(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 969 142**

(51) Int. Cl.:

H04W 48/14 (2009.01)
H04W 12/08 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.04.2010 E 20188777 (5)**

(97) Fecha y número de publicación de la concesión europea: **22.11.2023 EP 3754938**

(54) Título: **Métodos y aparatos para descubrir información de autenticación en un entorno de trabajo en red inalámbrica**

(30) Prioridad:

24.04.2009 US 172597 P
16.07.2009 US 504500

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.05.2024

(73) Titular/es:

MALIKIE INNOVATIONS LIMITED (100.0%)
The Glasshouses GH2, 92 Georges Street Lower
Dun Laoghaire, Dublin A96 VR66, IE

(72) Inventor/es:

MCCANN, STEPHEN y
MONTEMURRO, MICHAEL

(74) Agente/Representante:

ELZABURU, S.L.P

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

DESCRIPCIÓN

Métodos y aparatos para descubrir información de autenticación en un entorno de trabajo en red inalámbrica

Campo de la divulgación

La presente divulgación se refiere en general a comunicaciones en red y, más particularmente, a métodos y aparatos para descubrir información de autenticación en un entorno de trabajo en red inalámbrica.

Antecedentes

Los despliegues de redes inalámbricas, tales como las redes de área local inalámbricas (WLAN), permiten que los terminales inalámbricos accedan a servicios de redes e Internet cuando se encuentran cerca de señales de comunicación inalámbrica de esas redes inalámbricas. Las WLAN disponibles comercialmente, tales como las ubicadas en entornos minoristas u otros establecimientos de acceso público, funcionan en modos no seguros para posibilitar que los terminales inalámbricos establezcan comunicaciones con las WLAN y las redes externas (por ejemplo, redes de proveedores de servicios, redes de operadores, etc.) accesibles mediante esas redes WLAN. Este modo de funcionamiento no seguro permite a los terminales inalámbricos negociar información de conexión y registro con las redes externas mediante comunicaciones de alto nivel utilizando direcciones de protocolo de Internet (IP) y un protocolo de transferencia de hipertexto (HTTP) para posibilitar el registro de los terminales inalámbricos en las redes externas. Sin embargo, estos modos de funcionamiento no seguros que utilizan comunicaciones de alto nivel convierten a las redes externas en vulnerables a ataques maliciosos u otras actividades no deseables destinadas a eludir procedimientos de red creados para el registro ordenado y determinista de terminales inalámbricos.

El P802.11u™/D3.0 del IEEE, "Draft Amendment to Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks·Specific requirements", revela mejoras en el MAC 802.11 que admiten un Interfuncionamiento WLAN con Redes Externas. Las mejoras tienen como objetivo habilitar funcionalidades de capa superior para proporcionar una solución general de extremo a extremo, incluidas la habilitación de transferencia de información desde redes externas, ayudar en la selección de redes y la habilitación de servicios de emergencia.

Compendio

La invención se define en las reivindicaciones adjuntas.

Breve descripción de los dibujos

La figura 1 representa un ejemplo de red de comunicación en la que una pluralidad de ubicaciones de acceso a una red de área local inalámbrica está acoplada comunicativamente a una o más redes.

La figura 2 representa un ejemplo de arquitectura de capas de comunicación.

La figura 3 representa un ejemplo de estructura de datos de parámetros de autenticación (AuP).

La figura 4 representa un ejemplo de estructura de datos de capacidades de un conjunto básico de servicios (BSS) que puede usarse en relación con el ejemplo del proceso de intercambio de mensajería de la figura 6 para descubrir información de autenticación en una red inalámbrica.

La figura 5 representa un ejemplo de estructura de datos de información de autenticación que puede usarse en relación con el ejemplo del proceso de intercambio de mensajería de la figura 6 para descubrir información de autenticación en una red inalámbrica.

La figura 6 representa un ejemplo de proceso de intercambio de mensajería que puede usarse para descubrir información de autenticación en una red inalámbrica.

La figura 7 representa otro ejemplo de estructura de datos de capacidades de un conjunto básico de servicios (BSS) que puede usarse en relación con el ejemplo del proceso de intercambio de mensajería de la figura 9 para descubrir información de autenticación en una red inalámbrica.

La figura 8 representa otro ejemplo de estructura de datos de información de autenticación que puede usarse en relación con el ejemplo del proceso de intercambio de mensajería de la figura 9 para descubrir información de autenticación en una red inalámbrica.

La figura 9 representa otro ejemplo de proceso de intercambio de mensajería que puede usarse para descubrir información de autenticación en una red inalámbrica.

La figura 10 representa un ejemplo de terminal inalámbrico que puede usarse para implementar los ejemplos de métodos y aparatos descritos en el presente documento.

La figura 11 representa un ejemplo de punto de acceso inalámbrico que puede usarse para implementar los ejemplos de métodos y aparatos descritos en el presente documento.

La figura 12 representa un ejemplo de diagrama de flujo representativo de instrucciones legibles por ordenador que pueden usarse para descubrir información de autenticación en una red inalámbrica.

Descripción detallada

Aunque en lo sucesivo se revelan ejemplos de métodos y aparatos que incluyen, entre otros componentes, *software* ejecutado en *hardware*, cabe señalar que dichos métodos y aparatos son meramente ilustrativos y no deben considerarse limitativos. Por ejemplo, se contempla que cualquiera o la totalidad de estos componentes de *hardware* y *software* pudiera materializarse exclusivamente en *hardware*, exclusivamente en *software*, exclusivamente en *firmware* o en cualquier combinación de *hardware*, *software* y/o *firmware*. Por consiguiente, aunque en lo sucesivo se describen ejemplos de métodos y aparatos, las personas con conocimientos habituales en la técnica apreciarán fácilmente que los ejemplos proporcionados no son la única forma de implementar dichos métodos y aparatos.

Los ejemplos de métodos y aparatos descritos en el presente documento pueden ser utilizados por un terminal inalámbrico para descubrir información de autenticación (AI) y parámetros de autenticación (AuP) necesarios para autenticar el terminal inalámbrico con vistas a una conexión a una red inalámbrica. Los ejemplos de métodos y aparatos descritos en el presente documento se pueden usar en relación con dispositivos de comunicación móviles, dispositivos informáticos móviles o cualquier otro dispositivo capaz de comunicarse de forma inalámbrica con una red inalámbrica. Dichos dispositivos, también denominados terminales, terminales inalámbricos o equipo de usuario (UE), pueden incluir teléfonos móviles inteligentes (por ejemplo, un teléfono inteligente BLACKBERRY®), asistentes digitales personales (PDA) inalámbricos, ordenadores portátiles/de tipo *notebook*/de tipo *netbook* con adaptadores inalámbricos, etc. Los ejemplos de métodos y aparatos se describen en el presente documento en relación con el estándar de comunicación de red de área local inalámbrica (WLAN) conocido como 802.11 del IEEE® (Instituto de Ingenieros Eléctricos y Electrónicos), que, entre otras cosas, define el interfuncionamiento con redes externas. Sin embargo, los ejemplos de métodos y aparatos pueden implementarse adicional o alternativamente en relación con otros estándares de comunicación inalámbrica, incluidos otros estándares de WLAN, estándares de red de área personal (PAN), estándares de red de área amplia (WAN) o estándares de comunicación celular.

Aunque los ejemplos de métodos y aparatos descritos en el presente documento se pueden implementar en cualquier entorno que proporcione acceso de WLAN para conectividad con redes, los ejemplos de métodos y aparatos se pueden implementar ventajosamente en ubicaciones o entornos de acceso a WLAN en los que se espera que uno o más usuarios que lleven sus respectivos terminales inalámbricos se conecten y desconecten de forma frecuente de una WLAN cuando entren y salgan de las ubicaciones o entornos de acceso a WLAN. Las ubicaciones o entornos de WLAN en ocasiones se conocen como "puntos calientes" en referencia a una ubicación o entorno que está dentro del alcance de la comunicación de señales de WLAN. Tales ejemplos de ubicaciones o entornos de WLAN incluyen cafeterías, tiendas minoristas, instalaciones educativas, entornos de oficinas, aeropuertos, estaciones y vehículos de transporte público, hoteles, etc.

La experiencia del usuario asociada a técnicas o estándares conocidos para conectar un terminal inalámbrico a un punto de acceso (AP) de un punto caliente de WLAN a menudo puede resultar frustrante. Por ejemplo, a menudo es necesario descubrir correctamente el identificador de la red de radiocomunicaciones (por ejemplo, un parámetro del 802.11 del IEEE® Identificador de Conjunto de Servicios (SSID)), y también puede ser necesario descubrir AI y AuPs particulares (elegidos por el propietario/proveedor del punto caliente) que se requieren para conectarse a la red soportada por WLAN (por ejemplo, una red externa) que está detrás del AP del punto caliente.

En algunos casos, puede ser suficiente con que un terminal inalámbrico proporcione un Identificador de Dirección de Red (NAI) que indique la identidad del usuario al AP para proceder con la autenticación y situar el terminal inalámbrico en comunicación con la red externa por detrás del AP. En otros casos, es posible que sea necesario proporcionar a un terminal inalámbrico, por ejemplo, una tarjeta de módulo de identidad de abonado (SIM) para proceder con la autenticación. Estas situaciones a menudo crean experiencias de usuario frustrantes cuando los terminales inalámbricos no logran conectarse a ubicaciones de acceso de WLAN debido a la pérdida o falta de información de autenticación. En otras situaciones, incluso cuando los usuarios sí conocen la información de autenticación particular que debe proporcionarse, el proceso de proporcionar dicha información de autenticación desde el terminal inalámbrico al AP puede ser engorroso (por ejemplo, mediante introducción manual).

En referencia particularmente a ubicaciones de acceso de WLAN (o puntos calientes de WLAN) que funcionan bajo el estándar de comunicación inalámbrica 802.11 del IEEE®, este estándar actualmente carece de disposiciones para proporcionar a terminales inalámbricos los detalles necesarios relacionados con la autenticación sobre las redes soportadas por WLAN (por ejemplo, redes externas) a las que están conectados los AP de WLAN. Por lo tanto, un usuario que desea acceder a la red generalmente debe configurar de forma manual algunos aspectos de un terminal inalámbrico compatible con el 802.11 del IEEE®, a menos que el AP esté funcionando de manera abierta y no segura, en cuyo caso no se necesitan AuPs para acceder a la red. A medida que la tecnología de WLAN se vaya desplegando en diferentes lugares, un acceso abierto no seguro atraerá cada vez a menos proveedores de puntos calientes de WLAN. Los ejemplos de métodos y aparatos descritos en el presente documento se pueden usar para posibilitar que

terminales inalámbricos descubran u obtengan requisitos de AI y AuP asociados a puntos calientes de WLAN, reduciendo o eliminando así sustancialmente la dependencia de la participación del usuario cuando se accede a servicios inalámbricos y, por lo tanto, mejorando las experiencias del usuario con dichos servicios. A continuación se describen en relación con la figura 1 ejemplos de escenarios en los que pueden usarse ventajosamente los ejemplos de métodos y aparatos.

Aunque los ejemplos de métodos y aparatos se describen en el presente documento en relación con la posibilitación de que los terminales inalámbricos descubran requisitos de AI y AuP de APs, los ejemplos de métodos y aparatos también se pueden usar para permitir que APs descubran requisitos de AI y AuP de terminales inalámbricos. Por ejemplo, cuando un terminal inalámbrico ya está conectado a una red externa (por ejemplo, la red de un proveedor de servicios inalámbricos mediante un enlace de datos celular, una PAN mediante un enlace de BLUETOOTH®, etc.), se puede configurar un AP para descubrir requisitos de AI y AuP asociados a esa red externa consultando al terminal inalámbrico con el uso de los ejemplos de técnicas descritos en el presente documento. Los ejemplos de métodos y aparatos descritos en el presente documento también se pueden usar en relación con entornos de trabajo en redes en malla para posibilitar que un primer AP descubra requisitos de AI y AuP asociados a un segundo AP consultando a un terminal inalámbrico que está conectado directamente al segundo AP ó conectado indirectamente al segundo AP mediante otro u otros terminales inalámbricos. De esta manera, el primer AP puede conectarse a una red externa asociada al segundo AP si el primer AP tiene los valores de AI y/o AuP requeridos.

Volviendo ahora a la figura 1, se muestra un ejemplo de red 100 de comunicación en la que se pueden implementar los ejemplos de métodos y aparatos descritos en el presente documento. Como se muestra en la figura 1, el ejemplo de red 100 de comunicación incluye una pluralidad de ubicaciones 102a-c de acceso de WLAN que proporcionan acceso a una o más redes (por ejemplo, redes soportadas por WLAN ó redes externas) mediante puntos 104a-c de acceso respectivos. En el ejemplo ilustrado, el punto de acceso (AP) 104a proporciona acceso a una red privada 106a, que a su vez proporciona acceso a una red de proveedor de servicios de suscripción A (SSPN-A) 108a. También en el ejemplo ilustrado, el AP 104b proporciona acceso a una red privada 106b, que a su vez proporciona acceso a una red de proveedor de servicios de suscripción B (SSPN-B) 108b. Las SSPN 108a-b pueden ser propiedad de y/o pueden ser explotadas por proveedores de servicios de suscripción de datos, proveedores de servicios de suscripción de Internet, proveedores de servicios de suscripción de medios (por ejemplo, audio/vídeo), proveedores de servicios de suscripción de comunicaciones inalámbricas o cualquier combinación de los mismos.

