mensajes entre la estación 120 y el segundo punto de acceso 120 (o cualquier punto de acceso comparable), incluyendo la clave maestra por pares (PMK) y la clave transitoria por pares (PTK), aún no puede violar la integridad de esos flujos, ya que la re-creación de la clave efímera de Diffie-Hellman compartida (SharedDHEKey), necesaria para completar la violación, no es posible sin las claves efímeras de Diffie-Hellman privadas que pertenecen a la estación (SDHEPrivKey) y/o al punto de acceso (ADHEPrivKey), que han sido descartadas en un tiempo relativamente corto después de establecer la sesión.

El procesamiento de seguridad de acuerdo con los sistemas y procedimientos para proporcionar confidencialidad directa perfecta en las sesiones de red de Wi-Fi puede ser implementado en diversos entornos de red, incluyendo, por ejemplo, un entorno de red de Wi-Fi en el que se incorpora la capacidad de Configuración Rápida de Enlace Inicial (FILS). La Configuración Rápida de Enlace Inicial (FILS) comprende un conjunto de protocolos de comunicación emitidos por la norma 802.11ai del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), que está concebida para abordar escenarios donde el enfoque y el registro de una estación para un punto de acceso tiene lugar de manera transitoria, tal como un teléfono inteligente o un ordenador portátil inalámbrico atravesando un aeropuerto público, una terminal de autobuses y/u otro entorno, donde la velocidad con la que se pueden establecer conexiones inalámbricas es un bien escaso. Se apreciará, sin embargo, que las plataformas y las técnicas de acuerdo con las presentes enseñanzas pueden integrarse en otras configuraciones de red, ya sea utilizando el protocolo de Configuración Rápida de Enlace Inicial (FILS), o no.

De acuerdo con los aspectos de las presentes enseñanzas en otras cuestiones, la estación 120 y el segundo punto de acceso 124 (u otro punto de acceso o nodo) pueden, cada uno, almacenar la clave efímera de Diffie-Hellman compartida (SharedDHEKey) generada durante una sesión, para volver a utilizarse durante una segunda sesión posterior, entre los mismos dos dispositivos. Cuando la clave efímera de Diffie-Hellman compartida (SharedDHEKey) se recupera en lugar de generarse, se puede ahorrar una cantidad significativa de cálculo en ambos extremos. De acuerdo con tales modos de realización, cada uno entre la estación 120 y el segundo punto de acceso 124 (u otro punto de acceso o nodo) puede, por ejemplo, asociar un identificador con la clave efímera de Diffie-Hellman compartida (SharedDHEKey), por ejemplo, mediante la generación de una salida de función de troceo, en base a una de sus respectivas claves efímeras de Diffie-Hellman públicas (SDHEPubKey y ADHEPubKey), o ambas, o de otra manera. En modos de realización adicionales, la estación 120 y el punto de acceso 124 no necesitan crear un identificador explícito para la clave efímera de Diffie-Hellman compartida (SharedDHEKey), pero, en cambio, se pueden configurar para asociar y recuperar esa clave automáticamente cuando se encuentra o identifica la misma estación o punto de acceso que en una sesión anterior.

La FIG. 4 ilustra una secuencia de flujo de llamadas en particular para ejecutar una configuración y el funcionamiento de la disposición de cifrado de las FIGs. 3A y 3B con un mensaje ocasional-A retrasado, y se designa en general con 400.

Por ejemplo, en lugar de transmitir el mensaje ocasional-A desde el segundo punto de acceso 124 mediante el mensaje de baliza a la estación 120, como en la FIG. 3A, el segundo punto de acceso 124 puede transmitir el mensaje ocasional-A en un mensaje diferente. En un modo de realización particular, el segundo punto de acceso 124 transmite el mensaje ocasional-A después de la generación de la PTK en el segundo punto de acceso 124. Para ilustrar esto, antes de transmitir el mensaje ocasional-A a la estación 120, el segundo punto de acceso 124 puede recibir un mensaje de autorización desde la estación 120, en 402. El mensaje de autorización puede incluir el mensaje ocasional-S, la SDHEPubKey y el mensaje de EAP-Re-aut-iniciar. El segundo punto de acceso 124 puede generar la SharedDHEKey y obtener la PTK a partir de la rMSK, el mensaje ocasional-S y el mensaje ocasional-A, en 404. Además, la segunda estación 124 también puede generar la GTK y la IGTK, en 404.

El segundo punto de acceso 124 puede transmitir el mensaje ocasional-A a la estación 120 en un mensaje de respuesta de autorización, en 406. El mensaje de respuesta de autorización puede incluir el mensaje ocasional-A, el elemento de información EAP-Fin Re-aut y la ADHEPubKey. La estación 120 puede generar la SharedDHEKey y la PTK después de recibir el mensaje de respuesta de autorización, en 408. La estación 120 puede transmitir una solicitud de asociación al segundo punto de acceso 124, en 410. La solicitud de asociación puede incluir el mensaje DHCP-Descubrir con Compromiso Rápido y una confirmación de clave. El segundo punto de acceso 124 puede transmitir una respuesta de asociación a la estación 120, en 412. La respuesta de asociación puede incluir el mensaje DHCP-Ack con Compromiso Rápido (dir-IP), la GTK y la IGTK.

La FIG. 5 ilustra una variedad de hardware, software y otros recursos que se pueden utilizar en los modos de realización para proporcionar confidencialidad directa perfecta en sesiones de red de Wi-Fi, de acuerdo con los

modos de realización. En los modos de realización mostrados, el punto de acceso 108 puede comprender características de un procesador 142 que se comunica con la memoria 144, tal como una memoria electrónica de acceso aleatorio, así como con una interfaz de red, tal como una Ethernet y/u otra conexión cableada o inalámbrica a Internet y/u otras redes. El procesador 140 puede ser programado o configurado para llevar a cabo operaciones de codificación de conjuntos de caracteres, operaciones de conectividad de red y otras operaciones de acuerdo con las presentes enseñanzas. El procesador 140 también puede comunicarse con un almacén de datos local 146, tal como un disco duro local y/u otros medios de almacenamiento, así como con una interfaz inalámbrica 148, tal como un conjunto de chips compatible con Wi-Fi, incluyendo el (los) conjunto(s) de chips de radiofrecuencia y el hardware y software asociados, que pueden estar conectados a una antena de frecuencia de radio 152 (o múltiples antenas). La memoria 144 puede incluir las instrucciones 154. Las instrucciones 154 pueden hacer que un procesador (por ejemplo, el procesador 140) implemente la PFS para un intercambio de datos a través de una red de Wi-Fi.

