(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 387 599**

(51) Int. CI.:
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09013590 .6**
(96) Fecha de presentación: **20.06.2003**
(97) Número de publicación de la solicitud: **2144399**
(97) Fecha de publicación de la solicitud: **13.01.2010**

(54) Título: **Función de interoperación para la autenticación de un terminal en una red de área local inalámbrica**

(30) Prioridad:
20.06.2002 US 176562

(45) Fecha de publicación de la mención BOPI:
27.09.2012

(45) Fecha de la publicación del folleto de la patente:
27.09.2012

(73) Titular/es:
QUALCOMM INCORPORATED
5775 MOREHOUSE DRIVE
SAN DIEGO, CA 92121-1714, US

(72) Inventor/es:
Hsu, Raymond T.

(74) Agente/Representante:
Carpintero López, Mario

DESCRIPCIÓN

Función de interoperación para la autenticación de un terminal en una red de área local inalámbrica.

Descripción

Antecedentes

Campo

La presente invención se refiere a una función de interoperación para un sistema de comunicación y, más específicamente, a mecanismos para la autenticación común y el intercambio de claves a través de una función de interoperación para su uso en una red de área local inalámbrica (WLAN).

Antecedentes

Una red de área local inalámbrica (WLAN) permite a los usuarios un acceso prácticamente sin restricciones a redes de servicios y datos del protocolo de Internet (IP). El uso de una WLAN no se limita a ordenadores portátiles y otros dispositivos informáticos, sino que se está expandiendo rápidamente para incluir teléfonos móviles, asistentes digitales personales (PDA) y otros pequeños dispositivos inalámbricos con soporte por parte de una red o portadora externa. Por ejemplo, un dispositivo inalámbrico que se comunica a través de una portadora celular puede itinerar hacia una WLAN en un cibercafé o espacio de trabajo. En esta situación, el dispositivo inalámbrico tiene acceso al sistema celular, pero desea acceder a la WLAN. El acceso a la WLAN requiere autenticación. Como el dispositivo inalámbrico ya ha obtenido acceso al sistema celular, la necesidad de otra autenticación es redundante. Hay una necesidad, por tanto, de una función de interoperación que permita una autenticación común para el acceso a un sistema celular y a una WLAN. Se reclama atención al artículo “Wireless LAN Access Architecture for Mobile Operators” [“Arquitectura de acceso a LAN inalámbrica para operadores móviles”]: Ala-Laurila, J et al. Revista de Comunicación de IEEE, páginas 82 a 89, noviembre de 2001; Centro de Servicio de IEEE, Piscataway, N.J., EE UU. El artículo describe una arquitectura de sistema de LAN que combina tecnología de acceso por radio a WLAN con funciones de gestión de abonados basadas en el SIM del operador móvil e infraestructuras de itinerancia. En el sistema revelado el acceso a la WLAN es autenticado y facturado usando el SIM del GSM.

También se reclama atención al documento US 6 128 389 A, que da a conocer un centro de autenticación segura (SAC) que puede acoplarse a sistemas de gestión segura de claves de autenticación (SAMS) de diversos proveedores de sistemas de comunicación. En un ejemplo del proceso de autenticación para estaciones móviles a las que dan servicio sistemas basados en IS-41 usando el algoritmo CAVE de autenticación celular y cifrado de voz, un sistema de servicio transmite un indicador de desafío global y un número aleatorio a la estación móvil. En respuesta, la estación móvil genera una señal de autenticación. El sistema de servicio envía la señal de autenticación al SAC. Si el SAC no dispone de datos secretos compartidos (SSD), o quiere actualizar los SSD, el SAC transmite una petición al SAMS.

Resumen

Según la presente invención, se proporcionan un aparato de Función de Interoperación, IWF, en comunicación con una red de área local inalámbrica, WLAN, y una red de comunicación celular en comunicación con un dispositivo inalámbrico, según lo estipulado en la reivindicación 1, y un procedimiento para autenticar un dispositivo inalámbrico por parte de una red de comunicación celular para acceder a una red de área local inalámbrica, WLAN, según lo estipulado en la reivindicación 3, y un producto de programa de ordenador, según lo estipulado en la reivindicación 7. Realizaciones adicionales se reivindican en las reivindicaciones dependientes.

Breve descripción de los dibujos

La FIG. 1 es un sistema de comunicación que incluye una red de área local inalámbrica (WLAN).

La FIG. 2 es un sistema de comunicación que tiene una unidad de función de interoperación (IWF).

La FIG. 3 es un diagrama de sincronismo de un proceso de autenticación en un sistema de comunicación

La FIG. 4 es un diagrama de flujo de un proceso de autenticación.

La FIG. 5 es un diagrama de sincronismo de un proceso de autenticación en un sistema de comunicación.

La FIG. 6 es un diagrama de flujo de un proceso de autenticación en una IWF en un sistema de comunicación.

La FIG. 7 es un diagrama de flujo del procesamiento de autenticación en una estación móvil.

Descripción detallada

El término “ejemplar” se usa en el presente documento con el significado de “que sirve como un ejemplo, caso o

ilustración“. Cualquier realización descrita en el presente documento como “ejemplar” no debe interpretarse necesariamente como preferida o ventajosa respecto a otras realizaciones.

Una estación de abonado HDR, denominada en el presente documento un terminal de acceso (AT), puede ser móvil o fija, y puede comunicarse con una o más estaciones base HDR, denominadas en el presente documento transceptores de banco de módems (MPT). Un terminal de acceso transmite y recibe paquetes de datos a través de uno o más transceptores de banco de módems a un controlador de estación base HDR, denominado en el presente documento un controlador de banco de módems (MPC). Los transceptores de banco de módems y controladores de banco de módems son partes de una red denominada red de acceso. Una red de acceso transporta paquetes de datos entre múltiples terminales de acceso. La red de acceso puede estar conectada además a redes adicionales fuera de la red de acceso, tales como una intranet corporativa o Internet, y puede transportar paquetes de datos entre cada terminal de acceso y tales redes externas. Un terminal de acceso que ha establecido una conexión de canal de tráfico activo con uno o más transceptores de banco de módems se denomina terminal de acceso activo, y se dice que está en estado de tráfico. Un terminal de acceso que está en el proceso de establecer una conexión de canal de tráfico activo con uno o más transceptores de banco de módems se dice que está en un estado de establecimiento de conexión. Un terminal de acceso puede ser cualquier dispositivo de datos que se comunica a través de una canal inalámbrico o a través de un canal por cable usando, por ejemplo, fibra óptica o cables coaxiales. Un terminal de acceso puede ser además cualquiera entre varios tipos de dispositivos que incluyen, pero no se limitan a, tarjeta de PC, tarjeta Compact Flash, módem externo o interno, o teléfono inalámbrico o de línea fija. El enlace de comunicación a través del cual el terminal de acceso envía señales al transceptor de banco de módems se denomina enlace inverso. El enlace de comunicación a través del cual un transceptor de banco de módems envía señales a un terminal de acceso se denomina enlace directo.

Se ilustra una red 100 de de área local inalámbrica (WLAN) en la FIG. 1 que tiene múltiples puntos 106, 108, 110 de acceso (AP). Un AP es un concentrador o puente que proporciona un control de topología en estrella del lado inalámbrico de la WLAN 100, así como acceso a la red por cable.

Cada AP 106, 108, 110, así como otros no mostrados, da soporte a una conexión a un servicio de datos, tal como Internet. Una estación 102 de trabajo, tal como un ordenador portátil, u otro dispositivo informático digital, se comunica con un AP a través de la interfaz aérea, de ahí la expresión LAN Inalámbrica. El AP se comunica entonces con un servidor de autenticación (AS) o centro de autenticación (AC). El AC es un componente para realizar servicios de autenticación para dispositivos que solicitan su admisión a una red. Las implementaciones incluyen el servicio de usuario de acceso telefónico de autenticación remota (RADIUS), que es una autenticación de usuario de Internet descrita en el documento RFC 2138, “Remote Autentication Dial in User Service (RADIUS)” [“Servicio de usuario de acceso telefónico de autenticación remota (RADIUS)”] de C. Rigney *et al*., publicado en abril de 1997, y otros servidores de autenticación, autorización y contabilidad (AAA).

La conexión inalámbrica a redes está surgiendo como un aspecto significativo de la operación entre redes. Presenta un conjunto de aspectos únicos basado en el hecho de que el único límite de una red inalámbrica es la intensidad de la señal de radio. No hay ningún cableado para definir la pertenencia como miembro en una red. No hay ningún procedimiento físico que restrinja a un sistema dentro del alcance de radio para que sea un miembro de una red inalámbrica. La conexión inalámbrica a redes, más que cualquier otra tecnología de conexión a redes, necesita un mecanismo de control de acceso y autenticación. Diversos grupos están trabajando actualmente en el desarrollo de un mecanismo de autenticación estándar. Actualmente, la norma aceptada es la IEEE 802.11.