El AP 104c proporciona acceso a una red pública 110, que se muestra proporcionando acceso a Internet 112. Aunque no se muestra, cada uno de los AP 104a-c está provisto de una estación de AP (es decir, una STA de AP), que es la interfaz o componente, tal como un adaptador de red o una tarjeta de interfaz de red (NIC), que se conecta a un medio inalámbrico.

Cada una de las ubicaciones 102a-c de acceso de WLAN puede estar asociada a conjuntos diferentes de AuPs requeridos de un terminal inalámbrico 114 para obtener acceso a las redes 106a, 106b y/o 110 a través de los AP 104a-c. Estos AuP pueden ser seleccionados por propietarios u operadores respectivos de las redes 106a, 106b y 110. Los AuP pueden seleccionarse en función de diferentes factores tales como, por ejemplo, niveles de seguridad y/u objetivos comerciales deseados. Por ejemplo, si la ubicación 102a de acceso de WLAN es un aeropuerto, la red privada 106a puede requerir relativamente más parámetros de autenticación de un terminal inalámbrico que los que requeriría un establecimiento minorista para minimizar o prevenir vulnerabilidades en redes informáticas de aeropuertos/aerolíneas. De manera adicional o alternativa, las redes privadas 106a-b pueden tener términos de acuerdo contractual diferentes con proveedores respectivos de entre los proveedores de servicios de las SSPN 108a-b, lo que deriva en conjuntos diferentes de requisitos de AuP. Estos AuP diferentes pueden estar relacionados con estructuras diferentes de cobro/tarificación de acceso a la red o acuerdos diferentes de itinerancia de los dispositivos inalámbricos. Algunas redes, tales como la red pública 110, pueden requerir menos AuPs ó ninguno.

En cualquier caso, los ejemplos de métodos y aparatos descritos en el presente documento se pueden usar ventajosamente para posibilitar que el terminal inalámbrico 114 se mueva entre diferentes ubicaciones de acceso de WLAN (por ejemplo, las ubicaciones 102a-c de acceso de WLAN) sin requerir que el terminal inalámbrico 114 esté preconfigurado o se haya precargado con diferentes conjuntos o listas de requisitos AuP asociados al acceso a esas ubicaciones de acceso de WLAN diferentes. De esta manera, el terminal inalámbrico 114 puede recibir o adquirir dinámicamente AuPs requeridos de cualquier AP con el que no se haya encontrado antes o cuyos AuP requeridos hayan cambiado desde una sesión de acceso anterior entre el terminal inalámbrico 114 y el AP. En los ejemplos ilustrados descritos en el presente documento, el terminal inalámbrico 114 incluye una estación que no es AP (es decir, una STA que no es AP), mientras que cada uno de los AP 104a-c incluye una STA de AP respectiva.

Como se muestra de manera general en relación con la ubicación 102a de acceso de WLAN, el terminal inalámbrico 114 puede recuperar AI requerida (incluidos los AuP) del AP 104a transmitiendo un mensaje 116 de solicitud de AI y recibiendo un mensaje 118 de respuesta de AI que incluye identificadores que indican uno o más AI y/o AuPs requeridos. En el ejemplo ilustrado, el mensaje 116 de solicitud de AI y el mensaje 118 de respuesta de AI se pueden intercambiar antes de un proceso de autenticación usando un protocolo de consulta predefinido tal como un formato de consulta/respuesta del Servicio de Anuncios Genérico (GAS). El formato de consulta del GAS, tal como se define en el 802.11 del IEEE®, posibilita a STAs que no son AP (por ejemplo, el terminal inalámbrico 114) descubrir la disponibilidad de información (por ejemplo, capacidades de AP, AI, AuPs, etc.) relacionada con servicios de red

deseados. Alternativamente, el mensaje 116 de solicitud de AI y el mensaje 118 de respuesta de AI se pueden intercambiar durante un proceso de autenticación de acuerdo con, por ejemplo, disposiciones del estándar 802.11 del IEEE® que involucra comunicaciones seguras de toma de contacto que intercambian información de forma segura para garantizar la confidencialidad de dicha información.

Volviendo a la figura 2, se muestra un ejemplo de arquitectura 200 de capas de comunicación con siete capas que pueden implementarse de acuerdo con el ampliamente conocido Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI). En el ejemplo ilustrado, la arquitectura 200 de capas de comunicación incluye una capa 202 de enlace de datos, que incluye una subcapa 204 de control de acceso a medios (MAC). Para posibilitar que los terminales inalámbricos (por ejemplo, el terminal inalámbrico 114 de la figura 1) recuperen AI y AuPs de AP inalámbricos (por ejemplo, los AP inalámbricos 102a-c de la figura 1), los ejemplos de métodos y aparatos descritos en el presente documento se pueden usar para llevar a cabo operaciones o procesos que incluyen mensajería 206 de AI (por ejemplo, el mensaje 116 de solicitud de AI y el mensaje 118 de respuesta de AI de la figura 1) en la subcapa 204 de MAC. Es decir, un terminal inalámbrico puede recuperar valores de AI y/o valores de AuP requeridos de una memoria u otro *hardware* del terminal inalámbrico usando uno o más procesos de recuperación de valores de autenticación llevados a cabo por el terminal inalámbrico en la subcapa 204 de MAC sin necesidad de permitir que el(los) proceso(s) de recuperación de valores de autenticación lleve(n) a cabo operaciones en o por encima de una capa de protocolo de internet (IP) (por ejemplo, una capa 208 de red) ni necesidad de proporcionar de otro modo al(a los) proceso(s) de recuperación de valores de autenticación acceso a la capa de IP.

Algunas técnicas de autenticación que utilizan el protocolo de transferencia de hipertexto (HTTP) u otros procesos de protocolo de internet (IP) para mostrar sitios web de inicio de sesión y/o sitios web de términos y condiciones requieren establecer una conexión entre un terminal inalámbrico y un AP inalámbrico en una o más de las capas entre, y que incluyen, una capa 208 de red (por ejemplo, una capa de protocolo de internet (IP)) y una capa 210 de aplicación de la arquitectura 200 de capas de comunicación. Sin embargo, dichas técnicas a menudo pueden crear ciertas vulnerabilidades en redes soportadas por WLAN (por ejemplo, una de las redes privadas 106a-b) de las cuales se pueden aprovechar de manera dañina usuarios maliciosos o revoltosos. Es decir, los usuarios pueden acceder a recursos de red usando técnicas de elusión de autenticación basadas en comunicaciones de IP ó HTTP u otros protocolos de comunicación en o por encima de la capa 208 de red. La mensajería 206 de AI utilizada en relación con los ejemplos de métodos y aparatos descritos en el presente documento puede reducir sustancialmente o eliminar dichas vulnerabilidades mediante el uso de un proceso de autenticación que implique operaciones en una conexión de red de la subcapa de MAC, lo que hace relativamente más difícil o imposible para los usuarios acceder a dichos recursos de red de bajo nivel con el fin de eludir procesos de autenticación.

Además, las técnicas de autenticación implementadas en o por encima de la capa 208 de red requieren relativamente más potencia de procesamiento de un terminal inalámbrico que la implementación de procesos en la subcapa 204 de MAC. Los terminales inalámbricos móviles (por ejemplo, el terminal inalámbrico 114 de la figura 1) tales como los teléfonos móviles inteligentes, los PDA, etc. a menudo tienen ciclos de procesador y energía eléctrica disponible relativamente limitados en comparación con los dispositivos informáticos de ubicación fija alimentados con fuentes de electricidad de corriente alterna (AC). Por lo tanto, los ejemplos de métodos y aparatos descritos en el presente documento se pueden usar ventajosamente para configurar, diseñar o concebir de otro modo terminales inalámbricos móviles para que funcionen de manera más eficiente (es decir, hacer más con menos ciclos de procesador) al tiempo que minimizando el uso de energía de la batería. Es decir, los ejemplos de métodos y aparatos descritos en el presente documento se pueden usar ventajosamente para promover diseños de terminales inalámbricos móviles que consuman relativamente menos energía y funcionen relativamente de forma más eficiente. Por ejemplo, las operaciones de recursos de bajo nivel en la subcapa 204 de MAC requieren relativamente menos recursos del sistema que las operaciones exigentes en cuanto a la interfaz de usuario y exigentes en cuanto al sistema operativo (OS) (por ejemplo, operaciones de navegadores web) en la capa 210 de aplicación.

Otro ejemplo de ventaja de la mensajería 206 de AI en la subcapa 204 de MAC es que un terminal inalámbrico, sin la participación del usuario o con una participación mínima del mismo, puede determinar si conectarse a un AP particular es siquiera una opción basándose en la AI y/o los AuP requeridos anunciados por ese AP y que pueden ser solicitados por la red detrás del AP. Por ejemplo, si el AP 104a indica que requiere un identificador de tarjeta SIM, y el terminal inalámbrico 114 no tiene una tarjeta SIM que almacene un código particular, al usuario del terminal inalámbrico 114 no se le da la opción de descubrir que el AP está disponible para la conexión. Así, durante un proceso de descubrimiento de WLAN iniciado por el usuario del terminal inalámbrico 114, el terminal inalámbrico 114 no devuelve el SSID del AP 104a porque no sería posible que el terminal inalámbrico 114 se conectara al AP 104a sin una tarjeta SIM. Tal implementación reduciría sustancialmente o eliminaría la frustración del usuario ya que el usuario no se involucraría en ningún intento de conectarse cuando dicha conexión es imposible según las credenciales del usuario. En tal ejemplo, el requisito de la tarjeta SIM puede venir impuesto por un proveedor de servicios inalámbricos que posee o explota la SSPN-A 108a para, por ejemplo, garantizar que solamente terminales inalámbricos (por ejemplo, teléfonos inteligentes) asociados a su servicio puedan obtener acceso a la red. Es decir, cuando el terminal inalámbrico 114 determina que sí tiene el requisito de tarjeta SIM, muestra el SSID del AP 104a ya que tiene la capacidad de ser autenticado por el AP 104a. Aunque en relación con el ejemplo anterior y en otros ejemplos descritos a continuación se utiliza un SSID, un AP puede configurarse alternativamente para difundir un Identificador de Conjunto Ampliado y Homogéneo de Servicios (HESSID). Un HESSID incluye un SSID asociado a un AP particular y una identificación de

red correspondiente a una SSPN admitida. Por ejemplo, si el AP 104a de la figura 1 estuviera configurado para difundir un HESSID, incluiría el SSID del AP 104a y la identificación de red correspondiente a la SSPN-A 108a.

La figura 3 representa un ejemplo de estructura 300 de datos de parámetros de autenticación (AuP) mostrada en formato de tabla para facilitar su descripción. El ejemplo de estructura 300 de datos de AuP incluye una pluralidad de nombres 302 de AuP, cada uno de los cuales está asociado a uno respectivo de una pluralidad de identificadores 304 de AuP. En el ejemplo ilustrado, los identificadores 304 de AuP no son en sí mismos valores de AuP, sino que son, en cambio, identificadores usados por AP inalámbricos (por ejemplo, los AP inalámbricos 104a-c de la figura 1) para indicar a terminales inalámbricos (por ejemplo, el terminal inalámbrico 114 de la figura 1) qué valores de AuP deben tener los terminales inalámbricos para autenticarse y establecer comunicaciones de red mediante los AP inalámbricos. Por ejemplo, según la estructura 300 de datos de AuPs, se usa un ID de AuP de NAI (es decir, ID de AuP = 1) para indicar al terminal inalámbrico 114 que el terminal inalámbrico 114 debe proporcionar un valor de AuP igual a la identidad de un usuario asociada al terminal inalámbrico 114.

Los identificadores 304 de AuP identifican AuPs que normalmente implican una autenticación en la subcapa 204 de MAC. Sin embargo, en algunos ejemplos de implementación, algunos AuP pueden implicar solicitar una entrada de contraseña de usuario o entrada de PIN. En el ejemplo ilustrado, la estructura 300 de datos de AuPs incluye un parámetro de indicador de dirección de red (NAI) (por ejemplo, la identidad de un usuario de terminal inalámbrico), un parámetro de materia [*subject*] de servidor, un parámetro de red de área de almacenamiento (SAN) de servidor y entradas reservadas para parámetros específicos del proveedor. En otros ejemplos de implementación, la estructura 300 de datos de AuP puede estar provista de AuPs en un número menor, mayor y/o diferentes.