Conjuntamente con los modos de realización descritos, un aparato puede incluir medios para la comunicación con al menos una estación mediante una interfaz de red inalámbrica. Por ejemplo, los medios para comunicar pueden incluir uno o más componentes (por ejemplo, un transmisor, un receptor, una antena) de la estación 102 de la FIG. 1, uno o más componentes (por ejemplo, un transmisor, un receptor, una antena) del punto de acceso 108 de la FIG. 1, la antena de frecuencia de radio 150 de la FIG. 2, uno o más componentes (por ejemplo, un transmisor, un receptor, una antena) de la estación 120 de las FIGs. 3A, 3B y 4, uno o más componentes (por ejemplo, un transmisor, un receptor, una antena) del primer punto de acceso 120 de las FIGs. 3A, 3B y 4, uno o más componentes (por ejemplo, un transmisor, un receptor, una antena) del segundo punto de acceso 124 de las FIGs. 3A, 3B y 4, la interfaz inalámbrica 148 de la FIG. 5, la antena de frecuencia de radio 152 de la FIG. 5, uno o más otros dispositivos configurados para comunicar datos de forma inalámbrica, o cualquier combinación de los mismos. El aparato puede incluir también medios para el procesamiento, estando los medios de procesamiento configurados para generar un secreto maestro compartido y generar un conjunto de datos de clave efímera compartida. El conjunto de datos de clave efímera compartida se genera independiente de la clave maestra compartida. Una duración de validez del conjunto de datos de clave efímera compartida es inferior a una duración de validez del secreto maestro compartido. Los medios para el procesamiento también están configurados para cifrar al menos un mensaje que se va a transmitir a la al menos una estación, en base al menos al secreto maestro compartido y al conjunto de datos de clave efímera compartida. Por ejemplo, los medios para el procesamiento pueden incluir uno o más componentes (por ejemplo, un procesador) de la estación 102 de la FIG. 1, uno o más componentes (por ejemplo, un procesador) del punto de acceso 108 de la FIG. 1, el sistema operativo 112 y las instrucciones 116 de la FIG. 2, uno o más componentes (por ejemplo, un procesador) de la estación 120 de las FIGs. 3A, 3B y 4, uno o más componentes (por ejemplo, un procesador) del primer punto de acceso 120 de las FIGs. 3A, 3B y 4, uno o más componentes (por ejemplo, un procesador) del segundo punto de acceso 124 de las FIGs. 3A, 3B y 4, el procesador 142 y las instrucciones 154 de la FIG. 5, uno o más otros dispositivos configurados para procesar los datos, o cualquier combinación de los mismos.

La descripción anterior es ilustrativa, y las variaciones en la configuración e implementación se les pueden ocurrir a los expertos en la técnica. Por ejemplo, aunque se han descrito e ilustrado modos de realización en los que la estación 120 se acerca al segundo punto de acceso 124 para el registro y la aplicación de la confidencialidad directa perfecta (PFS), en otros modos de realización, es posible tener múltiples estaciones conectadas a un punto de acceso, por ejemplo, utilizando una clave maestra de grupo, una clave efímera de Diffie-Heilman compartida (DHESharedKey) de grupo y/u otras claves o datos. De forma alternativa, en otros modos de realización, cada estación que se acerca a, y se registra en, un punto de acceso puede intercambiar claves individuales ad hoc, o efímeras de Diffie-Hellman compartidas (DHESharedKeys), con la estación, de forma individual.

Aunque se han descrito e ilustrado modos de realización en los que se puede emplear la confidencialidad directa perfecta (PFS) en escenarios de redes que también emplean la norma de configuración rápida de enlace inicial (FILS) según la norma IEEE 802.11ai, la confidencialidad directa perfecta (PFS) de acuerdo con las presentes enseñanzas puede aplicarse en entornos que no incorporan la configuración rápida de enlace inicial (FILS). De manera similar, aunque se han descrito modos de realización en los que un servidor de autentificación 126 funciona para dar soporte al suministro de claves y al establecimiento de flujos de mensajes cifrados, en otros modos de realización, pueden utilizarse múltiples servidores y/o servicios de autentificación. Otros recursos, descritos como singulares o integrados, en otros modos de realización pueden ser plurales o distribuidos, y los recursos descritos como múltiples o distribuidos, en otros modos de realización pueden ser combinados. Además, aunque los modos de realización se han descrito como que operan en redes de Wi-Fi que están configuradas en una disposición de punto de acceso / estación, en otros modos de realización, se pueden aplicar las enseñanzas para incorporar la confidencialidad directa perfecta (PFS) y otras características también a configuraciones de punto a punto, u otras, de redes de Wi-Fi. Aún más: aunque se han descrito modos de realización que utilizan las normas de red inalámbrica de Wi-Fi, el suministro de confidencialidad directa perfecta (PFS) de acuerdo con las presentes enseñanzas también se puede aplicar a redes distintas a las redes de Wi-Fi.

Uno o más de los modos de realización divulgados pueden ser implementados 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 tableta, un ordenador portátil o un ordenador de sobremesa. Además, el sistema o el aparato puede incluir un decodificador, 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 por satélite, 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 discos de vídeo digital (DVD), un reproductor de vídeo digital portátil, cualquier otro dispositivo que almacene o recupere datos o instrucciones de ordenador, o una combinación de los mismos. Como otro ejemplo ilustrativo, no limitativo, el sistema o el aparato puede incluir unidades remotas, tales como teléfonos móviles, unidades de sistemas de comunicaciones personales de mano (PCS), unidades de datos portátiles tales como asistentes de datos personales, dispositivos habilitados para el sistema de localización global (GPS), dispositivos de navegación, unidades de datos de ubicación fija, tales como equipos de lectura de contadores, 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 a 5 puede ilustrar los 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 de manera adecuada en cualquier dispositivo que incluya unos circuitos integrados que incluyan memoria, un procesador y circuitos en un chip.

Debería entenderse que cualquier referencia a un elemento en el presente documento utilizando una designación tal como "primero," "segundo," etc., no limita, por lo general, la cantidad o el orden de esos elementos. En cambio, estas designaciones pueden usarse en el presente documento como un procedimiento conveniente para distinguir entre dos o más elementos o instancias de un elemento. Por lo tanto, una referencia a elementos primero y segundo no significa que solo puedan usarse dos elementos o que el primer elemento deba preceder al segundo elemento de alguna forma. Además, a menos que se indique lo contrario, un conjunto de elementos puede comprender uno o más elementos. Además, la expresión de la forma "al menos uno de: A, B o C", usada en la descripción o en las reivindicaciones, significa "A o B o C o cualquier combinación de estos elementos".