La naturaleza de una red basada en RF la deja abierta a la interceptación de paquetes por cualquier radio dentro del alcance de un transmisor. La interceptación puede producirse bastante lejos del alcance de “trabajo” de los usuarios, usando antenas de alta ganancia. Con herramientas fácilmente disponibles, el intruso no se limita simplemente a recopilar paquetes para su análisis posterior, sino que puede ver efectivamente sesiones interactivas, como páginas web que está visualizando un usuario inalámbrico válido. Un intruso también puede captar intercambios de autenticación débiles, como algunos inicios de sesión en sedes de la web. El intruso podría duplicar después el inicio de sesión y obtener acceso.

Una vez que un atacante ha obtenido el conocimiento de cómo una WLAN controla la admisión, puede o bien obtener su admisión a la red por sí mismo, o bien robar un acceso de usuario válido. Robar un acceso de usuario es sencillo si el atacante puede imitar la dirección MAC del usuario válido y usar su dirección IP asignada. El atacante espera hasta que el sistema válido deje de usar la red y entonces asume su posición en la red. Esto permitiría a un atacante el acceso directo a todos los dispositivos dentro de una red, o usar la red para obtener acceso a la red más amplia de Internet, pareciendo en todo momento ser un usuario válido de la red atacada. Por tanto, la autenticación y el cifrado se convierten en asuntos clave en la implementación de una WLAN.

La autenticación es el proceso de probar la identidad de un individuo o una aplicación en una comunicación. Tal identificación permite al proveedor de servicios verificar la entidad como un usuario válido y también verificar al usuario para los servicios específicos solicitados. La autenticación y la autorización tienen en realidad significados muy específicos, aunque los dos sustantivos se usan a menudo de manera intercambiable, y en la práctica a menudo no se distinguen claramente.

La autenticación es el proceso en el que un usuario establece el derecho a una identidad, en esencia, el derecho a usar un nombre. Existe un gran número de técnicas que pueden usarse para autenticar un usuario, contraseñas, técnicas biométricas, tarjetas inteligentes y certificados.

Un nombre o una identidad tiene atributos asociados al mismo, o a la misma. Los atributos pueden estar estrechamente ligados a un nombre (por ejemplo, en una carga útil de certificado) o pueden almacenarse en un directorio u otra base de datos con una clave correspondiente al nombre. Los atributos pueden cambiar con el tiempo.

La autorización es el proceso de determinar si una identidad (más un conjunto de atributos asociados a esa identidad) tiene permiso para realizar alguna acción, tal como acceder a un recurso. Obsérvese que el permiso para realizar una acción no garantiza que pueda realizarse la acción. Obsérvese que las decisiones de autenticación y autorización pueden tomarse en diferentes puntos, por diferentes entidades.

En una red celular, la característica de autenticación es una capacidad de red que permite que redes celulares validen la identidad de un dispositivo inalámbrico, reduciendo de ese modo el uso no autorizado de redes celulares. El proceso es transparente para los abonados. No se requiere que los clientes hagan nada para autenticar la identidad de sus teléfonos cuando realizan una llamada.

La autenticación normalmente implica un esquema criptográfico, en el que el proveedor de servicios y el usuario tienen cierta información compartida y cierta información privada. La información compartida se denomina normalmente “secreto compartido”.

La clave A

La clave de autenticación (clave A) es un valor secreto que es único para cada teléfono celular individual. Se registra en el proveedor de servicios celulares y se almacena en el teléfono y en el centro de autenticación (AC). La clave A es programada en el teléfono por el fabricante. También puede introducirla manualmente el usuario, desde el menú del dispositivo inalámbrico, o bien mediante un terminal especial en el punto de venta.

El dispositivo inalámbrico y el AC deben tener la misma clave A para producir los mismos cálculos. La función principal de la clave A es ser usada como parámetro para calcular los datos secretos compartidos (SSD).

Los datos secretos compartidos (SSD)

Se usan SSD como entrada para cálculos de autenticación en el dispositivo inalámbrico y el AC, y se almacenan en ambos lugares. A diferencia de la clave A, los SSD pueden modificarse a través de la red. El AC y el dispositivo inalámbrico comparten tres elementos que entran en el cálculo de los SSD: 1) el número de serie electrónico (ESN); 2) la clave de autenticación (clave A) y 3) un número aleatorio para el cálculo de datos secretos compartidos (RANDSSD).

El ESN y el RANDSSD se transmiten a través de la red y a través de la interfaz aérea. Los SSD se actualizan cuando un dispositivo realiza su primer acceso al sistema, y posteriormente de manera periódica. Cuando se calculan los SSD, el resultado son dos valores separados, SSD-A y SSD-B. SSD-A se usa para la autenticación. SSD-B se usa para el cifrado y la privacidad de voz.

Según las capacidades del sistema de servicio, los SSD pueden compartirse o no compartirse entre el AC y el centro de conmutación móvil (MSC) de servicio. Si se comparten datos secretos, significa que el AC los enviará al MSC de servicio y el MSC de servicio debe poder ejecutar el algoritmo CAVE. Si no se comparten, el AC guardará los datos y realizará la autenticación.

El modo de compartir afecta a cómo se lleva a cabo un desafío de autenticación. Un desafío de autenticación es un mensaje enviado para plantear un desafío sobre la identidad del dispositivo inalámbrico. Básicamente, el desafío de autenticación envía cierta información, normalmente datos numéricos aleatorios, para su procesamiento por el usuario. Entonces el usuario procesa la información y envía una respuesta. Se analiza la respuesta para la verificación del usuario. Con datos secretos compartidos, un desafío se gestiona en el MSC de servicio. Con datos secretos no compartidos, un desafío es gestionado por el AC. Compartiendo datos secretos, el sistema puede minimizar la cantidad de tráfico enviado y permitir que se produzcan desafíos más rápidamente en el conmutador de servicio.

Procedimientos de autenticación

En un sistema dado, un registro de posición base (HLR) controla el proceso de autenticación actuando como intermediario entre el MSC y el AC. Se configura el MSC de servicio para que dé soporte a la autenticación con el HLR del móvil y viceversa.

El dispositivo inicia el proceso notificando al MSC de servicio si puede realizar la autenticación, estableciendo un campo de autorización en el tren de mensajes de sobregasto. En respuesta, el MSC de servicio inicia el proceso de

registro / autenticación con una petición de autenticación.

Enviando la petición de autenticación, el MSC de servicio le dice al HLR / AC si puede realizar cálculos de CAVE. El AC controla cuál de los MSC de servicio, así como cuáles capacidades de dispositivo, se usarán entre los disponibles. Cuando el MSC de servicio no dispone de capacidad para CAVE, no pueden compartirse los SSD entre el AC y MSC y, por tanto, todos los procesos de autenticación se realizan en el AC.

El propósito de la petición de autenticación (AUTHREQ) es autenticar el teléfono y solicitar SSD. La AUTHREQ contiene dos parámetros para la autenticación, los parámetros AUTHR y RAND. Cuando el AC obtiene la AUTHREQ, usa el RAND y los últimos SSD conocidos para calcular AUTHR. Si coincide con el AUTHR enviado en la AUTHREQ, entonces la autenticación es satisfactoria. El resultado devuelto a la AUTHREQ contendrá los SSD si pueden compartirse.

El desafío

El proceso de autenticación consiste en un diálogo de desafío y respuesta. Si se comparten SSD, se ejecuta el diálogo entre el MSC y el dispositivo. Si no se comparten SSD, se ejecuta el diálogo entre el HLR / AC y el dispositivo. Según el tipo de conmutación, el MSC puede realizar un desafío único, un desafío global, o bien ambos. Algunos MSC no pueden actualmente realizar un desafío global. El desafío único es un desafío que sólo se produce durante intentos de llamada, porque usa el canal de voz. El desafío único presenta una autenticación a un único dispositivo durante el origen de la llamada y la entrega de la llamada. El desafío global es un desafío que se produce durante el registro, el origen de la llamada y la entrega de la llamada. El desafío global presenta un desafío de autenticación a todas las MS que estén usando un canal de control de radio particular. Se denomina desafío global porque se difunde por el canal de control de radio, y el desafío es usado por todos los teléfonos que acceden a ese canal de control.

Durante un desafío, el dispositivo responde a un número aleatorio proporcionado por el MSC o el AC. El dispositivo usa el número aleatorio y los datos secretos compartidos almacenados en el dispositivo para calcular una respuesta al MSC. El MSC también usa el número aleatorio y los datos secretos compartidos para calcular cuál debería ser la respuesta desde el dispositivo. Estos cálculos se realizan a través del algoritmo CAVE. Si las respuestas no son iguales, se deniega el servicio. El proceso de desafío no aumenta la cantidad de tiempo que lleva conectar la llamada. De hecho, la llamada puede continuar en algunos casos, sólo para interrumpirse cuando fracasa la autenticación.