Los propietarios u operadores de redes soportadas por WLAN pueden seleccionar uno o más de los AuP en la estructura 300 de datos de AuP como AuP necesarios para permitir la autenticación y la conexión a sus redes soportadas por WLAN. En algunos ejemplos de implementación, el terminal inalámbrico 114 puede configurarse para almacenar una lista completa de los AuP en la estructura 300 de datos de AuP, mientras que en otros ejemplos de implementación, el terminal inalámbrico 114 puede configurarse para almacenar algunos seleccionados de los AuP. Por ejemplo, si el terminal inalámbrico 114 es proporcionado por un proveedor de servicios inalámbricos de telefonía móvil que elige permitir que sus dispositivos se conecten de forma inalámbrica solo a puntos calientes de WLAN patrocinados o aprobados usando valores de identificación de tarjetas SIM, el terminal inalámbrico 114 puede almacenar solo un identificador de AuP de NAI (ID de AuP = 1) asociado a la estructura 300 de datos de AuP además de un identificador de *hardware* de seguridad que se analiza posteriormente en relación con la figura 5. En un ejemplo de implementación de este tipo, identificador de AuP de NAI se refiere a requerir un valor de identificación de usuario, e identificador de *hardware* de seguridad se refiere a requerir un valor de identificación de tarjeta SIM (u otro valor de identificación correspondiente a otro elemento de *hardware* de seguridad (por ejemplo, una tarjeta SIM universal). (USIM) o un elemento seguro de comunicación de campo cercano (NFC)).

El terminal inalámbrico 114 se puede configurar para descubrir uno o más de los AuP en la estructura 300 de datos de AuP usando el ejemplo de técnica de descubrimiento de AI que se describe más adelante en relación con las figuras 4-6, o usando el ejemplo de técnica de descubrimiento de AI que se describe más adelante en relación con las figuras 7-9.

Como se analiza más adelante en relación con las figuras 4-6, un AP puede configurarse para anunciar sus requisitos de autenticación en forma de dos tipos independientes de capacidades de autenticación, el primero de los cuales implica que un terminal inalámbrico lleve a cabo operaciones o procesos en o por encima de la capa 208 de red (figura 2) y el segundo de los cuales implica que el terminal inalámbrico lleve a cabo operaciones en la subcapa 204 de MAC (o la capa 202 de enlace de datos) (figura 2). Las operaciones en o por encima de la capa 208 de red (por ejemplo, operaciones de IP en la capa 208 de red, operaciones de HTTP en la capa 210 de aplicación, etc.) pueden incluir obtener una confirmación de que un usuario aceptó términos y condiciones particulares y/u obtener credenciales de nombre de usuario y/o contraseña de inicio de sesión utilizando una página de inicio de sesión que se muestra con una operación de redireccionamiento de un localizador uniforme de recursos (URL).

En ejemplos de implementación alternativos, como se analiza posteriormente en relación con las figuras 7-9, un AP se puede configurar para anunciar una capacidad de autenticación única que puede indicar requisitos de autenticación que implican operaciones en la subcapa 204 de MAC (o la capa 202 de enlace de datos) y requisitos de autenticación que implican operaciones en o por encima de la capa 208 de red.

Pasando ahora a las figuras 4-6, la figura 4 representa un ejemplo de estructura 400 de datos de capacidades de conjunto básico de servicios (BSS), la figura 5 representa un ejemplo de estructura 500 de datos de información de autenticación (AI) de capa 2, y la figura 6 representa un ejemplo de proceso de mensajería (por ejemplo, que puede usarse para implementar la mensajería 206 de AI de la figura 2) para descubrir AI en un entorno de WLAN (por ejemplo, una de las ubicaciones 102a-c de acceso de WLAN de la figura 1). El ejemplo de proceso de mensajería de la figura 6 se puede usar en relación con la información de la estructura 400 de datos de capacidades de BSS y la estructura 500 de datos de AI de capa 2 para implementar un ejemplo de técnica de descubrimiento de AI que implica el uso de una primera consulta de AI para descubrir requisitos de AI asociados a operaciones en la subcapa 204 de MAC (figura 2) y una segunda consulta de AI para descubrir requisitos de AI asociados a operaciones en o por encima de la capa 208 de red (figura 2).

El ejemplo de estructura 400 de datos de capacidades de BSS almacena IDs 402 de CAP (es decir, identificadores de capacidad) de APs y/o terminales inalámbricos. En el ejemplo ilustrado, la estructura 400 de datos de capacidades de BSS incluye una entrada 404 de capacidad de información de tipo de autenticación de capa 3+ y una entrada 406 de capacidad de información de tipo de autenticación de capa 2, cada una asociada a uno respectivo de los ID 402 de CAP. La entrada 404 de capacidad de información de tipo de autenticación de capa 3+ y la entrada 406 de capacidad de información de tipo de autenticación de capa 2 se usan para indicar capacidades de los AP 104a-c de la figura 1. Por lo tanto, en el ejemplo ilustrado, la estructura 400 de datos de capacidades de BSS se puede almacenar en los AP 104a-c y se puede descubrir usando formatos de protocolo de consulta predefinidos, por parte de terminales inalámbricos (por ejemplo, el terminal inalámbrico 114) que intentan conectarse a redes soportadas por WLAN respectivas (por ejemplo, las redes 106a-b y 110 de la figura 1). Un ejemplo de formato de protocolo de consulta predefinido incluye el formato de consulta de GAS descrito anteriormente.

En el ejemplo ilustrado, la entrada 404 de capacidad de información de tipo de autenticación de capa 3+ se puede utilizar para indicar que el AP asociado requiere una autenticación de nivel HTTP. Dicha autenticación se puede implementar utilizando técnicas de redireccionamiento de URL que implican redirigir el navegador web de un terminal inalámbrico a un URL particular que requiere que un usuario de un terminal inalámbrico lleve a cabo pasos adicionales necesarios para el acceso (por ejemplo, aceptar términos y condiciones, registro de inicio de sesión en línea, etc.). La entrada 406 de capacidad de información de tipo de autenticación de capa 2 se puede usar para indicar que el AP asociado requiere uno o más de los AuP mostrados en la estructura 300 de datos de AuPs de la figura 3 y/o AI descritos a continuación en relación con la figura 5.

El ejemplo de estructura 500 de datos de AI de capa 2 de la figura 5 almacena información de autenticación que es recuperada por el terminal inalámbrico 114 desde un AP (por ejemplo, uno de los AP 104a-c de la figura 1). En el ejemplo ilustrado, la estructura 500 de datos de AI de capa 2 se puede usar para indicar protocolos o información que requiere un AP para intercambiar información y llevar a cabo procesos de autenticación. Los tipos o protocolos de AI se muestran como tipos 502 de AI, y cada tipo de AI se identifica mediante un ID 504 de AI correspondiente.

En el ejemplo ilustrado, la estructura 500 de datos de AI de capa 2 almacena un tipo 506 de AI de método de Protocolo de Autenticación Extensible (EAP), que puede usarse para indicar que un AP (por ejemplo, uno de los AP 104a-c de la figura 1) admite y/o requiere uno o más protocolos de autenticación EAP. El EAP es un tipo de protocolo que se puede utilizar para llevar a cabo procesos de autenticación en redes inalámbricas y, en ocasiones, se utiliza en relación con los ampliamente conocidos estándares de Acceso Protegido de Wi-Fi (WPA). Durante su funcionamiento, cualquiera de los AP 104a-c de la figura 1 puede invocar comunicaciones de EAP según el ampliamente conocido estándar 802.1X del IEEE®, que forma parte de la arquitectura 802.11 del IEEE®. Los métodos EAP conocidos incluyen EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA y PEAP. Cada método de EAP se puede identificar utilizando un valor de formato entero correspondiente asignado por un organismo de coordinación de recursos estándar de la industria, tal como la Autoridad de Números Asignados de Internet (IANA) (http://www.iana.org). Otros métodos de EAP también pueden incluir métodos específicos del proveedor.

El ejemplo de estructura 500 de datos de AI de capa 2 también almacena un tipo 508 de AI de modo de autenticación interno, un tipo 510 de AI de tipo certificado, un tipo 512 de AI de *hardware* de seguridad, un tipo 514 de AI de AuP y tipos 516 de AI específicos del proveedor. El tipo 508 de AI de modo de autenticación interno se puede usar para indicar que un AP (por ejemplo, uno de los AP 104a-c de la figura 1) admite y/o requiere protocolos de tunelización seguros para intercambiar información de forma segura entre el AP y un terminal inalámbrico. El tipo 510 de AI de tipo certificado se puede usar para indicar que un AP (por ejemplo, uno de los AP 104a-c de la figura 1) admite y/o requiere certificados de seguridad para intercambiar información de forma segura. El tipo 512 de AI de *hardware* de seguridad se puede usar para indicar que un AP admite y/o requiere que un terminal inalámbrico tenga una o más credenciales proporcionadas o suministradas por un elemento de *hardware* asociado al terminal inalámbrico. Los elementos de *hardware* enumerados en el ejemplo ilustrado de la figura 5 incluyen una tarjeta SIM, una tarjeta USIM, un elemento seguro de NFC y un *token* de *hardware*.

El tipo 514 de AI de AuP se puede usar para indicar cuáles de los AuP en la estructura 300 de datos de AuP de la figura 3 son requeridos por un AP (por ejemplo, uno de los AP 104a-c de la figura 1) para permitir la autenticación de un terminal inalámbrico con el fin de establecer una conexión de red con el AP. El tipo 516 de AI específico del proveedor se puede usar para definir tipos de AI adicionales o alternativos definidos por propietarios u operadores de redes soportadas por WLAN (por ejemplo, las redes 106a-b, 108a-b y 110 de la figura 1). A continuación se describen ejemplos de formatos de tramas de mensajería que pueden ser utilizados por un terminal inalámbrico para recuperar la AI de la estructura 500 de datos de AI de capa 2 en relación con la figura 6.

Haciendo referencia ahora a la figura 6, el ejemplo ilustrado muestra un proceso 600 de intercambio de mensajería que puede usarse para descubrir requisitos de AI en una red inalámbrica en relación con las estructuras de datos descritas anteriormente en relación con las figuras 3-5. Como se muestra, el proceso 600 de intercambio de mensajería implica una pluralidad de intercambios de consulta/respuesta entre el terminal inalámbrico 114 y el AP 104a para descubrir AI admitida y/o requerida por el AP 104a con el fin de permitir que el terminal inalámbrico 114 establezca una conexión de red con la red privada 106a soportada por WLAN y/o la SSPN-A 108a de la figura 1. En el ejemplo ilustrado, las capacidades del AP 104a incluyen admisión de información de tipo de autenticación de capa 3+ descrita anteriormente en relación con la entrada 404 de capacidad de información de tipo de autenticación de capa 3+ de la

figura 4 y de información de tipo de autenticación de capa 2 descrita anteriormente en relación con la entrada 406 de capacidad de información de tipo de autenticación de capa 2 de la figura 4.

Como se muestra en la figura 6, el terminal inalámbrico 114 y el AP 104a realizan un primer conjunto de intercambios de mensajes que implican una primera consulta 602 de capacidades y una primera respuesta 604 de capacidades, que permiten al terminal inalámbrico 114 descubrir cuáles de la AI y los AuP de la estructura 500 de datos de AI de capa 2 y la estructura 300 de datos de AuPs requiere el AP 104a para autenticar el terminal inalámbrico 114. En el ejemplo ilustrado, el terminal inalámbrico 114 y el AP 104a también realizan un segundo conjunto de intercambios de mensajes que implican una segunda consulta 606 de capacidades y una segunda respuesta 608 de capacidades, que permiten al terminal inalámbrico 114 descubrir la información de tipo de autenticación de capa 3+ (por ejemplo, información de autenticación a nivel de IP, información de autenticación a nivel de HTTP, etc.) que es admitida y/o requerida por el AP 104a. Las consultas 602 y 606 pueden realizarse mediante el terminal inalámbrico 114 usando el formato de consulta de GAS descrito anteriormente. Aunque las consultas/respuestas 602/604 y 606/608 se describen como primera y segunda consulta/respuestas, dicha descripción no implica ninguna ordenación requerida de los conjuntos de intercambios de mensajes. Es decir, el intercambio de consulta/respuesta 606/608 podría realizarse alternativamente antes del intercambio de consulta/respuesta 602/604. Además, cualquiera de los intercambios de consulta/respuesta 602/604 y 606/608 podría producirse sin el otro.

Para permitir que el terminal inalámbrico 114 descubra información de tipo de autenticación de capa 2, el AP 104a responde a la consulta 602 de capacidades comunicando una trama 610 de información de tipo de autenticación de capa 2 al terminal inalámbrico 114 mediante la respuesta 604 de capacidades. En el ejemplo ilustrado, la trama 610 de información de tipo de autenticación de capa 2 incluye un campo 612 de ID de CAP, un campo 614 de longitud, un campo 616 de recuento y una pluralidad de campos de identificador de información de autenticación (ID de AI) y campos de valor de AI correspondientes.

El campo 612 de ID de CAP identifica la capacidad de BSS a la que está asociada la trama 610. Por lo tanto, para indicar que la trama 610 es una trama de información de tipo de autenticación de capa 2, el campo 612 de ID de CAP del ejemplo ilustrado almacena el identificador de capacidades (por ejemplo, ID de CAP = 270) correspondiente a la información 406 de tipo de autenticación de capa 2 de la estructura 400 de datos de capacidades de BSS de la figura 4.