Tal y como se usa en el presente documento, el término "determinar" engloba 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. "Determinar" también puede incluir recibir (por ejemplo, recibir información), acceder (por ejemplo, acceder a datos en una memoria) y similares. "Determinar" también puede incluir resolver, seleccionar, elegir, establecer y similares. Además, un "ancho de canal", como se usa en el presente documento, puede incluir o puede mencionarse también como un ancho de banda en determinados aspectos.

Tal y 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 elementos individuales. Como un ejemplo, "al menos uno de: a, b o c" pretende abarcar: a, b, c, a-b, a-c, b-c y a-b-c.

Los diversos componentes, bloques, configuraciones, módulos, circuitos y etapas ilustrativos se han descrito anteriormente, en general, en lo que respecta a su funcionalidad. Si tal funcionalidad se implementa como hardware o instrucciones ejecutables por procesador, depende de la aplicación particular y de las limitaciones de diseño impuestas sobre todo el sistema. Además, las diversas operaciones de los procedimientos descritos anteriormente pueden ser llevadas a cabo por cualquier medio adecuado capaz de realizar las operaciones, tales como diversos componentes, circuitos y/o módulos de hardware y/o software. En general, cualquier operación ilustrada en las FIGs. 1 a 5 puede ser llevada a cabo mediante medios funcionales correspondientes, capaces de llevar a cabo las operaciones. Los expertos en la técnica pueden implementar la funcionalidad descrita de diferentes maneras para cada aplicación particular, pero no debería interpretarse que tales decisiones de implementación suponen un alejamiento del alcance de la presente divulgación.

Los expertos en la técnica apreciarán además que los diversos bloques lógicos, configuraciones, módulos, circuitos y etapas de algoritmo 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 para la aplicación (ASIC), una formación de compuertas programables sobre el terreno (FPGA) u otro dispositivo de lógica programable (PLD), lógica de transistor o compuertas discretas, componentes de hardware discretos (por ejemplo, hardware electrónico), software de ordenador ejecutado por un procesador o cualquier combinación de los mismos diseñada para llevar a cabo las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador pero, como alternativa, el procesador puede ser cualquier procesador, controlador, micro-controlador o máquina de estados disponibles comercialmente. 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.

En uno o más aspectos, las funciones descritas pueden implementarse en hardware, software, firmware o cualquier combinación de los mismos. Si se implementan en software, las funciones pueden almacenarse como una o más instrucciones o código en un medio legible por ordenador. Los medios legibles por ordenador incluyen medios de almacenamiento legibles por ordenador y medios de comunicación, incluyendo cualquier medio que facilite la transferencia de un programa informático desde un lugar a otro. Un medio de almacenamiento puede ser cualquier medio disponible al que pueda accederse mediante un ordenador. A modo de ejemplo, y no de manera limitativa,

tales 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 eléctricamente borrable (EEPROM), uno o más registros, un disco duro, un disco extraíble, un disco compacto de memoria de solo lectura (CD-ROM), otro almacenamiento de disco óptico, almacenamiento de disco magnético, dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que pueda accederse mediante un ordenador. Como alternativa, el medio legible por ordenador (por ejemplo, medio de almacenamiento) puede estar integrado 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 un terminal de usuario. Como alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un dispositivo informático o terminal de usuario.

Además, cualquier conexión puede denominarse debidamente un medio legible por ordenador. Por ejemplo, si el software se transmite desde una sede de la Red, 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, se incluyen en la definición de medio. Los discos, tal y como se usan en el presente documento, incluyen el disco compacto (CD), el disco de láser, el disco óptico, el disco versátil digital (DVD), el disco flexible y el disco Blu-ray®, donde algunos discos normalmente reproducen los datos de manera magnética, mientras que otros discos reproducen los datos de manera óptica con láser. Por lo tanto, en algunos aspectos, el medio legible por ordenador puede comprender un medio legible por ordenador no transitorio (por ejemplo, medios tangibles). Además, en algunos aspectos, el medio legible por ordenador puede comprender un medio legible por ordenador transitorio (por ejemplo, una señal). Las combinaciones de lo anterior también deberían incluirse dentro del alcance de los medios legibles por ordenador.

Los procedimientos divulgados en el presente documento incluyen una o más etapas o acciones para realizar el procedimiento descrito. Las etapas y/o las acciones del procedimiento pueden intercambiarse entre sí sin apartarse del alcance de las reivindicaciones. En otras palabras, a no ser que se especifique un orden específico de etapas o acciones, el orden y/o el uso de etapas y/o acciones específicas pueden modificarse sin apartarse del alcance de las reivindicaciones.

Por lo tanto, determinados aspectos pueden incluir un producto de programa informático para realizar las operaciones presentadas en el presente documento. Por ejemplo, un producto de programa informático de ese tipo puede incluir un medio de almacenamiento legible por ordenador que tenga 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. En determinados aspectos, el producto de programa informático puede incluir material de embalaje.

El software o las instrucciones también pueden transmitirse a través de un medio de transmisión. Por ejemplo, si el software se transmite desde una sede de la Red, un servidor u otro origen remoto, 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 se incluyen en la definición de medio de transmisión.

Además, debería apreciarse que los módulos y/u otros medios adecuados para llevar a cabo los procedimientos y las técnicas descritos en el presente documento pueden ser descargados y/u obtenidos de otro modo por un terminal de usuario y/o una estación base, según corresponda. Como alternativa, pueden proporcionarse diversos procedimientos descritos en el presente documento mediante medios de almacenamiento (por ejemplo, RAM, ROM, un medio de almacenamiento físico tal como un disco compacto (CD) o un disco flexible, etc.). Además, puede utilizarse cualquier otra técnica adecuada para proporcionar los procedimientos y técnicas descritos en el presente documento a un dispositivo.

Debe entenderse que las reivindicaciones no están limitadas a la configuración y componentes precisos ilustrados anteriormente. Se proporciona la anterior descripción de los modos de realización divulgados para permitir que cualquier experto en la técnica realice o use los modos de realización divulgados. Aunque lo anterior está enfocado a los aspectos de la presente divulgación, pueden concebirse aspectos diferentes y adicionales de la divulgación sin apartarse del alcance básico de la misma, y el alcance está determinado por las reivindicaciones siguientes. Pueden realizarse 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 que comprende:

generar un secreto maestro compartido, en el que el secreto maestro compartido comprende una clave maestra por pares, PMK;

generar un conjunto de datos de clave efímera compartida, en el que el conjunto de datos de clave efímera compartida se genera independiente del secreto maestro compartido, y en el que una duración de validez del conjunto de datos de clave efímera compartida es menor que una duración de validez del secreto maestro compartido;

obtener una clave transitoria por pares, PTK, basada en el secreto maestro compartido; y

cifrar al menos un mensaje que se va a transmitir a al menos una estación (118, 120) en base al menos al secreto maestro compartido, a la PTK y al conjunto de datos de clave efímera compartida.