Las redes de área local inalámbricas (WLAN) han adquirido una tremenda popularidad como medio de proporcionar a los usuarios un acceso sin cables a redes de datos de IP. Las redes inalámbricas de tercera generación (3G) también están diseñadas para ofrecer acceso a datos de alta velocidad; aunque las velocidades de datos a las que dan soporte normalmente son inferiores a las de las WLAN, las redes 3G ofrecen una cobertura de datos sobre una zona mucho más amplia. Aunque podrían verse como competidores, las redes WLAN y 3G pueden ser complementarias: las WLAN ofrecen cobertura de “puntos calientes” de alta capacidad en zonas públicas tales como salas de aeropuertos y vestíbulos de hoteles, mientras que las redes 3G pueden proporcionar a los usuarios un servicio de datos casi ubicuo cuando están en movimiento. Por tanto, el mismo operador puede proporcionar servicios de acceso tanto a 3G como a WLAN con una única suscripción de usuario. Esto significa que la MS usa el mismo procedimiento de autenticación y el mismo secreto para ambos tipos de autenticación de acceso.

En una autenticación de acceso a 3G, el centro de autenticación (AC) autentica la MS. El AC y la MS tienen un secreto compartido. Del lado de la red, el secreto compartido se almacena de manera segura en el AC y no se distribuye a ninguna otra entidad de red. Del lado de la MS, el secreto compartido se almacena de manera segura en la memoria con seguridad y no se distribuye fuera de ésta. El AC y la MS usan o bien el algoritmo de autenticación celular y cifrado de voz (CAVE) o bien el de acuerdo de clave de autenticación (AKA) como algoritmo de autenticación. Los parámetros de autenticación se entregan entre la MS y el AC a través de mensajes de señalización aéreos de 3G y mensajes de señalización por la red (por ejemplo, IS-41).

En la autenticación de acceso a WLAN, es deseable que la MS sea autenticada por el mismo AC usando el mismo secreto compartido y algoritmo de autenticación (AKA o CAVE). Sin embargo, se usan diferentes mecanismos para entregar los parámetros de autenticación en la WLAN. Específicamente, los parámetros de autenticación se entregan a través del protocolo de autenticación extensible (EAP) y un protocolo AAA (RADIUS o Diameter). El desafío es hacer interoperar los mecanismos de entrega entre 3G y WLAN de modo que los parámetros de autenticación puedan entregarse entre la MS y el AC para la autenticación de acceso a la WLAN.

Tal como se estableció anteriormente, el algoritmo CAVE se usa comúnmente para comunicaciones celulares y, por tanto, está ampliamente usado y distribuido. También se usan algoritmos alternativos para la autenticación. Específicamente, en comunicaciones de datos existe una gran variedad de algoritmos de complejidad y aplicación variables. Para coordinar estos mecanismos, se ha desarrollado el protocolo de autenticación extensible (EAP) como un marco de protocolo general que da soporte a múltiples mecanismos de autenticación y distribución de claves. El EAP se describe en el documento “PPP Extensible Autentication Protocol (EAP)” [“Protocolo PPP de autenticación extensible”] de L. Blunk *et al*., RFC 2284, publicado en marzo de 1998.

Un mecanismo de este tipo con soporte por parte del EAP, según se define en el documento “EAP AKA Autentication” [“Autenticación AKA del EAP”] de J. Arkko *et al*., publicado como un borrador de Internet en febrero de 2002, es el algoritmo AKA. Existe una necesidad, por tanto, de extender el EAP para que incluya el algoritmo celular CAVE. Esto es deseable para proporcionar compatibilidad con versiones anteriores para nuevos sistemas y redes.

EAP

El protocolo de autenticación extensible (EAP) es un protocolo general para la autenticación que da soporte a múltiples mecanismos de autenticación. El EAP no selecciona un mecanismo de autenticación específico durante la configuración y el control de los enlaces, sino que más bien pospone esto hasta que comienza el procedimiento de autenticación. Esto permite al autenticador solicitar más información antes de determinar el mecanismo de autenticación específico. El autenticador se define como el extremo del enlace que requiere la autenticación. El autenticador especifica el protocolo de autenticación que va a usarse durante el establecimiento del enlace.

Función de interoperación (IWF)

Según una realización, se implementa una nueva entidad de red y se denomina función de interoperación (IWF) o más específicamente, la función de interoperación (IWF) AAA / IS-41. La IWF realiza la interoperación de los mecanismos de entrega de los parámetros de autenticación (por ejemplo, CAVE, AKA) entre redes inalámbricas, tales como redes 3G y WLAN. Se ilustra una IWF 204 en la FIG. 2 como parte de un sistema 200 de comunicación. El sistema 200 incluye una WLAN 202, una IWF 204 y un AC 206. Como se ilustra, una estación 208 de trabajo está actualmente dentro del alcance de comunicación de la WLAN 202. La IWF 204 proporciona una interfaz entre el AC 206 y la WLAN 202, que permite el uso de una autenticación común para permitir que la MS 208 obtenga acceso a la red. Obsérvese que la MS 208 puede ser una estación de trabajo inalámbrica, un usuario remoto u otro dispositivo inalámbrico que pueda comunicarse a través de una red distinta a la WLAN 202, que en este caso es la red de la que el AC 206 es una parte.

La IWF 204 es una función de interoperación unidireccional, es decir, la petición de autenticación se origina desde la WLAN 202. Obsérvese que en la presente realización e ilustración, AAA es el mecanismo de entrega para transportar parámetros de autenticación entre la WLAN 202 y la IWF 204. Además, IS-41 es el mecanismo de entrega para transportar parámetros de autenticación entre la IWF 204 y el AC 206. De manera específica en este ejemplo, se usará RADIUS como protocolo AAA.

En la FIG. 3 se ilustra el procesamiento de autenticación. Inicialmente, la IWF 204 recibe un mensaje de petición de acceso de RADIUS que contiene la identidad de la MS 208 (o estación de trabajo inalámbrica) que desea realizar la autenticación para el acceso a la WLAN 202. La IWF 204 está configurada con una base 210 de datos que almacena la capacidad de autenticación asociada con la MS 208, así como otra MS 208 registrada actualmente a través del AC 206. La base 210 de datos está indizada por cada identidad de la MS 208. Por tanto, la IWF 204 puede determinar la capacidad de autenticación de la MS 208 (por ejemplo, AKA y / o CAVE).

Si la MS 208 sólo da soporte a CAVE, la IWF 204 realiza el siguiente procedimiento concordante con la FIG. 3. La IWF envía un mensaje de desafío de acceso de RADIUS que contiene un mensaje de petición del EAP que contiene un desafío de CAVE. Como se ha expuesto anteriormente en el presente documento, el desafío contiene un número aleatorio que va a usar la MS 208 para calcular una respuesta de autenticación. La IWF 204 recibe el mensaje de petición de acceso de RADIUS que contiene el mensaje de respuesta del EAP (que contiene la respuesta al desafío de CAVE). La respuesta de CAVE contiene la respuesta de autenticación de la MS 208, es decir, el resultado de los cálculos usando el número aleatorio, y otros parámetros específicos de la MS 208.

Si la IWF 204 no es capaz de verificar el mensaje de respuesta del EAP o, específicamente, no es capaz de verificar la respuesta de CAVE al desafío de CAVE, la IWF 204 envía un mensaje de AUTHREQ, que es un mensaje de IS-41, al AC 206. En este caso, la IWF 204 no dispone de la información necesaria para confirmar la respuesta al desafío. El mensaje de AUTHREQ contiene la IMSI asignada a la MS 208, el número aleatorio (es decir, el desafío) y la respuesta de autenticación producida por la MS 208. El AC 206, que tiene conocimiento del secreto compartido específico de la MS 208, verifica entonces la respuesta al desafío de la MS 208. El AC 206 devuelve el mensaje de AUTHREQ, que es un mensaje de IS-41, a la IWF. El mensaje de AUTHREQ contiene el resultado de la autenticación. Si es satisfactorio, el mensaje de AUTHREQ también contiene una clave denominada clave del algoritmo de cifrado de mensajes celulares (CMEA), que se usa para proteger el tráfico de la MS 208 en la WLAN 202. Si la IWF 204 no es capaz de recibir el mensaje de AUTHREQ desde el AC 206 tras un número de reintentos predeterminado, la IWF 204 envía el mensaje de rechazo de acceso de RADIUS que contiene el fracaso del EAP para la WLAN 202. La incapacidad para recibir un mensaje de AUTHREQ puede indicar problemas de red entre la IWF 204 y el AC 206.

Si la IWF 204 es capaz de verificar la respuesta al desafío desde la MS 208, y tal verificación es satisfactoria, la IWF 204 genera la clave de CMEA. Si la MS 208 se autentica satisfactoriamente, la IWF 204 envía un mensaje de aceptación de acceso de RADIUS a la WLAN 202. Un mensaje de este tipo contiene un mensaje de éxito del EAP así como la clave de CMEA. Si la MS 208 fracasa en la autenticación, la IWF 204 envía un mensaje de rechazo de acceso de RADIUS que contiene un mensaje de fracaso del EAP a la WLAN 202.