El campo 614 de longitud almacena la longitud en bytes de la trama 610 de información de tipo de autenticación de capa 2 para posibilitar la recuperación de la misma de la memoria después de que la trama 610 sea recibida por el terminal inalámbrico 114. El campo 616 de recuento almacena la cantidad de IDs de AI a seguir en la trama 610 de información de tipo de autenticación de capa 2.

En el ejemplo ilustrado, cada uno de los campos de ID de AI (ID de AI n.º 1 a ID de AI n.º M) en la trama 610 de información de tipo de autenticación de capa 2 almacena un ID exclusivo, de entre los ID 504 de AI de la estructura 500 de datos de AI de capa 2, para indicar uno o más de los tipos 502 de AI que son admitidos y/o requeridos por el AP 104a. Un primero de los campos de ID de AI (es decir, ID de AI n.° 1) se indica con el número de referencia 618 y su campo de valor de AI correspondiente (es decir, valor de AI n.° 1) se indica con el número de referencia 620. Un segundo de los campos de ID de AI (es decir, ID de AI n.º 2) se indica con el número de referencia 622 y su campo de valor de AI correspondiente (es decir, valor de AI n.º 2) se indica con el número de referencia 624. En algunos ejemplos de implementación, el campo 618 de ID de AI n.º 1 puede almacenar un identificador de ID de AI igual a 1, que se corresponde con el tipo 506 de AI de método de EAP como se muestra en la estructura 500 de datos de AI de capa 2 de la figura 5. En tales ejemplos, el campo 620 de valor de AI n.º 1 puede almacenar el valor en formato entero de un protocolo de autenticación EAP particular (por ejemplo, EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA, PEAP, etc.).

En el ejemplo ilustrado, el campo 622 de ID de AI n.º 2 almacena un identificador ID de AI igual a 5, que se corresponde con el tipo 514 de AI de AuP como se muestra en la estructura 500 de datos de AI de capa 2. Además, el campo 624 de valor de AI n.º 2 almacena una lista 626 de AuP, que incluye uno o más AuP separados por comas de la estructura 300 de datos de AuPs de la figura 3 (por ejemplo, NAI [ID de AuP = 1], SAN de servidor [ID de AuP = 3], etc.).

Con referencia ahora al intercambio de consulta/respuesta 606/608, para permitir que el terminal inalámbrico 114 descubra información de tipo de capa 3+, el AP 104a responde a la consulta 606 de capacidades comunicando una trama 628 de información de tipo de autenticación de capa 3+ al terminal inalámbrico 114 mediante la respuesta 608 de capacidades. En el ejemplo ilustrado, la trama 628 de información de tipo de autenticación de capa 3+ incluye un campo 630 de ID de CAP, un campo 632 de longitud y una pluralidad de campos 634a y 634b de unidad de tipo de autenticación de capa 3+.

El campo 630 de ID de CAP identifica la capacidad de BSS a la que está asociada la trama 628. Por lo tanto, para indicar que la trama 628 es una trama de información de tipo de autenticación de capa 3+, el campo 630 de ID de CAP del ejemplo ilustrado almacena el identificador de capacidades (por ejemplo, ID de CAP = 260) correspondiente a la entrada 404 de capacidad de información de tipo de autenticación de capa 3+ de la estructura 400 de datos de capacidades de BSS de la figura 4. El campo 632 de longitud almacena la longitud en bytes de la trama 628 de

información de tipo de autenticación de capa 3+ para posibilitar la recuperación de la misma de la memoria después de que la trama 628 sea recibida por el terminal inalámbrico 114.

Cada uno de los campos 634a-b de unidad de tipo de autenticación de capa 3+ almacena una trama 636 de URL de redireccionamiento, de las cuales solamente se muestra una. La trama 636 de URL de redireccionamiento se puede usar para implementar otros procedimientos de autenticación cuando se requieren pasos adicionales para el acceso (por ejemplo, aceptar términos y condiciones, registro de inicio de sesión en línea, etc.) para establecer una conexión con el AP 104a. En el ejemplo ilustrado, la trama 636 de URL de redireccionamiento posibilita la autenticación o procedimientos adicionales asociados a procesos implementados en la capa 210 de aplicación de la arquitectura 200 de capas de comunicación de la figura 2. Dichos procedimientos pueden ser adicionales o alternativos a procesos de autenticación asociados a la trama 610 de información de tipo de autenticación de capa 2 analizada anteriormente. En algunos ejemplos de implementación, la trama 636 de URL de redireccionamiento puede especificar que un navegador web del terminal inalámbrico 114 debe mostrar términos y condiciones que deben ser aceptados por un usuario o una página de registro de inicio de sesión en línea en la que un usuario debe iniciar sesión. La trama 636 de URL de redireccionamiento puede especificar adicional o alternativamente un redireccionamiento de HTTP/HTTPS y/o un redireccionamiento de servidor de nombres de dominio (DNS).

Volviendo a las figuras 7-9, la figura 7 representa otro ejemplo de estructura 700 de datos de capacidades de conjunto básico de servicios (BSS), la figura 8 representa un ejemplo de estructura 800 de datos de información de autenticación (AI) de capa 2+, y la figura 9 representa otro ejemplo de proceso de mensajería (por ejemplo, que puede usarse para implementar la mensajería 206 de AI de la figura 2) para descubrir AI en un entorno de WLAN (por ejemplo, una de las ubicaciones 102a-c de acceso de WLAN de la figura 1). Como se analiza a continuación, la estructura 700 de datos de capacidades de BSS es una versión modificada de la estructura 400 de datos de capacidades de BSS de la figura 4, y la estructura 800 de datos de AI de capa 2+ es una versión modificada de la estructura 500 de datos de AI de capa 2 de la figura 5.

A diferencia de la estructura 400 de datos de capacidades de BSS de la figura 4 que almacena la entrada 404 de capacidad de información de tipo de autenticación de capa 3+ separada de la entrada 406 de capacidad de información de tipo de autenticación de capa 2, la estructura 700 de datos de capacidades de BSS de la figura 7 almacena una entrada 702 de capacidad de información de tipo de autenticación de capa 2+. En el ejemplo ilustrado, la entrada 702 de capacidad de información de tipo de autenticación de capa 2+ indica que un AP (por ejemplo, los AP 104a-c de la figura 1) admite todos los procesos y datos de autenticación (que implican operaciones en o por encima de la subcapa 204 de MAC de la figura 2) que, por otro lado, se indican por separado mediante la entrada 404 de capacidad de información de tipo de autenticación de capa 3+ y la entrada 406 de capacidad de información de tipo de autenticación de capa 2 de la figura 4. Es decir, la entrada 702 de capacidad de información de tipo de autenticación de capa 2+ indica que todos los tipos de AI de la estructura 500 de datos de AI de capa 2 de la figura 5 se combinan con la capacidad de redireccionamiento de URL descrita anteriormente en relación con la trama 636 de URL de redireccionamiento de la figura 6. De esta manera, cuando un terminal inalámbrico consulta a un AP sobre capacidades admitidas y/o requeridas asociadas a la autenticación, el terminal inalámbrico puede realizar una única consulta de GAS para descubrir la totalidad de la información y/o parámetros de autenticación analizados anteriormente en relación con las figuras 3-6 en lugar de dos consultas separadas como se describe en relación con la figura 6.

Para posibilitar un descubrimiento de autenticación de consulta única, la estructura 800 de datos de AI de capa 2+ de la figura 8 es una versión modificada de la estructura 500 de datos de AI de capa 2 de la figura 5. Es decir, además de los tipos 506, 508, 510, 512, 514 y 516 de AI mostrados en relación con la estructura 500 de datos de AI de capa 2, la estructura 800 de datos de AI de capa 2+ también incluye un tipo 802 de AI de URL de direccionamiento, que se corresponde con las capacidades de autenticación que, por otro lado, se indican mediante la entrada 404 de capacidad de información de tipo de autenticación de capa 3+ de la figura 4 y la trama 636 de URL de redireccionamiento de la figura 6.

Volviendo ahora a la figura 9, el ejemplo ilustrado muestra un proceso 900 de intercambio de mensajería de consulta única que puede usarse para descubrir requisitos de AI en una red inalámbrica en relación con las estructuras de datos descritas anteriormente en relación con las figuras 3, 7 y 8. Como se muestra, el proceso 900 de intercambio de mensajería de consulta única implica una única consulta 902 de capacidades comunicada por el terminal inalámbrico 114 seguida de una única respuesta 904 de capacidades comunicada por el AP 104a. En el ejemplo ilustrado, las capacidades del AP 104a incluyen admisión de la información de tipo de autenticación de capa 2+ descrita anteriormente en relación con la entrada 702 de capacidad de información de tipo de autenticación de capa 2+ de la figura 7.

Como se muestra en la figura 9, una trama 906 de información de tipo de autenticación de capa 2+ comunicada mediante la respuesta 904 de capacidades es capaz de transportar la misma información que se ha descrito anteriormente en relación con la trama 610 de información de tipo de autenticación de capa 2 de la figura 6. Además, la trama 906 de información de tipo de autenticación de capa 2+ también es capaz de transportar la trama 636 de URL de redireccionamiento descrita anteriormente en relación con la trama 628 de información de tipo de autenticación de capa 3+ de la figura 6. En el ejemplo ilustrado, un campo 908 de ID de AI n.º 3 almacena un valor de ID de AI de 6, que se muestra como correspondiente al tipo 802 de AI de URL de redireccionamiento en la figura 8.

Haciendo referencia ahora a la figura 10, se muestra en forma de diagrama de bloques un ejemplo ilustrado del terminal inalámbrico 114 de las figuras 1, 6 y 9. En el ejemplo ilustrado, el terminal inalámbrico 114 incluye un procesador 1002 que puede usarse para controlar el funcionamiento general del terminal inalámbrico 114. El procesador 1002 puede implementarse usando un controlador, un procesador de propósito general, un procesador de señales digitales o cualquier combinación de los mismos.

El terminal inalámbrico 114 también incluye un generador 1004 de mensajes de terminal y un analizador sintáctico 1006 de datos de terminal. El generador 1004 de mensajes de terminal puede usarse para generar consultas (por ejemplo, las consultas 602 y 606 de la figura 6 y la consulta 902 de la figura 9) de acuerdo con cualquier protocolo de consulta, incluido el formato del protocolo de consulta de GAS analizado anteriormente. El analizador sintáctico 1006 de datos de terminal puede usarse para recuperar de memoria (por ejemplo, una RAM 1010) tramas de información y recuperar información particular de interés a partir de esas tramas. Por ejemplo, el analizador sintáctico 1006 de datos de terminal se puede usar para recuperar AI y/o AuPs de cualquiera de los formatos de trama de datos analizados anteriormente en relación con las figuras 6 y 9. Aunque el generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal se muestran separados del y conectados al procesador 1002, en algunos ejemplos de implementación, el generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal pueden implementarse en el procesador 1002 y/o en un subsistema de comunicación inalámbrica (por ejemplo, un subsistema 1018 de comunicación inalámbrica). El generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal se pueden implementar usando cualquier combinación deseada de *hardware*, *firmware* y/o *software*. Por ejemplo, se pueden usar uno o más circuitos integrados, componentes de semiconductores discretos y/o componentes electrónicos pasivos. Así, por ejemplo, el generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal, o partes de los mismos, podrían implementarse usando uno o más circuito(s), procesador(es) programable(s), circuito(s) integrado(s) de aplicación específica (ASIC(s)), dispositivo(s) lógico(s) programable(s) (PLD(s)), dispositivo(s) lógico(s) programable(s) in situ (FPLD(s)), etc. El generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal, o partes de los mismos, pueden implementarse usando instrucciones, código y/u otro *software* y/o *firmware*, etc. almacenado en un medio accesible por máquina y ejecutable, por ejemplo, por un procesador (por ejemplo, el procesador 1002 ilustrativo). Cuando se lea cualquiera de las reivindicaciones adjuntas para cubrir una implementación puramente de *software*, al menos uno del generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal se define expresamente por la presente de manera que incluye un medio tangible tal como una memoria de estado sólido, una memoria magnética, un DVD, un CD, etc.

El terminal inalámbrico 114 también incluye una memoria FLASH 1008, una memoria de acceso aleatorio (RAM) 1010 y una interfaz 1012 de memoria expandible acopladas comunicativamente al procesador 1002. La memoria FLASH 1008 se puede usar para, por ejemplo, almacenar datos y/o instrucciones legibles por ordenador. En algunos ejemplos de implementación, la memoria FLASH 1008 se puede usar para almacenar una o más de las estructuras de datos analizadas anteriormente en relación con las figuras 3, 4, 5, 7 y 8 y también puede almacenar valores de AuP asociados al terminal inalámbrico 114. La RAM 1010 también puede usarse para, por ejemplo, almacenar datos y/o instrucciones.