2. El procedimiento de la reivindicación 1, en el que el conjunto de datos de clave efímera compartida permite un intercambio de claves de Diffie-Hellman, DH, asociado a un punto de acceso y a la al menos una estación.

3. El procedimiento de la reivindicación 2, en el que el intercambio de claves de DH utiliza un conjunto de claves seleccionadas de una lista de grupos de DH, especificada por el punto de acceso.

4. El procedimiento de la reivindicación 3, en el que el intercambio de claves de DH utiliza un conjunto de claves generadas en base a la aritmética de campo finito.

5. El procedimiento de la reivindicación 1, en el que el conjunto de datos de clave efímera compartida está asociado con un intercambio de coloquios iniciales, asociado con un punto de acceso y la al menos una estación, con el intercambio de coloquios iniciales realizado para autentificar las comunicaciones asociadas con el punto de acceso y la al menos una estación.

6. El procedimiento de la reivindicación 5, en el que el intercambio de coloquios iniciales, asociado con el punto de acceso y la al menos una estación, comprende un intercambio de coloquios iniciales utilizando un protocolo de Wi-Fi.

7. El procedimiento de la reivindicación 1, en el que el cifrado del al menos un mensaje asociado con el punto de acceso y la al menos una estación implementa la confidencialidad directa perfecta, PFS.

8. Un programa informático que comprende instrucciones para realizar un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 7.

9. Un aparato (108, 124), que comprende:

medios para comunicarse con al menos una estación mediante una interfaz de red inalámbrica;

medios para procesamiento configurados para:

generar un secreto maestro compartido, en el que el secreto maestro compartido comprende una clave maestra por pares,
generar un conjunto de datos de clave efímera compartida,
en el que el conjunto de datos de clave efímera compartida se genera independiente del secreto maestro compartido, y en el que una duración de validez del conjunto de datos de clave efímera compartida es menor que una duración de validez del secreto maestro compartido,
obtener una clave transitoria por pares, PTK, en base al secreto maestro compartido, y

cifrar al menos un mensaje que se va a transmitir a la al menos una estación (118, 120) en base al menos al secreto maestro compartido, a la PTK y al conjunto de datos de clave efímera compartida.

10. El aparato de la reivindicación 9, en el que el conjunto de datos de clave efímera compartida permite un intercambio de claves de Diffie-Hellman, DH.

11. El aparato de la reivindicación 10, en el que el intercambio de claves de DH utiliza un conjunto de claves seleccionadas de una lista de grupos de DH, especificada mediante un punto de acceso.

12. El aparato de la reivindicación 11, en el que el intercambio de claves de DH utiliza un conjunto de claves generadas en base a aritmética de campo finito.

13. El aparato de la reivindicación 9, en el que el conjunto de datos de clave efímera compartida está asociado con un intercambio de coloquios iniciales, asociado con un punto de acceso y la al menos una estación, con el intercambio de coloquios iniciales realizado para autentificar las comunicaciones asociadas con el punto de acceso y la al menos una estación.

14. El aparato de la reivindicación 13, en el que el intercambio de coloquios iniciales está asociado con un sistema de punto de acceso y la al menos una estación y el intercambio de coloquios iniciales utiliza un protocolo de Wi-Fi.

15. El aparato de la reivindicación 9, en el que el cifrado del al menos un mensaje asociado con la al menos una estación implementa la confidencialidad directa perfecta, PFS.

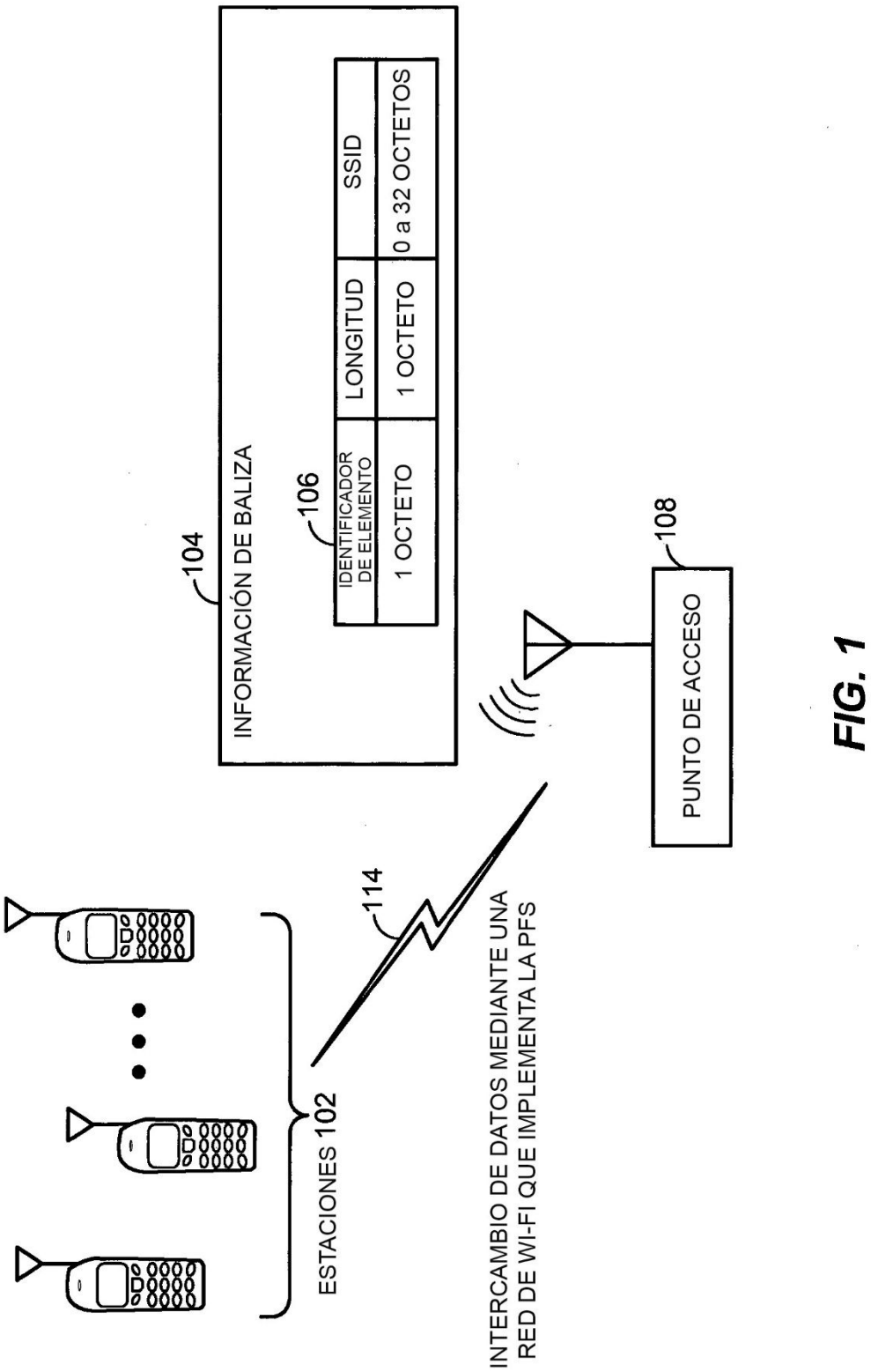
INFORMACIÓN DE BALIZA
104
106
IDENTIFICADOR DE ELEMENTO
LONGITUD
SSID
1 OCTETO
1 OCTETO
0 a 32 OCTETOS
108
PUNTO DE ACCESO
114
ESTACIONES 102
INTERCAMBIO DE DATOS MEDIANTE UNA RED DE WI-FI QUE IMPLEMENTA LA PFS