La FIG. 4 ilustra un proceso 400 de autenticación según una realización, en el que la MS 208 da soporte al protocolo CAVE. El proceso se inicia cuando la MS 208 y la WLAN 202 empiezan las negociaciones de identificación en la etapa 402. También en esta etapa, la WLAN 202 envía un mensaje de petición de acceso de RADIUS que contiene la identidad de la MS 208. Como se ha indicado anteriormente en el presente documento, la identidad puede proporcionarse por medio de la IMSI u otro identificador único para la MS 202. El proceso implica que la MS 208 trate de acceder a la WLAN 202 y, en respuesta, la WLAN 202 solicite la identificación de la MS 208, etapa 402. En este punto, la IWF 204 envía un mensaje de desafío de acceso de RADIUS a la WLAN 202, que contiene el desafío de CAVE en la etapa 404. En respuesta al desafío, la MS 208 calcula una respuesta y proporciona la respuesta a la WLAN 208 (no mostrado). La respuesta se envía entonces a la IWF 204 en un mensaje de respuesta de acceso de RADIUS en la etapa 406. Si la IWF 204 no dispone de conocimiento del secreto compartido para la MS 208 en el rombo 408 de decisión, el procesamiento continúa hacia la etapa 410 en la que la IWF 204 envía un mensaje de AUTHREQ al AC 206. El mensaje de AUTHREQ solicita la autenticación de la MS 208. Si se devuelve un mensaje de AUTHREQ en el rombo 412 de decisión, el procesamiento continúa hacia el rombo 414 de decisión para determinar si el mensaje de AUTHREQ indica una autenticación satisfactoria, es decir, el resultado de la autenticación es la aprobación para el acceso a la WLAN. Si no se recibe el mensaje de AUTHREQ en el rombo 412 de decisión, el procesamiento continúa hacia la etapa 416, en la que la IWF envía un mensaje de rechazo de acceso de RADIUS.

Continuando desde el rombo 408 de decisión, si la IWF 204 tiene conocimiento de la información secreta compartida de la MS 208, la IWF 204 es capaz de determinar si la autenticación es satisfactoria en el rombo 418 de decisión. Una autenticación satisfactoria avanza a la etapa 420 para calcular la clave de CMEA. Un mensaje de aceptación de acceso de RADIUS se envía entonces en la etapa 424. Obsérvese que una autenticación satisfactoria en la etapa 414 (para la autenticación por el AC 206) también avanza a la etapa 420. Desde el rombo 418 de decisión, si la autenticación no es satisfactoria, la IWF envía un mensaje de rechazo de acceso de RADIUS en la etapa 422.

En una realización alternativa, la IWF 204 usa el protocolo AKA para enviar un desafío. Como se ilustra en la FIG. 5, si la MS 208 da soporte al AKA, la IWF 204 implementa el desafío de AKA, y se cambia el orden del procesamiento de autenticación. En este escenario, la información suficiente para autenticar un usuario, tal como la MS 208, se proporciona en un vector de autenticación (AV). Obsérvese que el AC 206 puede enviar la información del secreto compartido (SS) en el AV a la IWF 204. Según la presente realización, el AV incluye el SS, el desafío y una clave de cifrado (CK). La CK se usa para cifrar tráfico de la MS.

Si la IWF 204 no dispone del vector de autenticación (AV) para autenticar la MS 208, la IWF 204 envía un mensaje de AUTHREQ para solicitar el AV al AC 206. El mensaje de AUTHREQ contiene la identidad de la MS 208, tal como la IMSI, y la petición del AV. El AC 206 responde con el mensaje de AUTHREQ que contiene el AV. El AV consiste en un número aleatorio (RAND), una respuesta esperada (XRES), una clave de cifrado (CK) y un testigo de autenticación (AUTN). El AC puede proporcionar múltiples AV en el mensaje de AUTHREQ, de modo que no sea necesario que la IWF solicite al AC 206 una autenticación posterior.

Si la IWF 204 no puede recibir el mensaje de AUTHREQ desde el AC 206 (lo que puede ser tras cierto número predeterminado de reintentos), la IWF 204 envía un mensaje de rechazo de acceso de RADIUS que contiene un mensaje de fracaso del EAP a la WLAN 202, tal como cuando existen problemas de red entre la IWF 204 y el AC 206.

Si la AUTHREQ recibida no contiene el AV, la IWF 204 envía el mensaje de rechazo de acceso de RADIUS que contiene el mensaje de fracaso del EAP a la WLAN 202. Por ejemplo, un caso de este tipo puede presentarse cuando la MS 202 tiene una suscripción que ha caducado.

Si la IWF 204 tiene el AV, la IWF 204 envía un mensaje de desafío de acceso de RADIUS, que contiene un mensaje de petición del EAP que tiene un desafío del AKA, a la WLAN 202. El desafío del AKA contiene el AUTN y el RAND. El AUTN lleva las credenciales del AC 206 y será verificado por la MS 208. El RAND es un desafío para la MS 208 que se usa para calcular una respuesta de autenticación (RES). La MS 208 proporciona la RES a la WLAN 202.

La IWF 204 recibe el mensaje de petición de acceso de RADIUS, que contiene una respuesta del EAP que incluye un desafío de CAVE, desde la WLAN 202. El desafío de CAVE contiene la respuesta de autenticación (RES) de la MS 208 recibida a través de la WLAN 202. La IWF 204 compara la RES con XRES. Para una coincidencia, la MS 208 se autentica satisfactoriamente, y la IWF 204 envía un mensaje de aceptación de acceso de RADIUS a la WLAN 202. Un mensaje de este tipo contiene un mensaje de éxito del EAP y una CK. La CK se usará para proteger el tráfico de la MS 208 en la WLAN 202. Si la MS 208 fracasa en la autenticación, la IWF 204 envía un mensaje de rechazo de acceso de RADIUS, que contiene un mensaje de fracaso del EAP, a la WLAN 202.

La FIG. 6 ilustra un procedimiento 500 de autenticación que usa el AV. Si la IWF 204 tiene el AV suficiente para verificar la MS 208 en el rombo 502 de decisión, el proceso continúa hasta la etapa 506; si no, el procesamiento continúa hacia la etapa 504. En la etapa 506, la IWF 204 envía un mensaje de desafío de acceso de RADIUS a la WLAN 202 para la MS 208. El desafío se remite entonces a la MS 208 para su procesamiento, y se proporciona una respuesta de vuelta a la WLAN 202 (no mostrado). La IWF 204 recibe el mensaje de petición de acceso de RADIUS en la etapa 510, y determina si la autenticación de la MS es satisfactoria en el rombo 512 de decisiones. En una

autenticación satisfactoria, la IWF 204 envía un mensaje de aceptación de acceso de RADIUS en la etapa 514; si no, la IWF 204 envía un mensaje de rechazo de acceso de RADIUS en la etapa 516.

Volviendo al rombo 502 de decisión, si la IWF 204 no dispone del AV, la IWF envía un mensaje de AUTHREQU al AC 206 en la etapa 504. Al recibir el AV, la IWF 204 continúa el procesamiento hacia la etapa 506; si no, el procesamiento continúa hacia la etapa 516.

La FIG. 7 ilustra una IWF 600 adaptada para obrar como interfaz entre una WLAN (no mostrada) y, por tanto, capaz de realizar los procedimientos necesarios para la comunicación, autenticación, intercambio de claves y otras comunicaciones de seguridad con la misma, y un AC (no mostrado) y, por tanto, capaz de realizar los procedimientos necesarios para la comunicación, autenticación, intercambio de claves y otras comunicaciones de seguridad con el mismo. La IWF 600 incluye una unidad 602 de interfaz de WLAN, que prepara, transmite, recibe e / o interpreta comunicaciones con una WLAN. De manera similar, la IWF 600 incluye una unidad 604 de interfaz de AC, que prepara, transmite, recibe e / o interpreta comunicaciones con un AC. La IWF 600 incluye además una unidad 608 de procedimiento de CAVE, una unidad 610 de procedimiento de EAP y una unidad 612 de procedimiento de RADIUS. La IWF 600 puede incluir cualquier número de tales unidades de procedimiento (no mostradas) según se requiera para la función de interoperación en un sistema dado. Las unidades de procedimiento, tales como la unidad 608 de procedimiento de CAVE, la unidad 610 de procedimiento de EAP y la unidad 612 de procedimiento de RADIUS, pueden implementarse en software, hardware, firmware o una combinación de los mismos. Los diversos módulos dentro de la IWF 600 se comunican a través de un bus 614 de comunicación.

Los expertos en la técnica entenderán que la información y las señales pueden representarse usando cualquiera entre una gran variedad de tecnologías y técnicas diferentes. Por ejemplo, los datos, instrucciones, comandos, información, señales, bits, símbolos y segmentos de código a los que pueda hacerse referencia a lo largo de la descripción anterior pueden representarse mediante tensiones, corrientes, ondas electromagnéticas, partículas o campos magnéticos, partículas o campos ópticos, o cualquier combinación de los mismos.