El terminal inalámbrico 114 está provisto de una interfaz 1014 de *hardware* de seguridad para recibir una tarjeta SIM (o una tarjeta USIM ó un elemento seguro de NFC) de un proveedor de servicios inalámbricos. Como se ha analizado anteriormente, una tarjeta SIM se puede usar como parámetro de autenticación para autenticar el terminal inalámbrico 114 con el fin de establecer una conexión con una red soportada por WLAN. El terminal inalámbrico 114 también está provisto de una interfaz 1016 de I/O de datos externos. La interfaz 1016 de I/O de datos externos puede ser utilizada por un usuario para transferir información al terminal inalámbrico 114 a través de un medio por cable. Se puede usar una ruta de transferencia de datos por cable, por ejemplo, para cargar una clave de cifrado u otro tipo de AuP en el terminal inalámbrico 114 a través de una conexión directa y, por lo tanto, fiable y de confianza para proporcionar una comunicación segura del dispositivo.

El terminal inalámbrico 114 está provisto de un subsistema 1018 de comunicación inalámbrica para posibilitar comunicaciones inalámbricas con APs de WLAN (por ejemplo, los AP 104a-c de la figura 1). Aunque no se muestra, el terminal inalámbrico 114 también puede tener un subsistema de comunicación de largo alcance para recibir mensajes de, y enviar mensajes a, una red inalámbrica celular. En los ejemplos ilustrados descritos en el presente documento, el subsistema 1018 de comunicación inalámbrica se puede configurar de acuerdo con el estándar 802.11 del IEEE®. En otros ejemplos de implementación, el subsistema 1018 de comunicación inalámbrica se puede implementar usando un módulo de radiocomunicaciones de BLUETOOTH®, un dispositivo de ZIGBEE®, un dispositivo de USB inalámbrico o un módulo de radiocomunicaciones de banda ultraancha (UWB).

Para posibilitar que un usuario use e interactúe con o mediante el terminal inalámbrico 114, el terminal inalámbrico 114 está provisto de un altavoz 1020, un micrófono 1022, una pantalla 1024 y una interfaz 1026 de entrada de usuario. La pantalla 1024 puede ser una pantalla LCD, una pantalla de papel electrónico, etc. La interfaz 1026 de entrada de usuario podría ser un teclado alfanumérico y/o un teclado de tipo telefónico, un actuador multidireccional o rueda de desplazamiento con capacidad de pulsación dinámica de botones, un panel táctil, etc. En el ejemplo ilustrado, el terminal inalámbrico 114 es un dispositivo alimentado por batería y, por lo tanto, está provisto de una batería 1028 y una interfaz 1030 de batería.

Volviendo ahora a la figura 11, se muestra en forma de diagrama de bloques el ejemplo de AP 104a de las figuras 1, 6 y 9. El ejemplo de AP 104a incluye un procesador 1102 para llevar a cabo las operaciones generales del AP 104a. Además, el AP 104a incluye un generador 1104 de mensajes de AP para generar mensajes de consulta y/o respuesta y un analizador sintáctico 1106 de datos de AP para recuperar información a partir de tramas de datos recibidas. El generador 1104 de mensajes de AP es sustancialmente similar al generador 1004 de mensajes de terminal de la figura 10, y el analizador sintáctico 1106 de datos de AP es sustancialmente similar al analizador sintáctico 1006 de datos de terminal de la figura 10. Por lo tanto, el generador 1104 de mensajes de AP y el analizador sintáctico 1106 de datos de AP pueden implementarse en el procesador 1102 y/o un subsistema de comunicación inalámbrica (por ejemplo, un subsistema 1112 de comunicación inalámbrica) usando cualquier combinación de *hardware*, *firmware* y/o *software*, incluidas instrucciones almacenadas en un medio legible por ordenador.

El ejemplo de AP 104a también incluye una memoria FLASH 1108 y una RAM 1110, están acopladas ambas al procesador 1102. La memoria FLASH 1108 puede configurarse para almacenar AuP requeridos de la estructura de datos de AuP de la figura 300, indicadores de capacidad admitidos de las estructuras 400 ó 700 de datos de capacidades de BSS, y tipos de AI admitidos de las estructuras 500 u 800 de datos.

Para comunicarse con terminales inalámbricos tales como el terminal inalámbrico 114, el AP 104a está provisto de un subsistema 1112 de comunicación inalámbrica, que puede ser sustancialmente similar o idéntico al subsistema 1018 de comunicación inalámbrica (figura 10) del terminal inalámbrico 114. Para comunicarse con una red soportada por WLAN (por ejemplo, las redes 106a-b, 110 y 108a-b), el AP 104a está provisto de una interfaz 1114 de comunicación de enlace ascendente de red.

La figura 12 representa un ejemplo de diagrama de flujo representativo de instrucciones legibles por ordenador que pueden usarse para descubrir AuP asociados al acceso a una red soportada por WLAN (por ejemplo, las redes 106a-b, 108a-b y 110 de la figura 1). Los ejemplos de operaciones de la figura 12 se pueden llevar a cabo usando un procesador, un controlador y/o cualquier otro dispositivo de procesamiento adecuado. Por ejemplo, los ejemplos de operaciones de la figura 12 se pueden implementar usando instrucciones codificadas almacenadas en un medio tangible tal como una memoria *flash*, una memoria de solo lectura (ROM) y/o una memoria de acceso aleatorio (RAM) asociada a un procesador (por ejemplo, el procesador 1002 de la figura 10 y/o el procesador 1102 de la figura 11). Alternativamente, parte o la totalidad de los ejemplos de operaciones de la figura 12 se puede implementar utilizando cualquier(cualesquiera) combinación(es) de circuito(s) integrado(s) de aplicación específica (ASIC(s)), dispositivo(s) lógico(s) programable(s) (PLD(s)), dispositivo(s) lógico(s) programable(s) in situ (FPLD(s)), lógica discreta, *hardware*, *firmware*, etc. Además, parte o la totalidad de los ejemplos de operaciones de la figura 12 puede implementarse manualmente o en forma de cualquier(cualesquiera) combinación(es) de cualquiera de las técnicas anteriores, por ejemplo, cualquier combinación de *firmware*, *software*, lógica discreta y/o *hardware*. Además, aunque los ejemplos de operaciones de la figura 12 se describen con referencia al diagrama de flujo de la figura 12, se pueden utilizar otros métodos de implementación de las operaciones de la figura 12. Por ejemplo, se puede cambiar el orden de ejecución de los bloques y/o algunos de los bloques descritos se pueden cambiar, eliminar, subdividir o combinar. Además, cualquiera o la totalidad de los ejemplos de operaciones de la figura 12 puede llevarse a cabo secuencialmente y/o en paralelo mediante, por ejemplo, hilos de procesamiento, procesadores, dispositivos, lógica discreta, circuitos, etc., independientes.

En general, el ejemplo de diagrama de flujo de la figura 12 se puede utilizar para implementar el ejemplo de proceso 600 de intercambio de mensajería de la figura 6 y/o el ejemplo de proceso 900 de intercambio de mensajería de la figura 9 durante un proceso de descubrimiento de WLAN. El ejemplo de diagrama de flujo de la figura 12 incluye un proceso 1202 de terminal inalámbrico y un proceso 1204 de AP. El proceso 1202 de terminal inalámbrico se puede implementar usando el terminal inalámbrico 114 (figuras 1, 6, 9 y 10) para consultar al AP 104a con el fin de descubrir AuP requeridos por el AP 104a. El proceso 1204 de AP se puede implementar usando el AP 104a (figuras 1, 6, 9 y 11) para transmitir la AI y/o los AuP requeridos por el AP 104a.

Volviendo en detalle a la figura 12, inicialmente, el terminal inalámbrico 114 transmite una solicitud de sondeo (bloque 1206) mediante el subsistema 1018 de comunicación inalámbrica. En el ejemplo ilustrado, la solicitud de sondeo se usa para consultar al AP 104a si admite el interfuncionamiento con redes externas (por ejemplo, las redes 106a-b, 108a-b y 110). El AP 104a recibe la solicitud de sondeo (bloque 1208) mediante el subsistema 1112 de comunicación inalámbrica y transmite una respuesta de sondeo (bloque 1210) para indicar si admite el interfuncionamiento con redes externas y si requiere autenticación.

El terminal inalámbrico 114 recibe la respuesta de sondeo (bloque 1212) mediante el subsistema 1018 de comunicación inalámbrica y el analizador sintáctico 1006 de datos de terminal (figura 1) analiza sintácticamente la respuesta de sondeo para determinar si se requiere autenticación (bloque 1214). Por ejemplo, la respuesta de sondeo puede incluir un campo de bits de Paso Adicional Requerido para el Acceso (ASRA) (por ejemplo, un campo de bits de autenticación requerido) (no mostrado) para indicar si se requiere autenticación. Cuando se requiere autenticación (bloque 1212) (por ejemplo, el campo de bits de ASRA es verdadero), el terminal inalámbrico 114 transmite un mensaje de solicitud de capacidades de autenticación (bloque 1216) (por ejemplo, una de las consultas 602 de la figura 6 ó 902 de la figura 9) utilizando, por ejemplo, una consulta de GAS. El terminal inalámbrico 114 espera entonces hasta recibir una respuesta (bloque 1218).

El AP 104a recibe el mensaje de solicitud de capacidades de autenticación (bloque 1220), y el generador 1104 de mensajes de AP (figura 11) empaqueta o inserta los identificadores de AI y AuP requeridos en un mensaje de respuesta de capacidades de autenticación (bloque 1222) (por ejemplo, una de las respuestas 604 de capacidades de la figura 6 ó 904 de la figura 9). Los identificadores de AI y AuP asociados al AP 104a pueden almacenarse en una memoria (por ejemplo, una de la memoria *flash* 1108 ó la RAM 1110 de la figura 11) del AP 104a. El AP 104a transmite entonces el mensaje de respuesta de capacidades de autenticación (bloque 1224).

Si el ejemplo de método de la figura 12 se implementa utilizando la técnica de descubrimiento de AI descrita anteriormente en relación con las figuras 4-6, el mensaje de solicitud de capacidades de autenticación del bloque 1216 es la consulta 602 de capacidades de la figura 6, el mensaje de respuesta de capacidades de autenticación del bloque 1222 es la respuesta 604 de capacidades de la figura 6, y el mensaje de respuesta de capacidades de autenticación se implementa usando el formato de la trama 610 de información de tipo de autenticación de capa 2 de la figura 6. Si el ejemplo de método de la figura 12 se implementa utilizando la técnica de descubrimiento de AI descrita anteriormente en relación con las figuras 7-9, el mensaje de solicitud de capacidades de autenticación del bloque 1216 es la consulta 902 de capacidades de la figura 9, el mensaje de respuesta de capacidades de autenticación del bloque 1224 es la respuesta 904 de capacidades de la figura 9, y el mensaje de respuesta de capacidades de autenticación se implementa usando el formato de la trama 906 de información de tipo de autenticación de capa 2+ de la figura 9.

Cuando el terminal inalámbrico 114 recibe el mensaje de respuesta de capacidades de autenticación (bloque 1218), el analizador sintáctico 1006 de datos de terminal (figura 10) recupera los identificadores de AI y AuP de la trama de mensaje recibida (bloque 1226). Si el terminal inalámbrico 114 determina que tiene los valores de AI y/o AuP requeridos indicados por los identificadores de AI y AuP recibidos (bloque 1228), el generador 1004 de mensajes de terminal (figura 10) empaqueta o inserta los valores de AI y/o AuP en un mensaje de solicitud de conexión (bloque 1230). Por ejemplo, el terminal inalámbrico 114 puede ejecutar uno o más procesos de recuperación de valores de autenticación que llevan a cabo operaciones en la subcapa 204 de MAC para recuperar los valores de AI y/o AuP sin necesidad de permitir que el(los) proceso(s) de recuperación de valores de autenticación lleve(n) a cabo operaciones en o por encima de una capa de protocolo de Internet (IP) (por ejemplo, la capa 208 de red de la figura 2) ni necesidad de proporcionar de otro modo al(a los) proceso(s) de recuperación de valores de autenticación acceso a la capa de IP.

En algunos ejemplos de implementación, cuando el terminal inalámbrico 114 determina en el bloque 1228 que tiene los valores de AI y/o AuP requeridos, se le puede solicitar a un usuario el SSID (ó HESSID) asociado al AP 104a antes de generar el mensaje de solicitud de conexión. De esta manera, al usuario se le puede dar la opción de conectarse al AP 104a en lugar de permitir que el terminal inalámbrico 114 se conecte automáticamente al AP 104a. En algunos ejemplos de implementación, si el terminal inalámbrico 114 determina en el bloque 1228 que no tiene los valores de AI y/o AuP requeridos, el terminal inalámbrico 114 (por ejemplo, el procesador 1002 de la figura 10) puede abstenerse de mostrar el SSID (ó HESSID) asociado al AP 104a. De esta manera, la red privada 106a no se muestra como disponible para conectarse ya que el terminal inalámbrico 114 no podría conectarse a ella sin los valores de AI y/o AuP requeridos. Además, en algunos ejemplos de implementación, el terminal inalámbrico 114 se puede configurar para almacenar los identificadores de AI y AuP obtenidos en el bloque 1226 en relación con un SSID del AP 104a como perfil para el AP 104a. De esta manera, cuando el terminal inalámbrico 114 redescubre posteriormente la presencia del AP 104a, el terminal inalámbrico 114 puede usar los identificadores de AI y AuP almacenados para determinar los valores de AI y/o AuP que debe proporcionar al AP 104a para su autenticación sin tener que volver a solicitar AI y/o AuPs requeridos del AP 104a.