FIG. 1

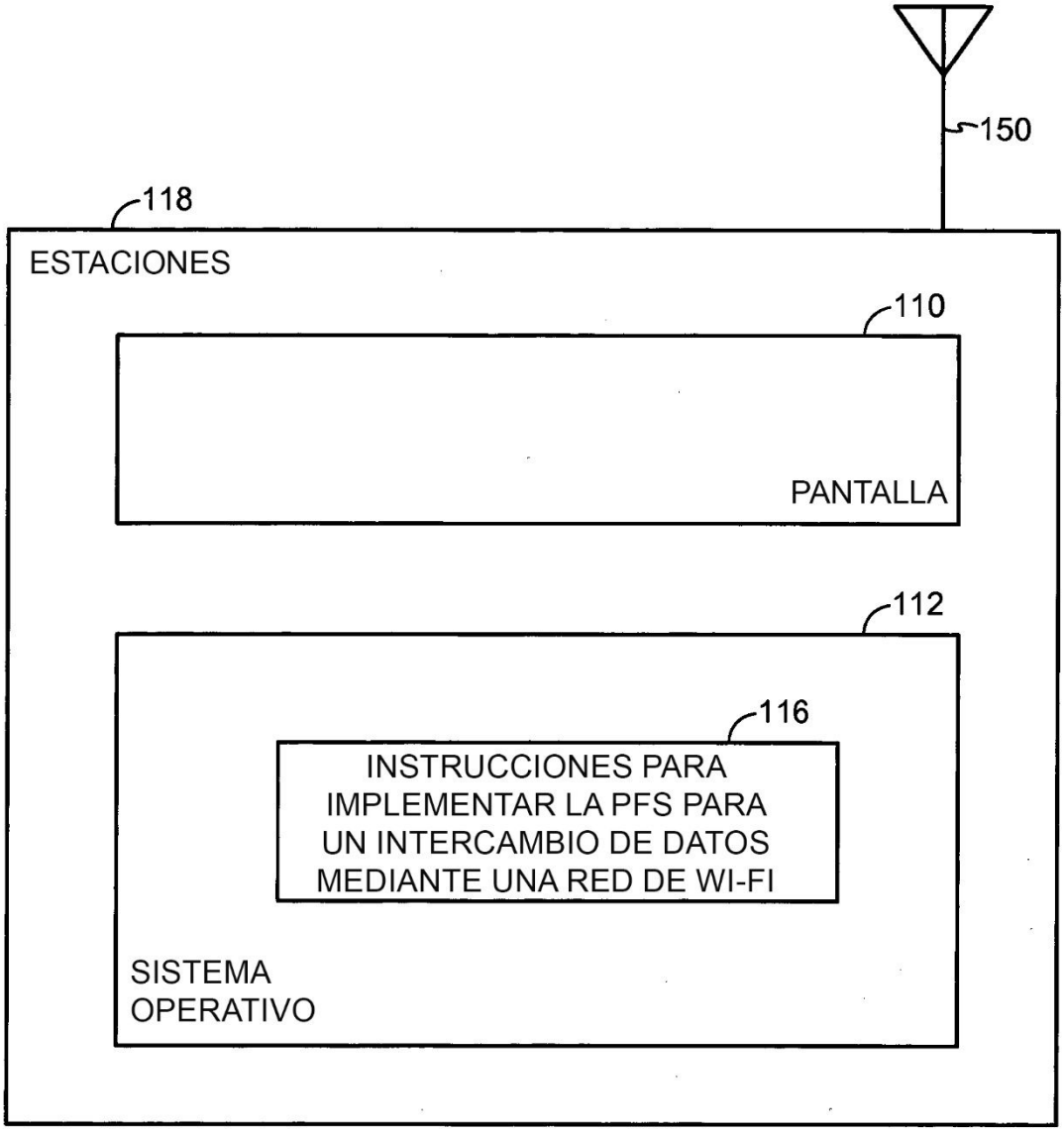
150
118
ESTACIONES
110
PANTALLA
112
116
INSTRUCCIONES PARA
IMPLEMENTAR LA PFS PARA
UN INTERCAMBIO DE DATOS
MEDIANTE UNA RED DE WI-FI
SISTEMA
OPERATIVO