Los expertos apreciarán además que los diversos bloques lógicos, módulos, circuitos y etapas algorítmicas ilustrativos descritos con respecto a las realizaciones dadas a conocer en el presente documento pueden implementarse como hardware electrónico, software informático o combinaciones de los mismos. Para ilustrar con claridad esta intercambiabilidad de hardware y software, se han descrito anteriormente diversos componentes, bloques, módulos, circuitos y etapas ilustrativos, en general, en cuanto a su funcionalidad. El que tal funcionalidad se implemente como hardware o software depende de las limitaciones particulares de aplicación y diseño impuestas al sistema global. Los expertos en la técnica pueden implementar la funcionalidad descrita de diversas maneras para cada aplicación particular, pero no debe interpretarse que tales decisiones de implementación provocan un apartamiento del alcance de la presente invención.

Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos con respecto a las realizaciones dadas a conocer en el presente documento 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 en el terreno (FPGA) u otro dispositivo lógico programable, compuerta discreta o lógica de transistor, componentes de hardware discretos o cualquier combinación de los mismos diseñada para realizar 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, microcontrolador o máquina de estados convencional. También puede implementarse un procesador como una combinación de dispositivos de computación, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores conjuntamente con un núcleo de DSP, o cualquier otra configuración de este tipo.

Las etapas de un procedimiento o algoritmo descritas con respecto a las realizaciones dadas a conocer en el presente documento pueden realizarse directamente en hardware, en un módulo de software ejecutado por un procesador, o en una combinación de ambos. Un modulo de software puede residir en memoria RAM, memoria *flash*, memoria ROM, memoria EPROM, memoria EEPROM, registros, disco duro, un disco extraíble, un CD-ROM, o cualquier otra forma de medio de almacenamiento conocida en la técnica. Un medio de almacenamiento ejemplar se acopla al procesador de modo que el procesador pueda leer información de, y escribir información en, el medio de almacenamiento. Como alternativa, el medio de almacenamiento puede estar integrado en el procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un terminal de usuario. Como alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

La descripción anterior de las realizaciones dadas a conocer se proporciona para permitir a cualquier experto en la técnica realizar o usar la presente invención. Diversas modificaciones de estas realizaciones serán inmediatamente evidentes para los expertos en la técnica, y los principios genéricos definidos en el presente documento pueden aplicarse a otras realizaciones sin apartarse del alcance de la invención reivindicada.

REIVINDICACIONES

1. Un aparato (204) de función de interoperación, IWF, en comunicación con una red (202) de área local inalámbrica, WLAN, y una red de comunicación celular, que se comunica con un dispositivo (208) inalámbrico, estando el aparato (204) de IWF adaptado para determinar una capacidad de autenticación asociada al dispositivo (208) inalámbrico a partir de una base (210) de datos usando una identidad recibida de dicho dispositivo (208) inalámbrico, en el que dicha capacidad de autenticación comprende bien un algoritmo de autenticación celular y cifrado de voz, CAVE, o bien un algoritmo de acuerdo de clave de autenticación, AKA, comprendiendo el aparato (204) de IWF:

dicha base (210) de datos adaptada para almacenar la capacidad de autenticación correspondiente al dispositivo (208) inalámbrico;

una interfaz de WLAN configurada para:

enviar, a través de la WLAN (202), un desafío de acceso al dispositivo (208) inalámbrico basándose en dicha capacidad de autenticación determinada; y

recibir, a través de la WLAN (202), una petición de acceso desde el dispositivo (208) inalámbrico para acceder a la WLAN, conteniendo la petición de acceso una respuesta al desafío de acceso desde el dispositivo (208) inalámbrico, en el que la respuesta al desafío de acceso es generada por el dispositivo (208) inalámbrico basándose en una clave de autenticación predeterminada; y

una interfaz de control de acceso, AC, configurada para transmitir una petición de autenticación a la red de comunicación celular, y para recibir una respuesta de autenticación generada por la red de comunicación celular basándose en la clave de autenticación predeterminada, en la cual se determina si el aparato de IWF posee información necesaria para autenticar el dispositivo inalámbrico (208) para acceder a la WLAN, en el cual la solicitud de autenticación se transmite a la red de comunicación celular si el aparato de IWF no posee la información necesaria para autenticar el dispositivo inalámbrico (208) para acceder a la WLAN, y en el cual la solicitud de autenticación no se transmite a la red de comunicación celular si se determina que el aparato de IWF ya posee la información necesaria para autenticar el dispositivo inalámbrico para acceder a la WLAN.

2. El aparato de IWF según la reivindicación 1, estando el aparato de IWF adaptado para comunicarse con la WLAN mediante un primer protocolo de transporte, y para comunicarse con la red de comunicación celular mediante un segundo protocolo de transporte.

3. Un procedimiento para autenticar un dispositivo (208) inalámbrico mediante una red de comunicación celular para acceder a una red de área local inalámbrica, WLAN, (202), comprendiendo el procedimiento:

determinar una capacidad de autenticación asociada al dispositivo (208) inalámbrico a partir de una base (210) de datos usando una identidad recibida de dicho dispositivo (208) inalámbrico, en el que dicha capacidad de autenticación comprende bien un algoritmo de autenticación celular y cifrado de voz, CAVE, o bien un algoritmo de acuerdo de clave de autenticación, AKA;

enviar, a través de la WLAN (202), un desafío de acceso al dispositivo (208) inalámbrico basándose en dicha capacidad de autenticación determinada;

generar una petición de acceso por parte del dispositivo (208) inalámbrico basándose en una clave de autenticación predeterminada, conteniendo la petición de acceso una respuesta al desafío de acceso desde el dispositivo (208) inalámbrico;

recibir la petición de acceso desde el dispositivo inalámbrico a través de la WLAN (202) en un aparato (204) de función de interoperación IWF, en comunicación con el dispositivo (208) inalámbrico y la red de comunicación celular;

transmitir una petición de autenticación a la red de comunicación celular por parte del aparato (204) de IWF, si el aparato (204) de IWF no posee información necesaria para autenticar el dispositivo inalámbrico (208) para acceder a la WLAN, en el cual se determina si el aparato (204) de IWF posee la información necesaria para autenticar el dispositivo inalámbrico (208) para acceder a la WLAN (202), y en el cual la petición de autenticación no se transmite a la red de comunicación celular si se determina que el aparato (204) de IWF ya posee la información necesaria para autenticar el dispositivo inalámbrico (208) para acceder a la WLAN (202); y

si el aparato (204) de IWF no posee ya información necesaria para autenticar el dispositivo inalámbrico (208) para acceder a la WLAN (202):

autenticar el dispositivo (208) inalámbrico mediante la red de comunicación celular basándose en la clave de autenticación predeterminada;

y recibir una respuesta de autenticación generada por la red de comunicación celular en base a la clave de autenticación predeterminada.

4. El procedimiento según la reivindicación 3, que comprende además:

conceder acceso inalámbrico, por parte de la WLAN, a la WLAN si la petición de autenticación es autenticada por la red de comunicación celular en base a la clave de autenticación predeterminada.

5. El procedimiento según la reivindicación 3, la petición de acceso se recibe en el aparato de IWF a través de un primer protocolo de transporte.

6. El procedimiento según la reivindicación 3, la petición de autenticación se transmite a la red de comunicación celular a través de un segundo protocolo de transporte.

7. Un producto de programa de ordenador para autenticar un dispositivo inalámbrico (208), por parte de una red de comunicación celular, para acceder a una red de área local inalámbrica, WLAN (202), comprendiendo el producto de programa de ordenador un medio de almacenamiento legible por ordenador que contiene instrucciones en el mismo, las cuales, cuando son ejecutadas en un ordenador, realizan un procedimiento de cualquiera de las reivindicaciones 3 a 6.