Después de que los valores de AI y/o AuP se empaquetan o insertan en un mensaje de solicitud de conexión (bloque 1230) o si el terminal inalámbrico 114 determinó en el bloque 1214 que el AP 104a no requiere autenticación, el terminal inalámbrico 114 transmite el mensaje de solicitud de conexión (bloque 1232). Después de que el AP 104a recibe el mensaje de solicitud de conexión (bloque 1234), el analizador sintáctico 1106 de datos de AP (figura 11) analiza sintácticamente los valores de AI y/o AuP del mensaje de solicitud de conexión (bloque 1236) y el AP 104a (u otro sistema u ordenador conectado en red al AP 104a) lleva a cabo un proceso de autenticación (bloque 1238). A continuación, el AP 104a autentica y establece una conexión con el terminal inalámbrico 114 ó deniega una conexión con el terminal inalámbrico 114 en función de si los valores de AI y/o AuP proporcionados por el terminal inalámbrico 114 resultaron satisfactorios para la autenticación.

Después de que el AP 104a se conecte al terminal inalámbrico 114 ó deniegue la conexión (bloque 1240), o si el terminal inalámbrico 114 determina que no tiene los valores de AI y/o AuP requeridos, el ejemplo de proceso de la figura 12 finaliza.

REIVINDICACIONES

1. Un método para descubrir información de autenticación de red en una red inalámbrica (102a), comprendiendo el método:

transmitir, desde un terminal inalámbrico (114), durante el descubrimiento de la red y antes de la autenticación, una solicitud (606, 902) de Servicio de Anuncios Genérico, GAS, a un punto (104a) de acceso a la red, solicitando la solicitud de GAS información de autenticación de red;

recibir, por parte del terminal inalámbrico (114), una respuesta (608, 904) a la solicitud de GAS desde el punto (104a) de acceso a la red; y

recuperar, a partir de la respuesta, la información (628) de autenticación de red;

en el que la información (628) de autenticación de red incluye una primera información (634a) de tipo de autenticación, incluyendo la primera información (634a) de tipo de autenticación un primer campo (636) de localizador uniforme de recursos, URL, de redireccionamiento para que el terminal inalámbrico (114) obtenga términos y condiciones, y

en el que la información (628) de autenticación de red incluye además una segunda información (634b) de tipo de autenticación, incluyendo la segunda información (634b) de tipo de autenticación un segundo campo (636) de URL de redireccionamiento configurado para proporcionar la implementación de otros procedimientos de autenticación necesarios cuando se requieren pasos adicionales para el terminal inalámbrico (114) con el fin de establecer una conexión con el punto (104a) de acceso a la red.

2. El método de la reivindicación 1, en el que el terminal inalámbrico es un dispositivo (114) de comunicación móvil.

3. El método de la reivindicación 1, en el que la primera y segunda informaciones (634a, 634b) de tipo de autenticación están asociadas, cada una de ellas, a un identificador de valor correspondiente.

4. Un terminal inalámbrico (114) que comprende un procesador (1002) configurado para llevar a cabo el método de cualquiera de las reivindicaciones 1 a 3.

5. Un medio legible (1010) por ordenador que comprende instrucciones que, cuando son ejecutadas por un procesador (1002) de un terminal inalámbrico (114), hacen que el terminal inalámbrico lleve a cabo el método de cualquiera de las reivindicaciones 1 a 3.

6. Un método para proporcionar información de autenticación de red en una red inalámbrica (102a), comprendiendo el método:

recibir, por parte de un punto (104a) de acceso a la red, durante el descubrimiento de la red y antes de la autenticación, una solicitud (606, 902) de Servicio de Anuncios Genérico, GAS, desde un terminal inalámbrico (114), solicitando la solicitud de GAS información de autenticación de red; y

transmitir, por parte del punto (104a) de acceso a la red al terminal inalámbrico (114), una respuesta (608, 904) a la solicitud de GAS;

en el que la respuesta incluye la información (628) de autenticación de red,

en el que la información (628) de autenticación de red incluye una primera información (634a) de tipo de autenticación, incluyendo la primera información (634a) de tipo de autenticación un primer campo (636) de localizador uniforme de recursos, URL, de redireccionamiento para que el terminal inalámbrico (114) obtenga términos y condiciones, y

en el que la información (628) de autenticación de red incluye además una segunda información (634b) de tipo de autenticación, incluyendo la segunda información (634b) de tipo de autenticación un segundo campo (636) de URL de redireccionamiento configurado para proporcionar la implementación de otros procedimientos de autenticación necesarios cuando se requieren pasos adicionales para el terminal inalámbrico (114) con el fin de establecer una conexión con el punto (104a) de acceso a la red.

7. El método de la reivindicación 6, en el que el terminal inalámbrico es un dispositivo (114) de comunicación móvil.

8. El método de la reivindicación 6, en el que la primera y la segunda informaciones de tipo de autenticación están asociadas, cada una de ellas, a un identificador de valor.

9. Un punto (104a) de acceso a la red que comprende un procesador (1102) configurado para llevar a cabo el método de cualquiera de las reivindicaciones 6 a 8.

10. Un medio legible por ordenador que comprende instrucciones que, cuando son ejecutadas por un procesador (1102) de un punto (104a) de acceso a la red, hacen que el punto de acceso a la red lleve a cabo el método de cualquiera de las reivindicaciones 6 a 8.

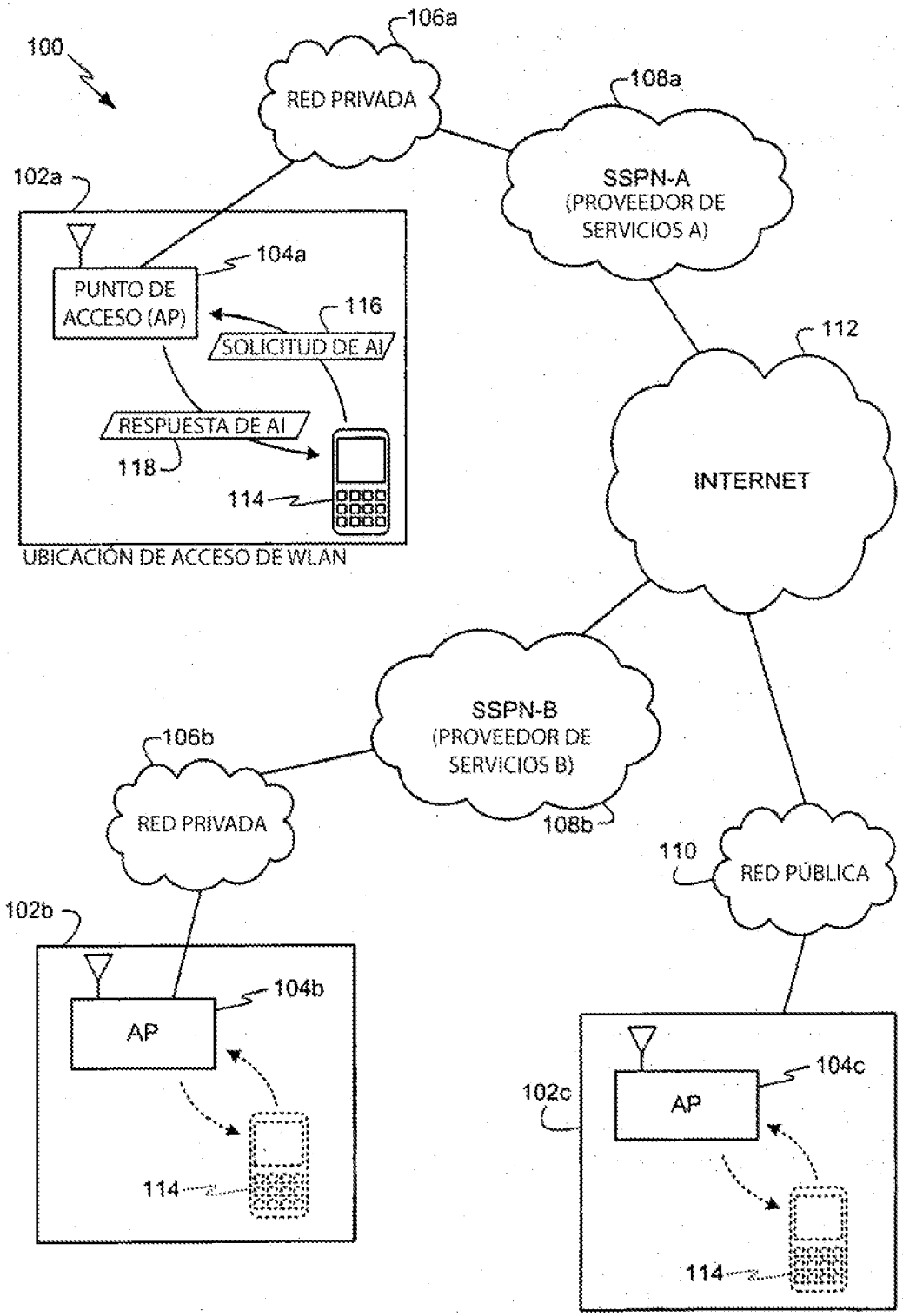
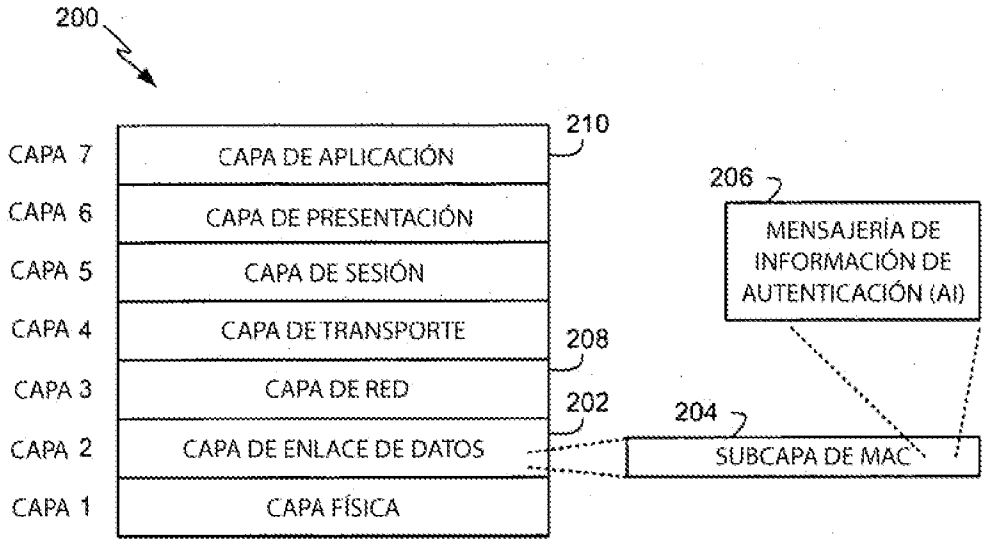

100
106a
RED PRIVADA
108a
SSPN-A
(PROVEEDOR DE
SERVICIOS A)
102a
104a
PUNTO DE
ACCESO (AP)
116
SOLICITUD DE AI
RESPUESTA DE AI
118
114
UBICACIÓN DE ACCESO DE WLAN
112
INTERNET
SSPN-B
(PROVEEDOR DE
SERVICIOS B)
106b
RED PRIVADA
108b
110
RED PÚBLICA
102b
104b
AP
114
102c
104c
AP
114

FIG. 1



ARQUITECTURA DE CAPAS DE COMUNICACION

FIG. 2

302 304

NOMBRE DE AuP	ID DE AuP
INDICADOR DE DIRECCIÓN DE RED (NAI)	1
MATERIA DEL SERVIDOR	2
RED DE ÁREA DE ALMACENAM. DEL SERVIDOR (SAN)	3
ESPECÍFICO DEL PROVEEDOR	255

PARÁMETROS DE AUTENTICACIÓN (AuPs)