FIG. 2

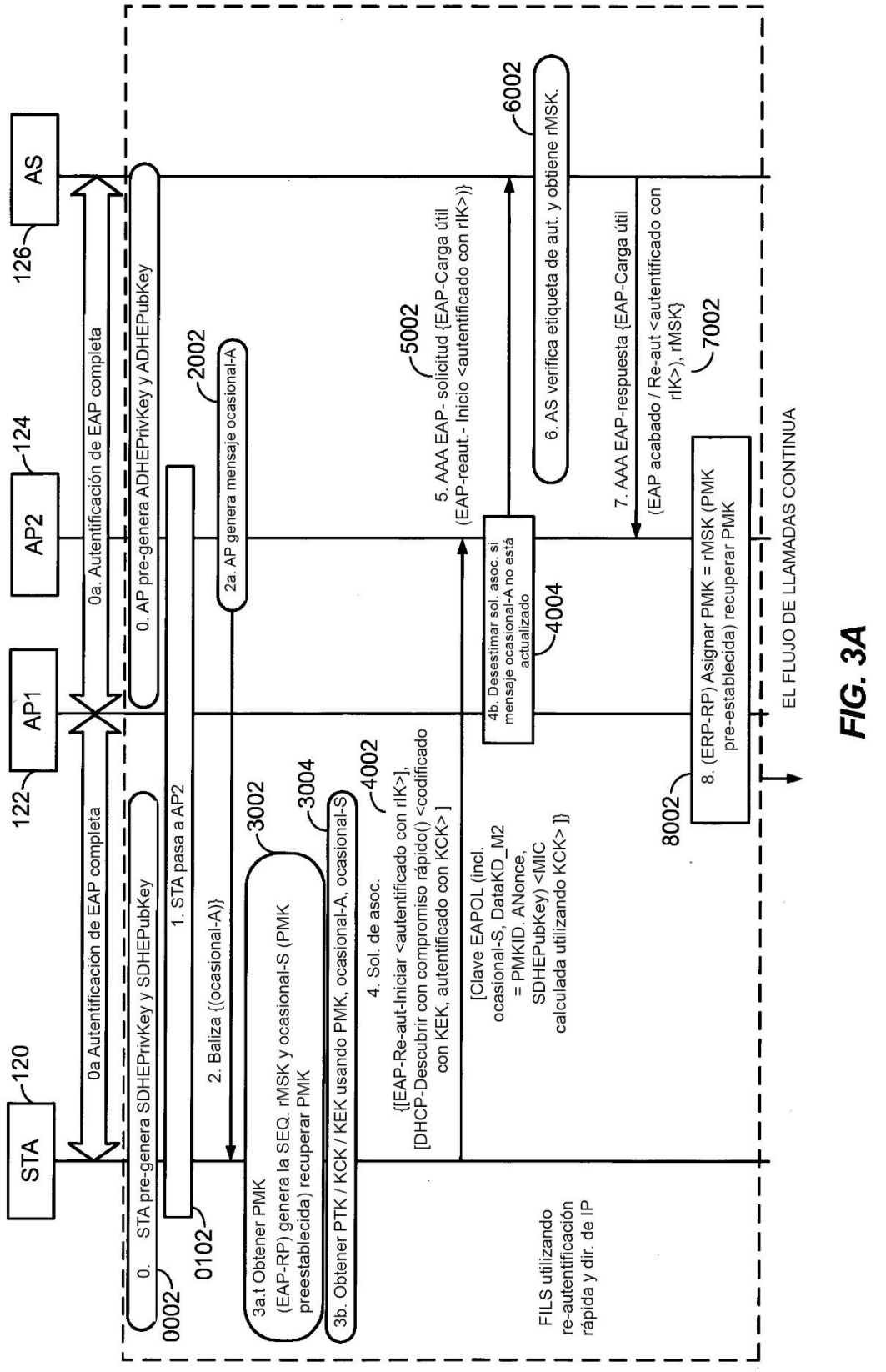
STA
120
AP1
122
AP2
124
AS
126
0a Autentificación de EAP completa
0a. Autentificación de EAP completa
0. STA pre-genera SDHEPrivKey y SDHEPubKey
0002
0. AP pre-genera ADHEPrivKey y ADHEPubKey
1. STA pasa a AP2
0102
2. Baliza {(ocasional-A)}
2002
2a. AP genera mensaje ocasional-A
3a.t Obtener PMK
(EAP-RP) genera la SEQ. rMSK y ocasional-S (PMK preestablecida) recuperar PMK
3002
3b. Obtener PTK / KCK / KEK usando PMK, ocasional-A, ocasional-S
3004
4. Sol. de asoc.
{[EAP-Re-aut-Iniciar <autentificado con rIK>],
[DHCP-Descubrir con compromiso rápido() <codificado con KEK, autentificado con KCK>]
4002
[Clave EAPOL (incl. ocasional-S, DataKD_M2 = PMKID. ANonce, SDHEPubKey) <MIC calculada utilizando KCK>]}
4b. Desestimar sol. asoc. si mensaje ocasional-A no está actualizado
4004
5. AAA EAP- solicitud {EAP-Carga útil (EAP-reaut.- Inicio <autentificado con rIK>)}
5002
6. AS verifica etiqueta de aut. y obtiene rMSK.
6002
7. AAA EAP-respuesta {EAP-Carga útil (EAP acabado / Re-aut <autentificado con rIK>), rMSK}
7002
8. (ERP-RP) Asignar PMK = rMSK (PMK pre-establecida) recuperar PMK
8002
FILS utilizando re-autentificación rápida y dir. de IP
EL FLUJO DE LLAMADAS CONTINUA