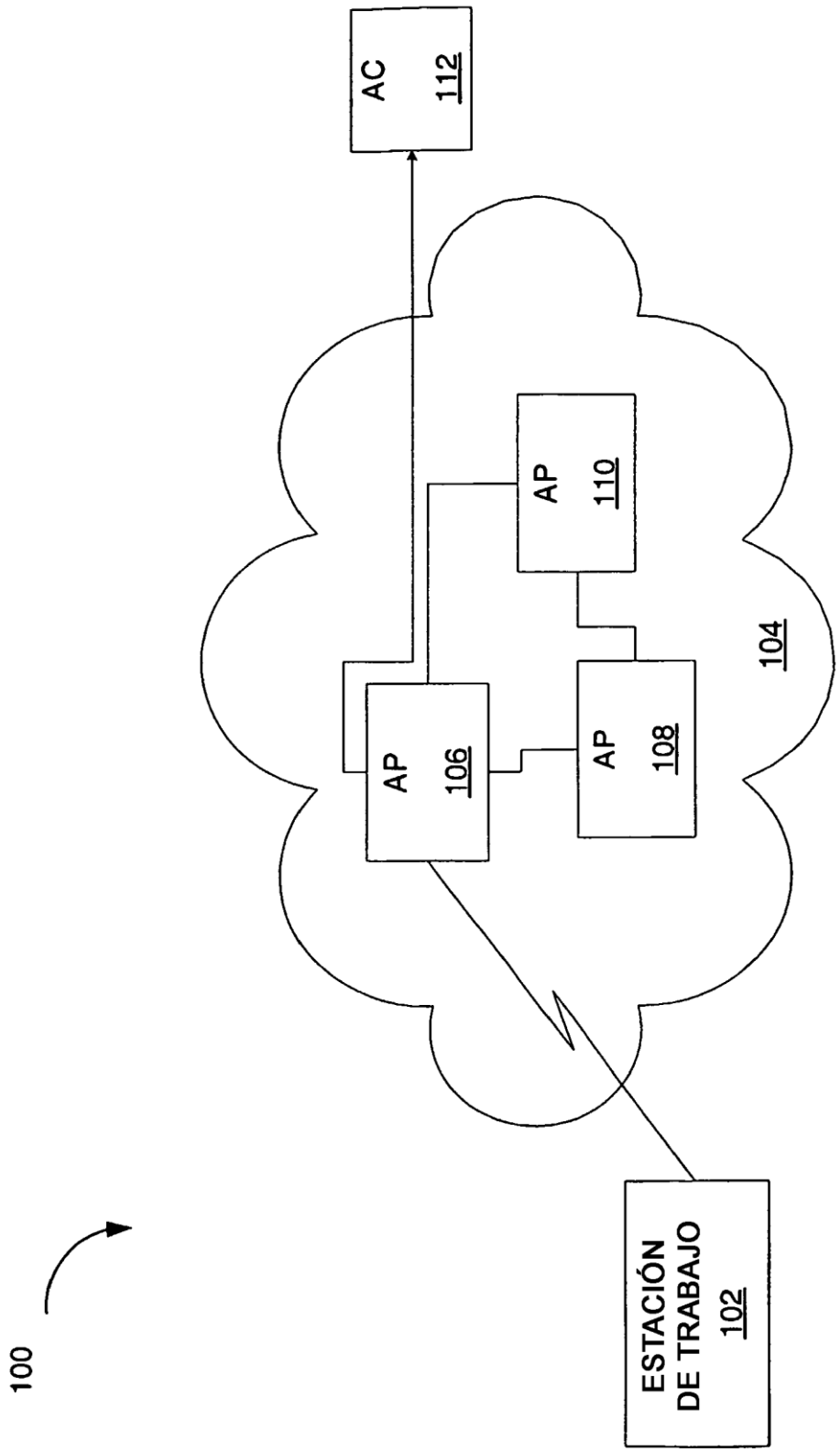

FIG. 1

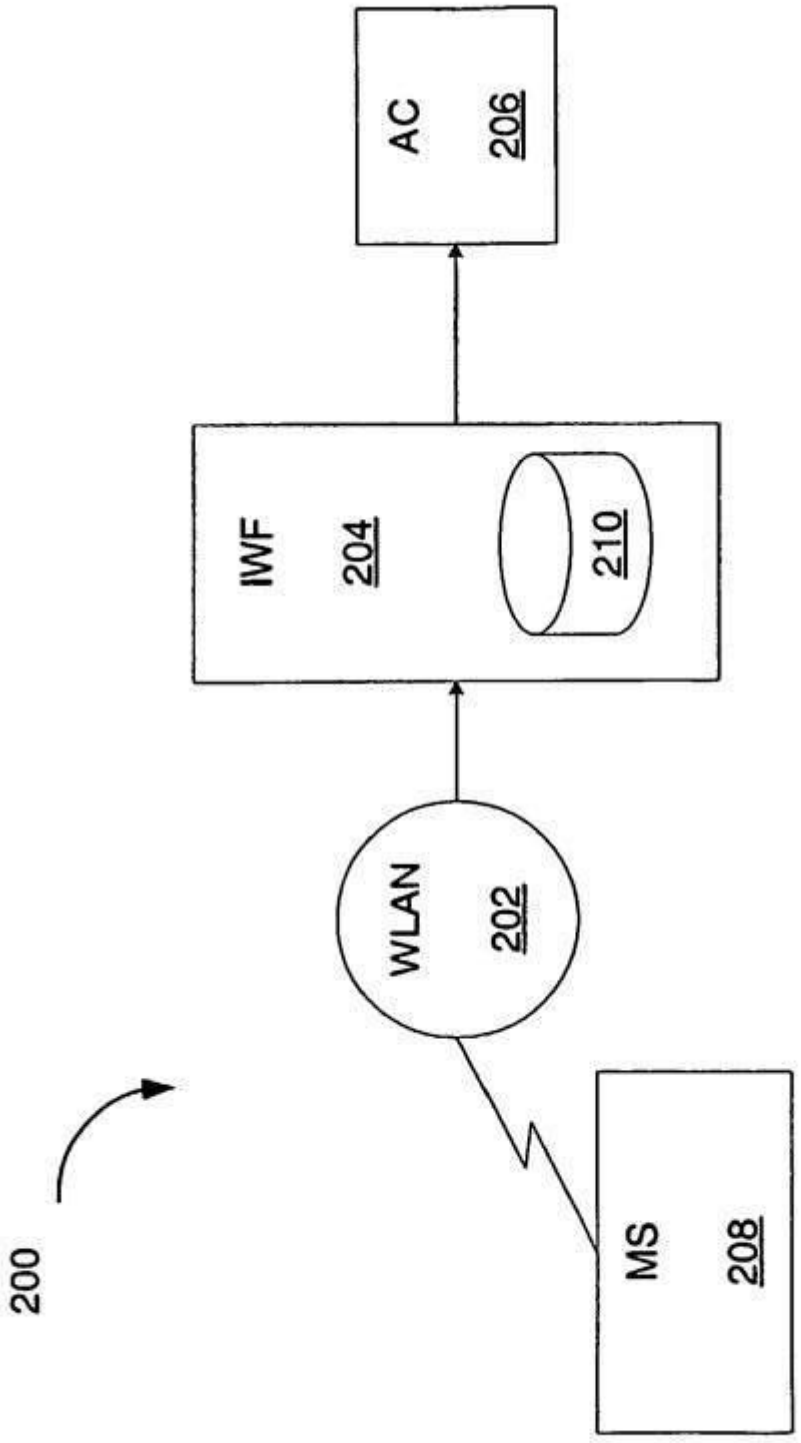

FIG. 2

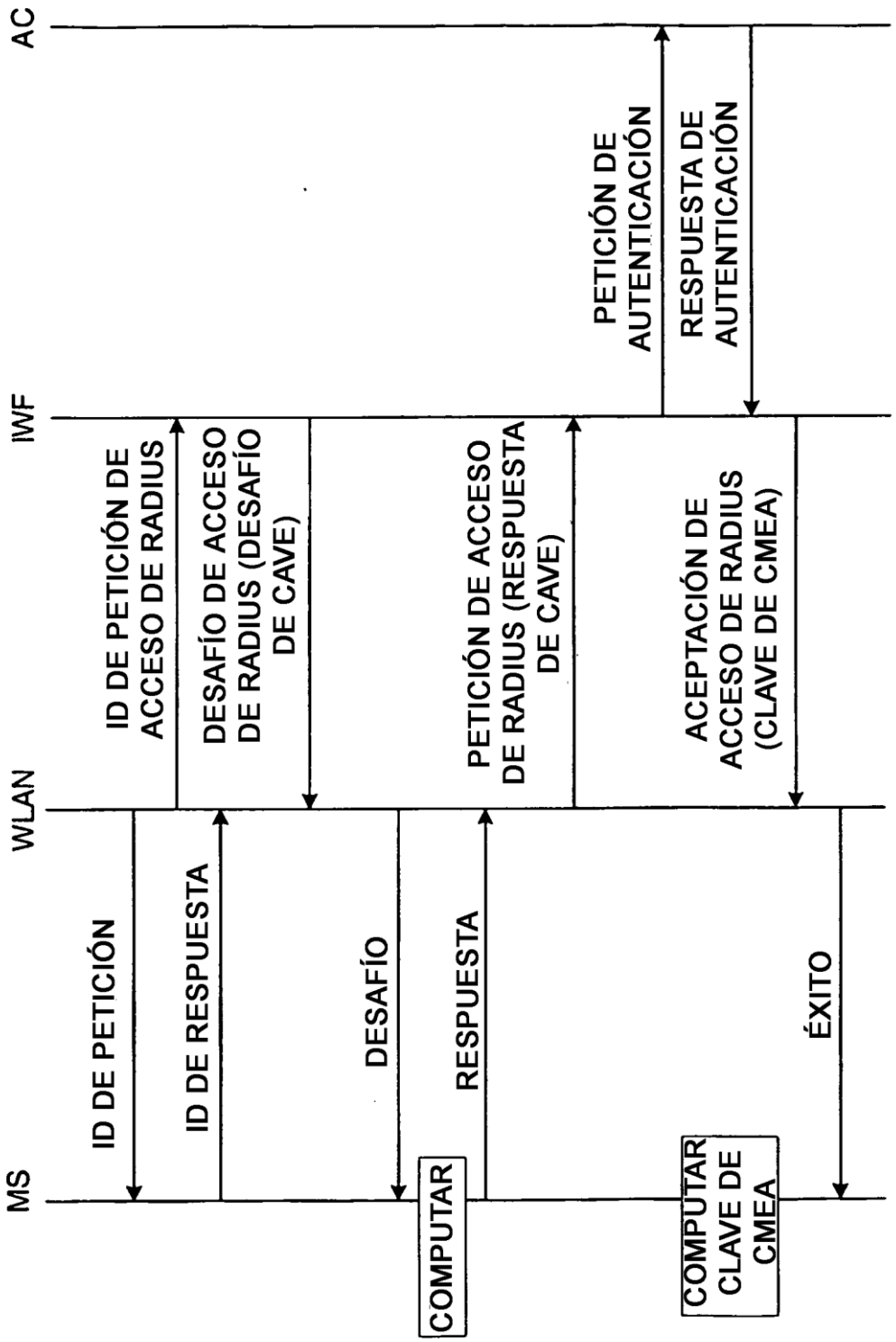
AC
IWF
WLAN
MS
ID DE PETICIÓN DE ACCESO DE RADIUS
DESAFÍO DE ACCESO DE RADIUS (DESAFÍO DE CAVE)
PETICIÓN DE ACCESO DE RADIUS (RESPUESTA DE CAVE)
ACEPTACIÓN DE ACCESO DE RADIUS (CLAVE DE CMEA)
PETICIÓN DE AUTENTICACIÓN
RESPUESTA DE AUTENTICACIÓN
ID DE PETICIÓN
ID DE RESPUESTA
DESAFÍO
RESPUESTA
ÉXITO
COMPUTAR
COMPUTAR CLAVE DE CMEA