300

FIG. 3

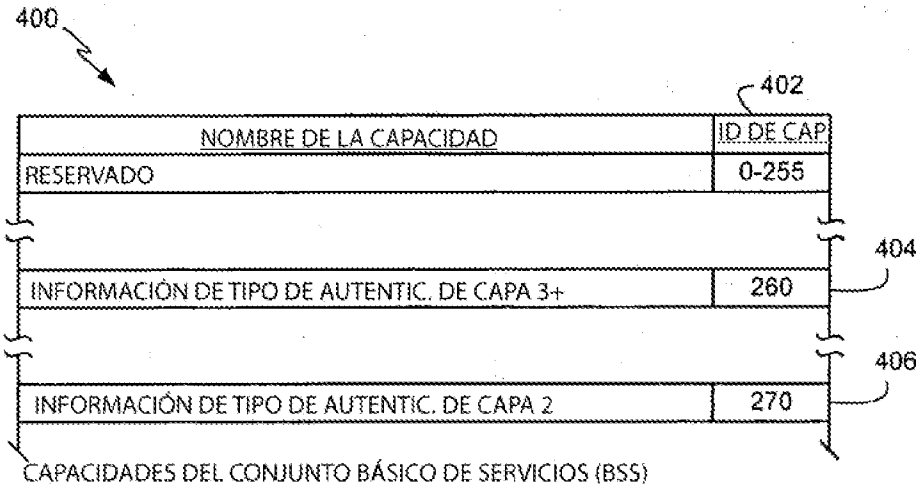


FIG. 4

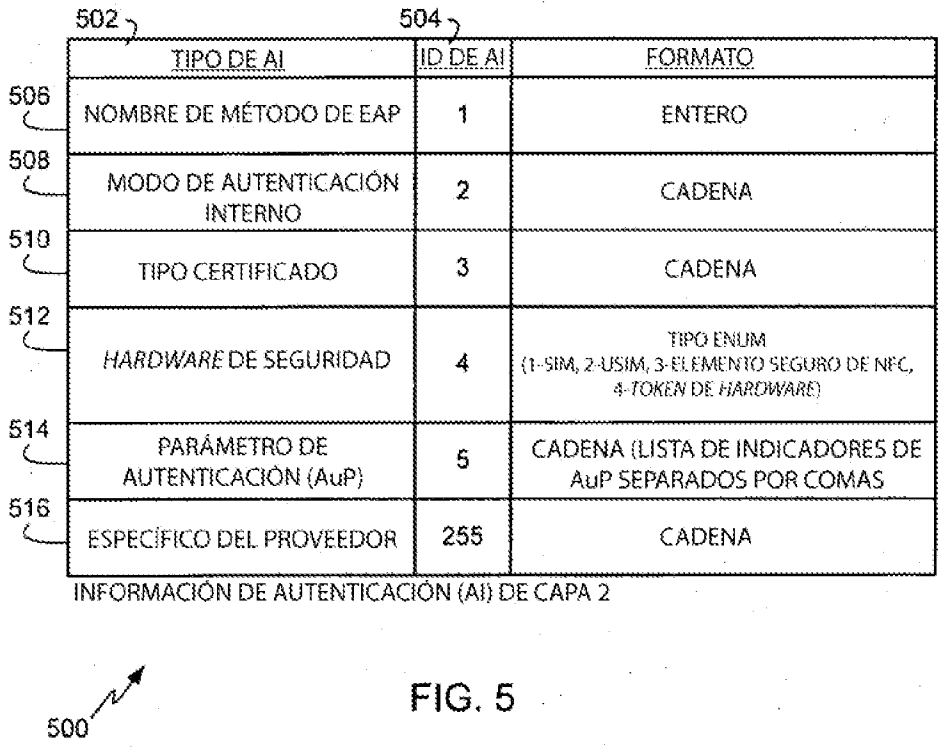


FIG. 5

500

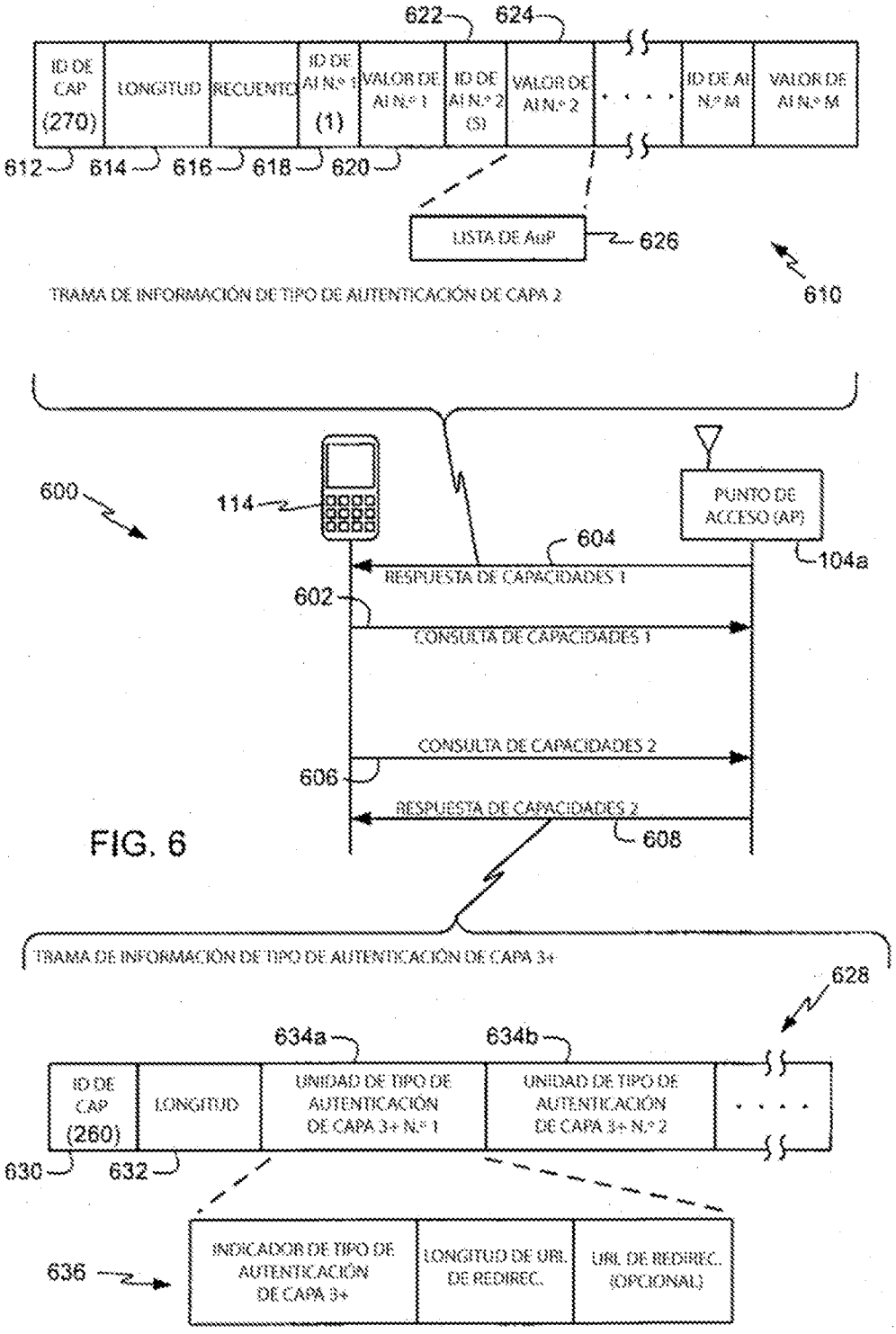

622
624
ID DE CAP (270)
LONGITUD
RECUENTO
ID DE AI N.º 1 (1)
VALOR DE AI N.º 1
ID DE AI N.º 2 (5)
VALOR DE AI N.º 2
ID DE AI N.º M
VALOR DE AI N.º M
612
614
616
618
620
LISTA DE AuP
626
TRAMA DE INFORMACIÓN DE TIPO DE AUTENTICACIÓN DE CAPA 2
610
600
114
PUNTO DE ACCESO (AP)
104a
604
RESPUESTA DE CAPACIDADES 1
602
CONSULTA DE CAPACIDADES 1
CONSULTA DE CAPACIDADES 2
606
RESPUESTA DE CAPACIDADES 2
608
TRAMA DE INFORMACIÓN DE TIPO DE AUTENTICACIÓN DE CAPA 3+
628
634a
634b
ID DE CAP (260)
LONGITUD
UNIDAD DE TIPO DE AUTENTICACIÓN DE CAPA 3+ N.º 1
UNIDAD DE TIPO DE AUTENTICACIÓN DE CAPA 3+ N.º 2
630
632
636
INDICADOR DE TIPO DE AUTENTICACIÓN DE CAPA 3+
LONGITUD DE URL DE REDIREC.
URL DE REDIREC. (OPCIONAL)

FIG. 6

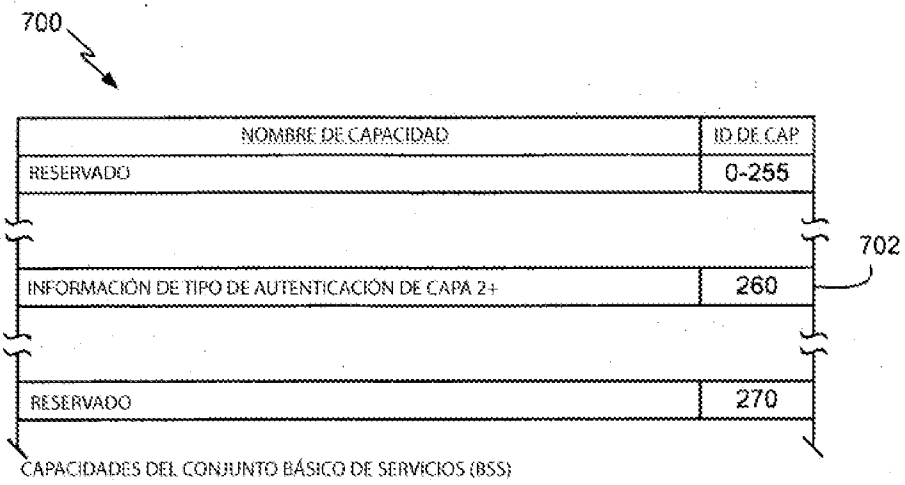


FIG. 7

800

TIPO DE AI	ID DE AI	FORMATO
NOMBRE DE METODO DE EAP	1	ENTERO
MODO DE AUTENTICACIÓN INTERNO	2	CADENA
TIPO CERTIFICADO	3	CADENA
HARDWARE DE SEGURIDAD	4	TIPO ENUM (1-SIM, 2-USIM, 3-ELEMENTO SEGURO DE NFC, 4-*TOKEN* DE *HARDWARE*)
PARÁMETRO DE AUTENTICACIÓN (AuP)	5	CADENA (LISTA DE INDICADORES DE AuP SEPARADOS POR COMAS)
URL DE REDIRECCIONAMIENTO	6	CADENA
ESPECÍFICO DEL PROVEEDOR	255	CADENA

802

INFORMACIÓN DE AUTENTICACIÓN (AI) DE CAPA 2+

FIG. 8

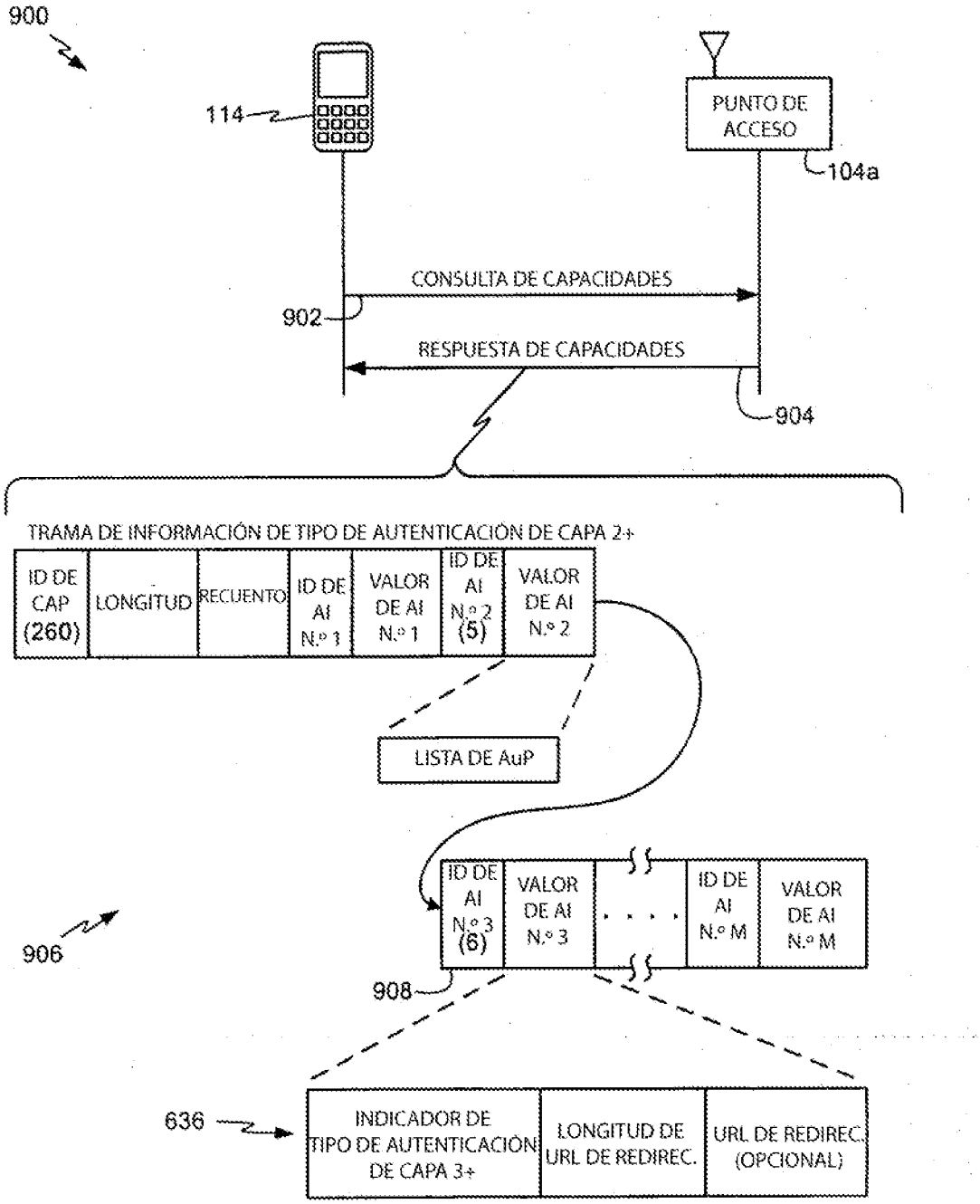

900
114
PUNTO DE ACCESO
104a
CONSULTA DE CAPACIDADES
902
RESPUESTA DE CAPACIDADES
904
TRAMA DE INFORMACIÓN DE TIPO DE AUTENTICACIÓN DE CAPA 2+
ID DE CAP (260)
LONGITUD
RECUENTO
ID DE AI N.º 1
VALOR DE AI N.º 1
ID DE AI N.º 2 (5)
VALOR DE AI N.º 2
LISTA DE AuP
906
ID DE AI N.º 3 (6)
VALOR DE AI N.º 3
ID DE AI N.º M
VALOR DE AI N.º M
908
636
INDICADOR DE TIPO DE AUTENTICACIÓN DE CAPA 3+
LONGITUD DE URL DE REDIREC.
URL DE REDIREC. (OPCIONAL)