FIG. 3A

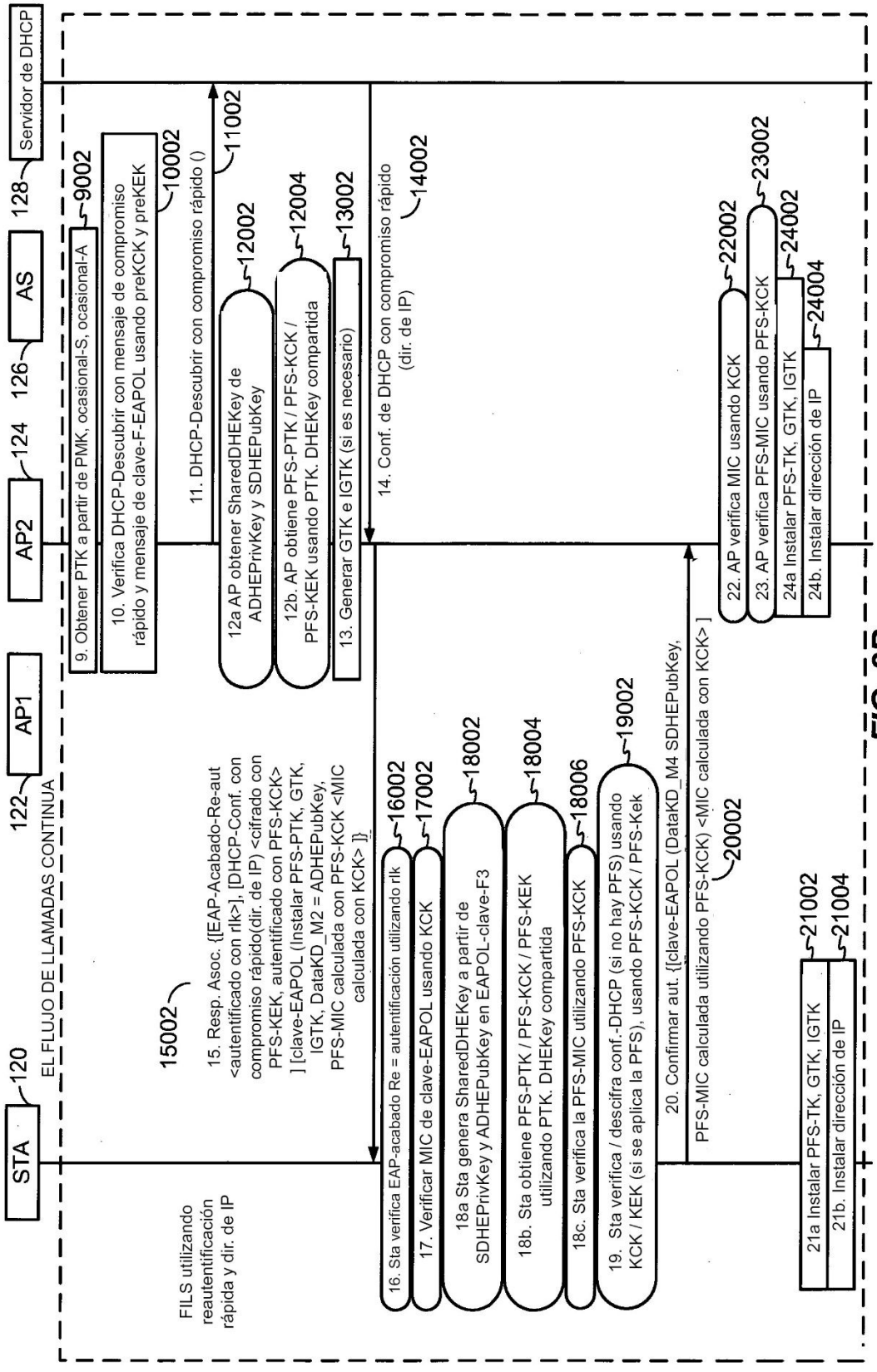
STA
120
EL FLUJO DE LLAMADAS CONTINUA
122
AP1
AP2
124
126
AS
128
Servidor de DHCP
9002
9. Obtener PTK a partir de PMK, ocasional-S, ocasional-A
10002
10. Verifica DHCP-Descubrir con mensaje de compromiso rápido y mensaje de clave-F-EAPOL usando preKCK y preKEK
11002
11. DHCP-Descubrir con compromiso rápido ()
12002
12a AP obtener SharedDHEKey de ADHEPrivKey y SDHEPubKey
12004
12b. AP obtiene PFS-PTK / PFS-KCK / PFS-KEK usando PTK. DHEKey compartida
13002
13. Generar GTK e IGTK (si es necesario)
14002
14. Conf. de DHCP con compromiso rápido (dir. de IP)
15002
15. Resp. Asoc. {[EAP-Acabado-Re-aut <autentificado con rlk>], [DHCP-Conf. con compromiso rápido(dir. de IP) <cifrado con PFS-KEK, autentificado con PFS-KCK>] [clave-EAPOL (Instalar PFS-PTK, GTK, IGTK, DataKD_M2 = ADHEPubKey, PFS-MIC calculada con PFS-KCK <MIC calculada con KCK>]}
FILS utilizando reautentificación rápida y dir. de IP
16002
16. Sta verifica EAP-acabado Re = autentificación utilizando rlk
17002
17. Verificar MIC de clave-EAPOL usando KCK
18002
18a Sta genera SharedDHEKey a partir de SDHEPrivKey y ADHEPubKey en EAPOL-clave-F3
18004
18b. Sta obtiene PFS-PTK / PFS-KCK / PFS-KEK utilizando PTK. DHEKey compartida
18006
18c. Sta verifica la PFS-MIC utilizando PFS-KCK
19002
19. Sta verifica / descifra conf.-DHCP (si no hay PFS) usando KCK / KEK (si se aplica la PFS), usando PFS-KCK / PFS-Kek
20002
20. Confirmar aut. {[clave-EAPOL (DataKD_M4 SDHEPubKey, PFS-MIC calculada utilizando PFS-KCK) <MIC calculada con KCK>]
22002
22. AP verifica MIC usando KCK
23002
23. AP verifica PFS-MIC usando PFS-KCK
24002
24a Instalar PFS-TK, GTK, IGTK
24004
24b. Instalar dirección de IP
21002
21a Instalar PFS-TK, GTK, IGTK
21004
21b. Instalar dirección de IP

FIG. 3B

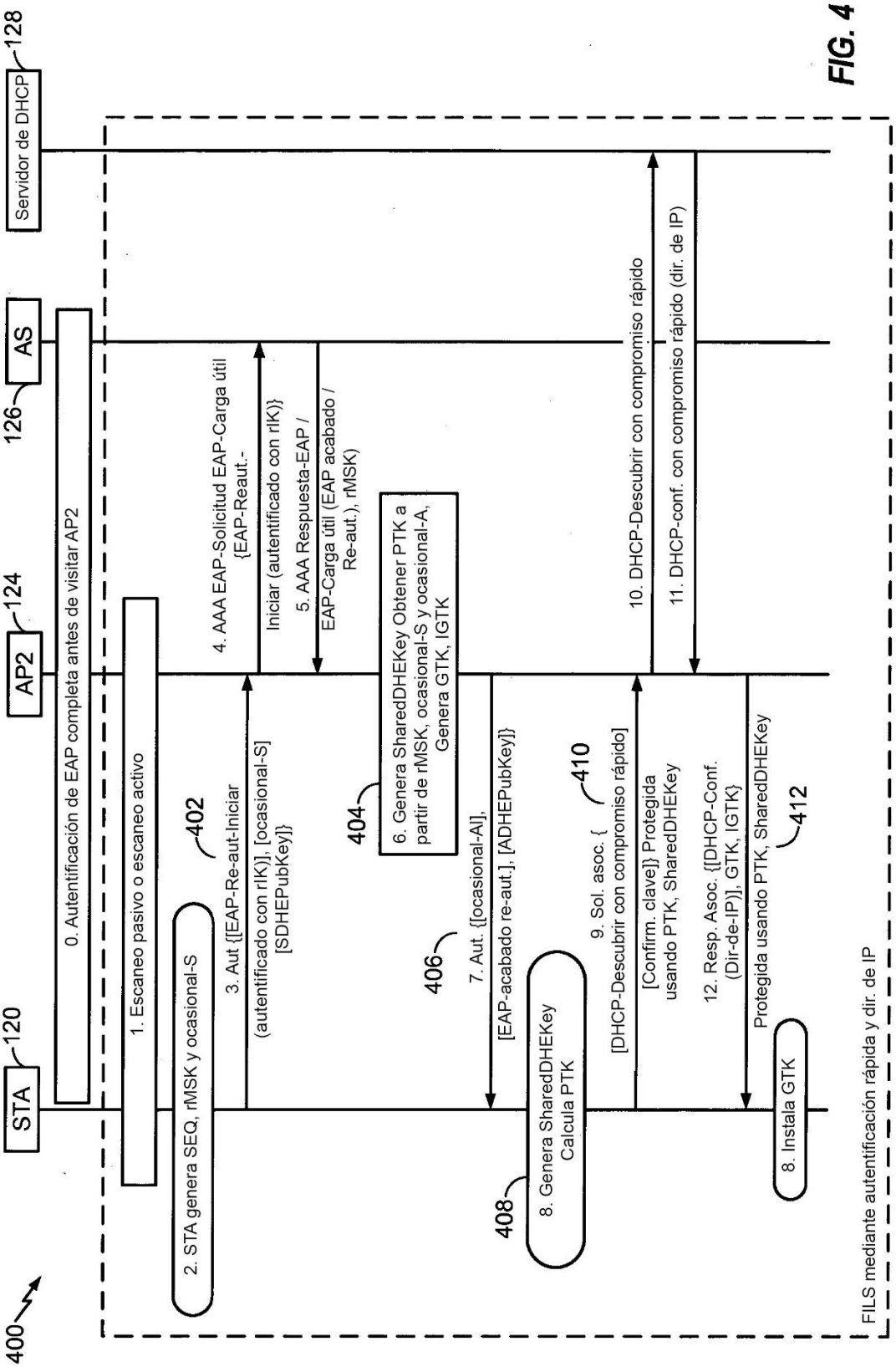
400
STA
120
AP2
124
AS
126
Servidor de DHCP
128
0. Autentificación de EAP completa antes de visitar AP2
1. Escaneo pasivo o escaneo activo
2. STA genera SEQ, rMSK y ocasional-S
402
3. Aut {[EAP-Re-aut-Iniciar (autentificado con rIK)], [ocasional-S] [SDHEPubKey]}
4. AAA EAP-Solicitud EAP-Carga útil {EAP-Reaut.-Iniciar (autentificado con rIK)}
5. AAA Respuesta-EAP / EAP-Carga útil (EAP acabado / Re-aut.), rMSK)
404
6. Genera SharedDHEKey Obtener PTK a partir de rMSK, ocasional-S y ocasional-A, Genera GTK, IGTK
406
7. Aut. {[ocasional-AI], [EAP-acabado re-aut.], [ADHEPubKey]}
408
8. Genera SharedDHEKey Calcula PTK
9. Sol. asoc. { [DHCP-Descubrir con compromiso rápido]
410
10. DHCP-Descubrir con compromiso rápido
11. DHCP-conf. con compromiso rápido (dir. de IP)
[Confirm. clave]} Protegida usando PTK, SharedDHEKey
12. Resp. Asoc. {[DHCP-Conf. (Dir-de-IP)], GTK, IGTK}
Protegida usando PTK, SharedDHEKey
412
8. Instala GTK
FILS mediante autentificación rápida y dir. de IP