FIG. 3

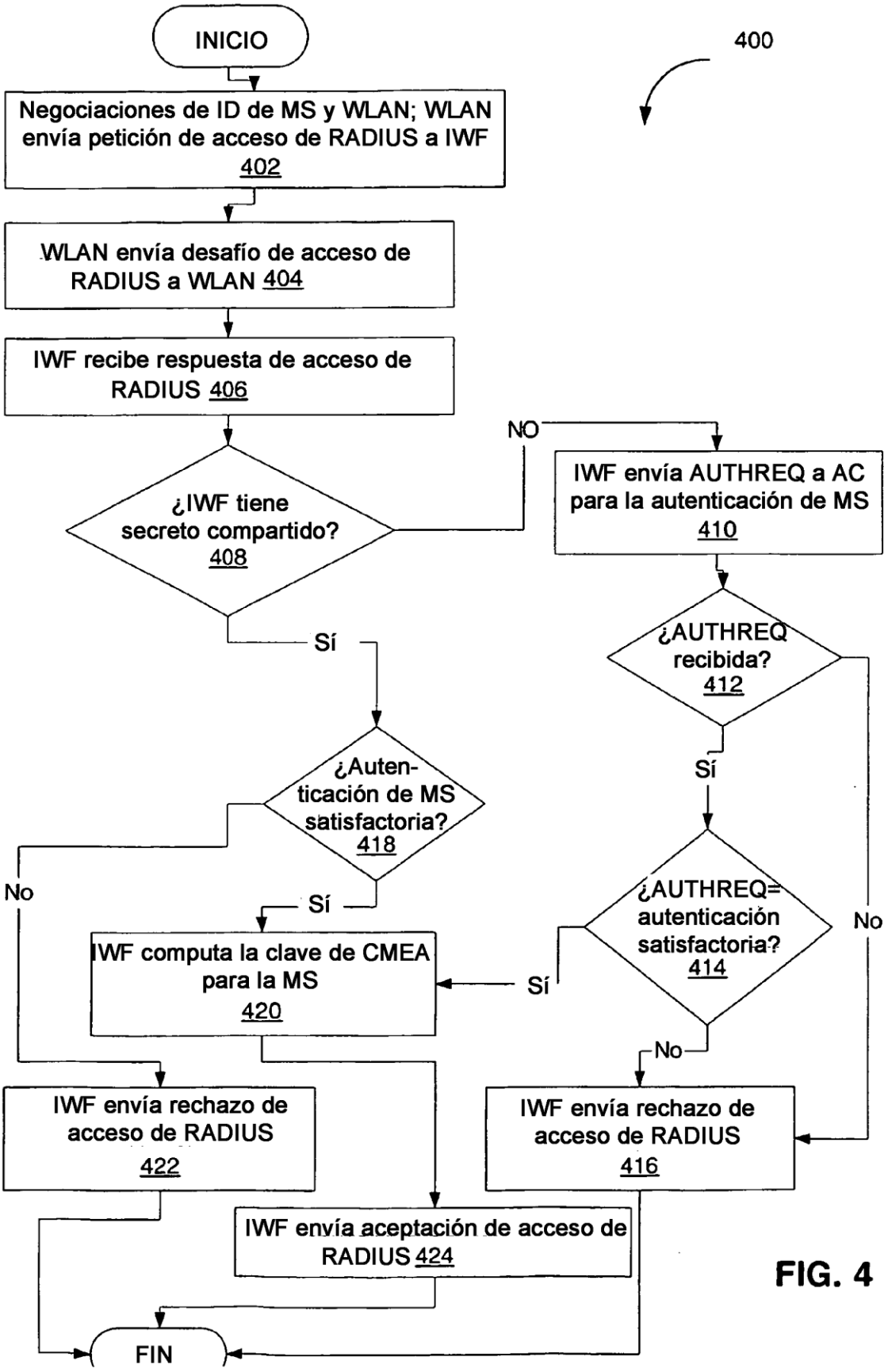
INICIO
400
Negociaciones de ID de MS y WLAN; WLAN envía petición de acceso de RADIUS a IWF 402
WLAN envía desafío de acceso de RADIUS a WLAN 404
IWF recibe respuesta de acceso de RADIUS 406
¿IWF tiene secreto compartido? 408
NO
IWF envía AUTHREQ a AC para la autenticación de MS 410
Sí
¿AUTHREQ recibida? 412
Sí
¿Auten-ticación de MS satisfactoria? 418
No
Sí
¿AUTHREQ= autenticación satisfactoria? 414
No
Sí
IWF computa la clave de CMEA para la MS 420
No
IWF envía rechazo de acceso de RADIUS 422
IWF envía rechazo de acceso de RADIUS 416
IWF envía aceptación de acceso de RADIUS 424
FIN