FIG. 9

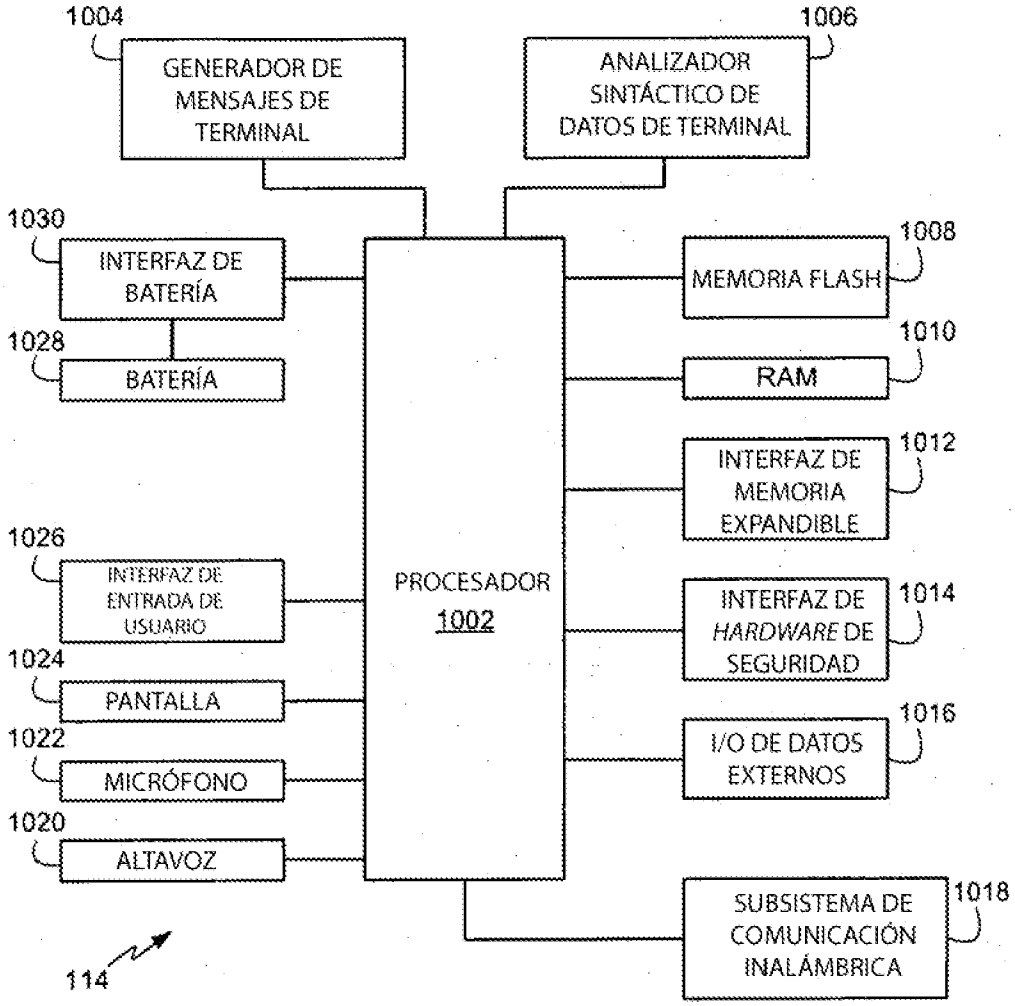
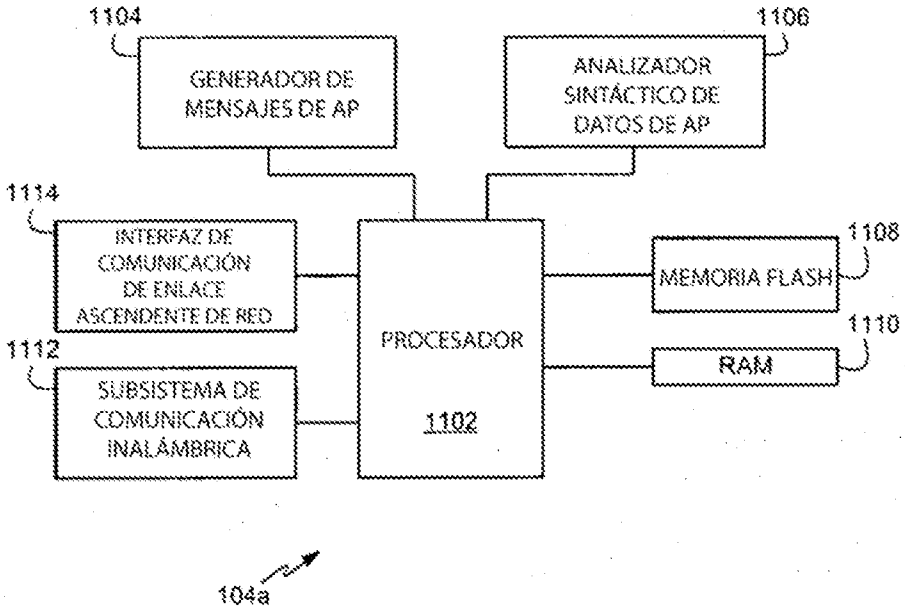

1004
GENERADOR DE MENSAJES DE TERMINAL
1006
ANALIZADOR SINTÁCTICO DE DATOS DE TERMINAL
1030
INTERFAZ DE BATERÍA
1028
BATERÍA
1026
INTERFAZ DE ENTRADA DE USUARIO
1024
PANTALLA
1022
MICRÓFONO
1020
ALTAVOZ
PROCESADOR 1002
1008
MEMORIA FLASH
1010
RAM
1012
INTERFAZ DE MEMORIA EXPANDIBLE
1014
INTERFAZ DE *HARDWARE* DE SEGURIDAD
1016
I/O DE DATOS EXTERNOS
1018
SUBSISTEMA DE COMUNICACIÓN INALÁMBRICA
114
TERMINAL INALÁMBRICO

FIG. 10



PUNTO DE ACCESO

FIG. 11

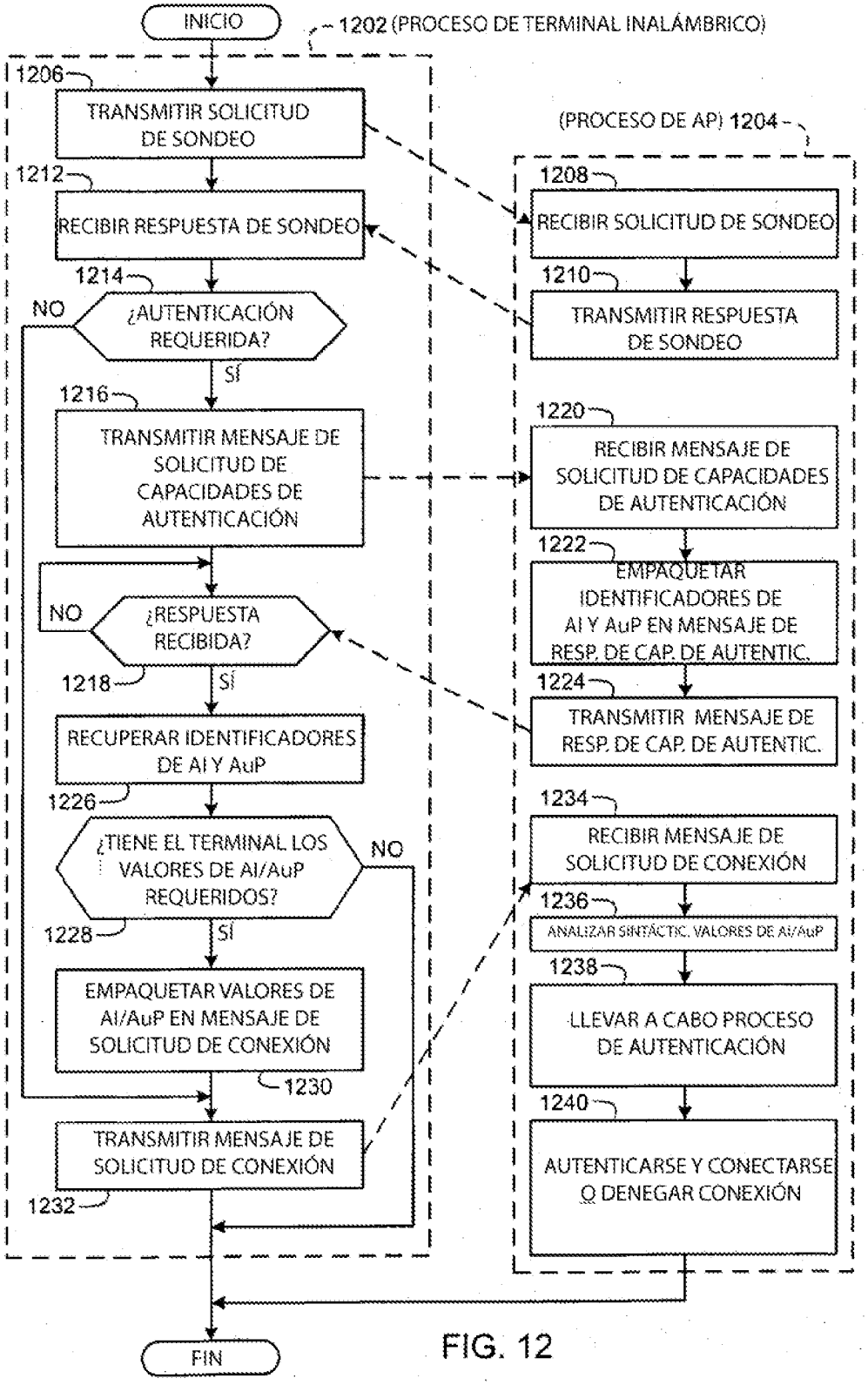

INICIO
1202 (PROCESO DE TERMINAL INALÁMBRICO)
1206
TRANSMITIR SOLICITUD DE SONDEO
1212
RECIBIR RESPUESTA DE SONDEO
1214
NO
¿AUTENTICACIÓN REQUERIDA?
SÍ
1216
TRANSMITIR MENSAJE DE SOLICITUD DE CAPACIDADES DE AUTENTICACIÓN
NO
¿RESPUESTA RECIBIDA?
1218
SÍ
RECUPERAR IDENTIFICADORES DE AI Y AuP
1226
¿TIENE EL TERMINAL LOS VALORES DE AI/AuP REQUERIDOS?
NO
1228
SÍ
EMPAQUETAR VALORES DE AI/AuP EN MENSAJE DE SOLICITUD DE CONEXIÓN
1230
TRANSMITIR MENSAJE DE SOLICITUD DE CONEXIÓN
1232
(PROCESO DE AP) 1204
1208
RECIBIR SOLICITUD DE SONDEO
1210
TRANSMITIR RESPUESTA DE SONDEO
1220
RECIBIR MENSAJE DE SOLICITUD DE CAPACIDADES DE AUTENTICACIÓN
1222
EMPAQUETAR IDENTIFICADORES DE AI Y AuP EN MENSAJE DE RESP. DE CAP. DE AUTENTIC.
1224
TRANSMITIR MENSAJE DE RESP. DE CAP. DE AUTENTIC.
1234
RECIBIR MENSAJE DE SOLICITUD DE CONEXIÓN
1236
ANALIZAR SINTÁCTIC. VALORES DE AI/AuP
1238
LLEVAR A CABO PROCESO DE AUTENTICACIÓN
1240
AUTENTICARSE Y CONECTARSE O DENEGAR CONEXIÓN
FIN

FIG. 12