FIG. 4

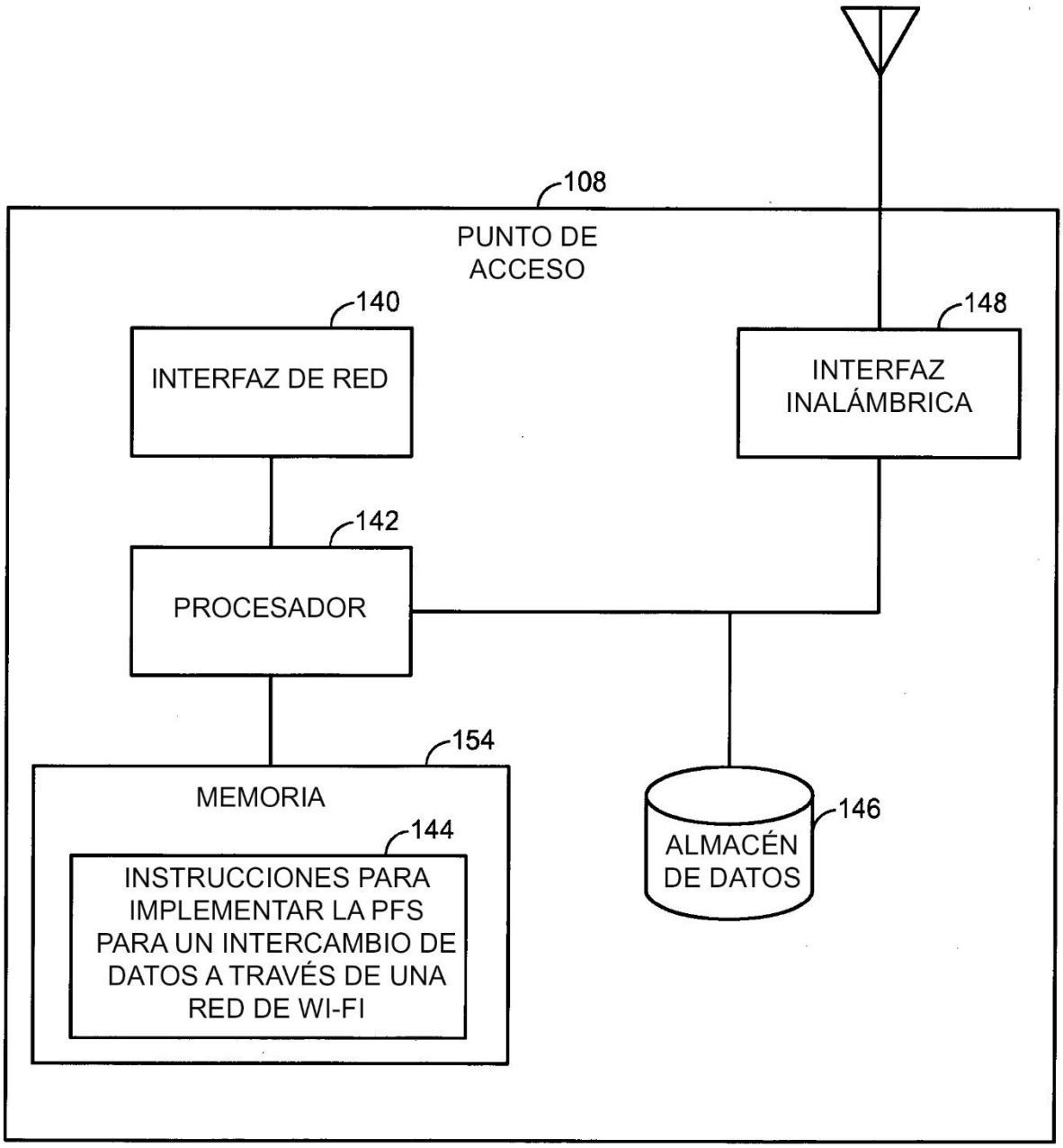
108
PUNTO DE ACCESO
140
INTERFAZ DE RED
148
INTERFAZ INALÁMBRICA
142
PROCESADOR
154
MEMORIA
144
INSTRUCCIONES PARA IMPLEMENTAR LA PFS PARA UN INTERCAMBIO DE DATOS A TRAVÉS DE UNA RED DE WI-FI
146
ALMACÉN DE DATOS

FIG. 5