FIG. 4

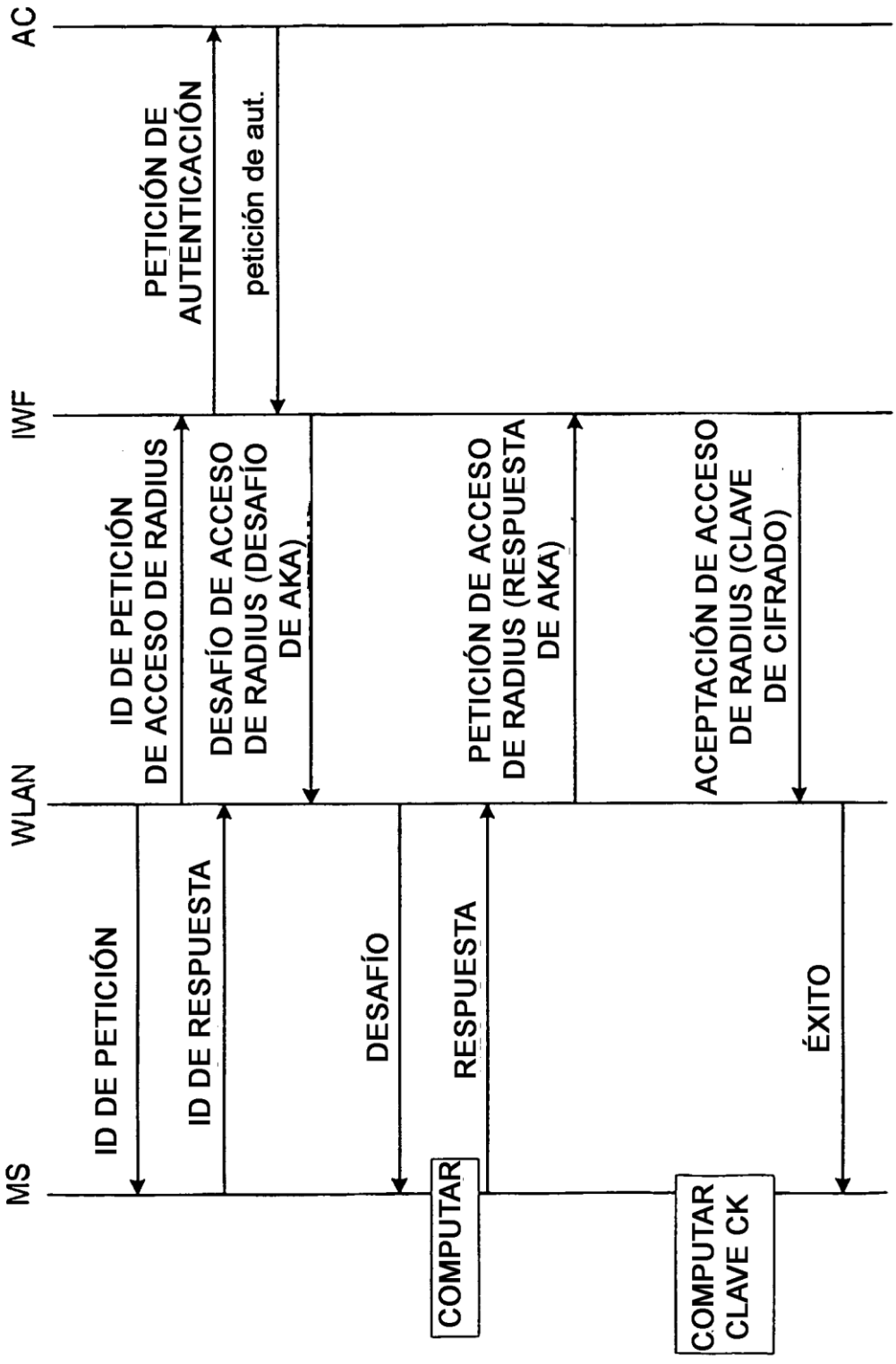
AC
IWF
WLAN
MS
PETICIÓN DE AUTENTICACIÓN
petición de aut.
ID DE PETICIÓN DE ACCESO DE RADIUS
DESAFÍO DE ACCESO DE RADIUS (DESAFÍO DE AKA)
PETICIÓN DE ACCESO DE RADIUS (RESPUESTA DE AKA)
ACEPTACIÓN DE ACCESO DE RADIUS (CLAVE DE CIFRADO)
ID DE PETICIÓN
ID DE RESPUESTA
DESAFÍO
RESPUESTA
ÉXITO
COMPUTAR
COMPUTAR CLAVE CK

FIG. 5

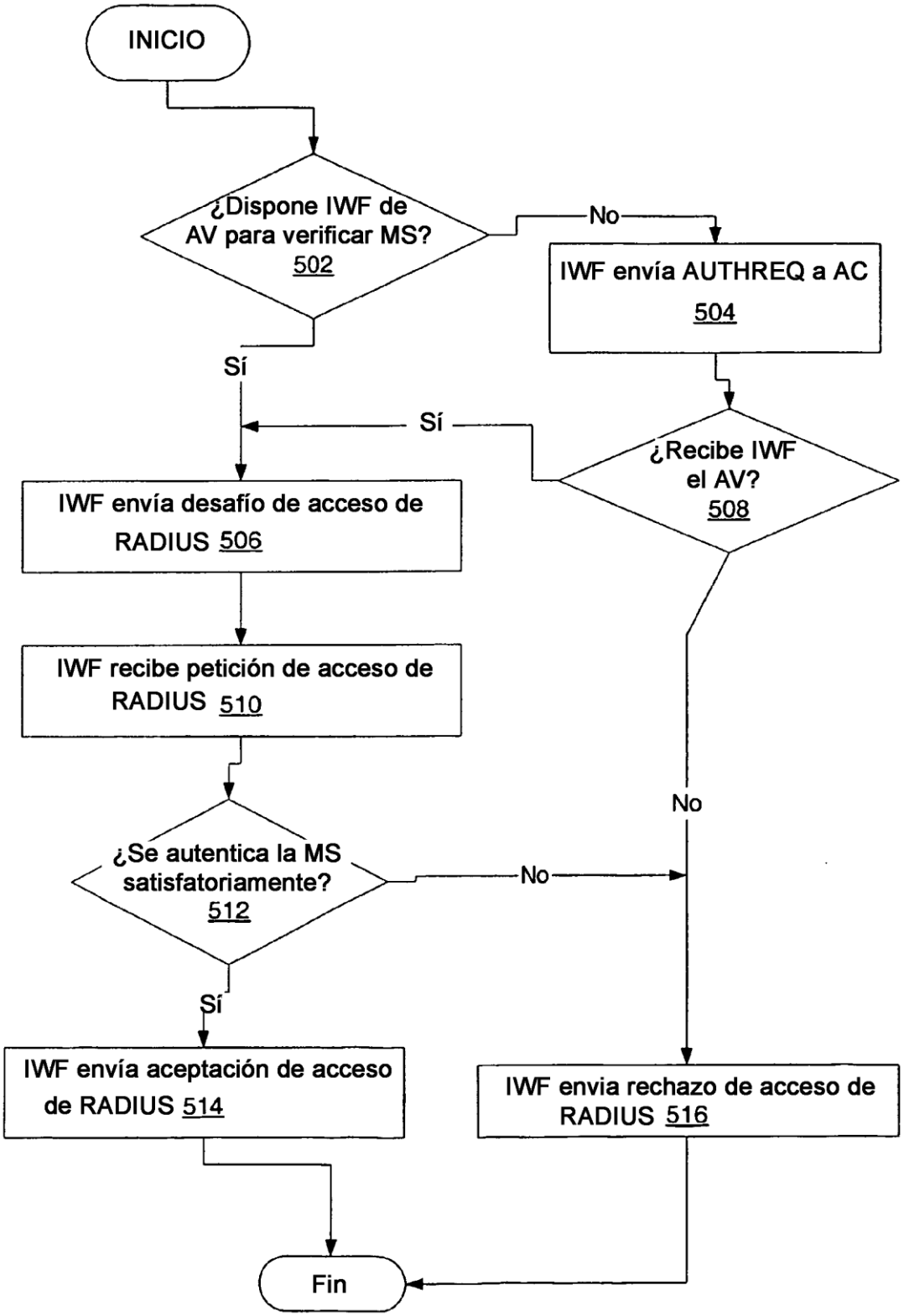
INICIO
¿Dispone IWF de AV para verificar MS? 502
No
IWF envía AUTHREQ a AC 504
Sí
Sí
¿Recibe IWF el AV? 508
IWF envía desafío de acceso de RADIUS 506
IWF recibe petición de acceso de RADIUS 510
No
¿Se autentica la MS satisfatoriamente? 512
No
Sí
IWF envía aceptación de acceso de RADIUS 514
IWF envia rechazo de acceso de RADIUS 516
Fin

FIG. 6

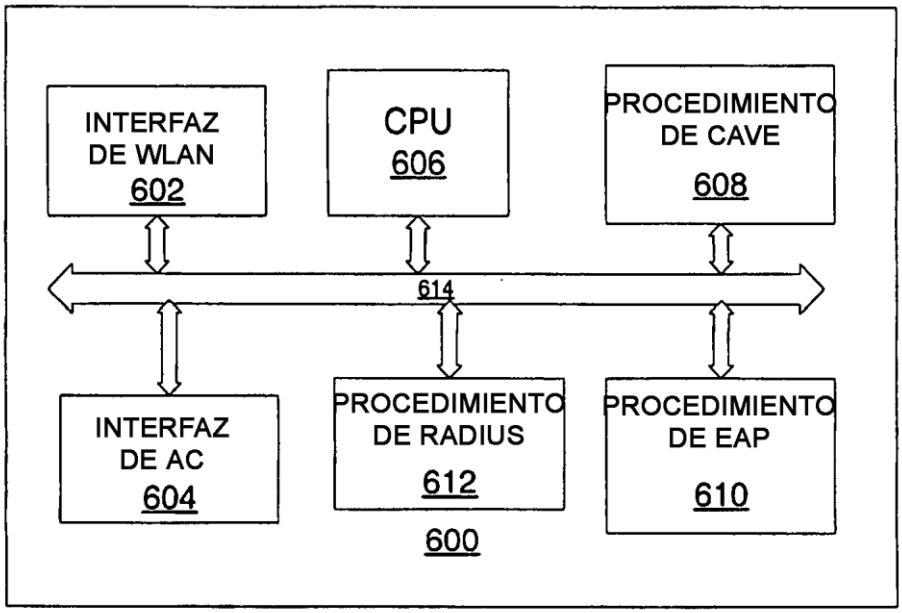
INTERFAZ DE WLAN 602
CPU 606
PROCEDIMIENTO DE CAVE 608
614
INTERFAZ DE AC 604
PROCEDIMIENTO DE RADIUS 612
PROCEDIMIENTO DE EAP 610
600

FIG. 7