(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 750 031**

(51) Int. CI.:

H04W 12/08 (2009.01)
H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04W 48/14 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.09.2011 PCT/FI2011/050778**

(87) Fecha y número de publicación internacional: **22.03.2012 WO12035203**

(96) Fecha de presentación y número de la solicitud europea: **12.09.2011 E 11824633 (9)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2019 EP 2617222**

(54) Título: **Creación dinámica de cuentas con red de zona con cobertura inalámbrica asegurada**

(30) Prioridad:

16.09.2010 US 383475 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.03.2020

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

BAJKO, GABOR y
PATIL, BASAVARAJ

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Creación dinámica de cuentas con red de zona con cobertura inalámbrica asegurada

Referencia cruzada a solicitud relacionada

Esta solicitud reivindica la prioridad a tenor de 35 USC 119(e) para la solicitud de patente de EE. UU. provisional con número de serie 61/383.475, presentada el 16 de septiembre de 2010.

Campo técnico

Las realizaciones ilustrativas y no limitantes de la presente invención se refieren, en general, a los sistemas, métodos, dispositivos y programas informáticos de comunicación inalámbrica y, más concretamente, se refieren a las redes de zona con cobertura inalámbrica Wi-Fi y la capacidad de autenticarse con los proveedores de servicios que operan tales redes.

Antecedentes

Esta sección tiene por objeto proporcionar unos antecedentes o contexto a la invención que se enuncia en las reivindicaciones. La descripción en el presente documento puede incluir conceptos que se podrían perseguir, pero no son necesariamente conceptos que previamente se hayan concebido, implementado o descrito. Por lo tanto, salvo que se indique lo contrario en el presente documento, lo que se describe en esta sección y en las reivindicaciones no es técnica anterior de la descripción en la presente solicitud y no se admite que sea técnica anterior por su inclusión en esta sección.

Wi-Fi es una marca comercial de la Alianza Wi-Fi y está asociada a diversos productos que pertenecen a una clase de dispositivos de red de área local inalámbrica (WLAN) basándose en las normas de IEEE 802.11. Se halla a menudo que la expresión Wi-Fi se usa como sinónimo de la tecnología de IEEE 802.11.

Las redes públicas de zona con cobertura inalámbrica Wi-Fi se están implementando ampliamente hoy en día en muchos entornos tales como hoteles, restaurantes, cafeterías, aeropuertos, centros comerciales y oficinas públicas/privadas. El acceso a Internet a través de estas redes de zona con cobertura inalámbrica requiere que un usuario tenga o bien un abono con el operador de esa red de zona con cobertura inalámbrica o bien algún tipo de disposición de itinerancia.

En la actualidad, se encuentra en marcha un esfuerzo por parte del foro de la industria denominado Hotspot 2.0 que tiene por objeto simplificar el proceso de acceso a las redes públicas de zona con cobertura inalámbrica Wi-Fi.

En la actualidad hay dos tipos principales de implementaciones públicas de red Wi-Fi:

- redes abiertas, en donde el dispositivo se puede asociar libremente a la red, pero no obtiene acceso a Internet hasta que este lanza un navegador y proporciona credenciales; y
- redes habilitadas para RSN, que requieren credenciales para asociarse. Una Red de Seguridad Robusta (RSN) es un elemento de los algoritmos de autenticación y cifrado de IEEE 802.11i que se van a usar para las comunicaciones entre puntos de acceso inalámbricos (WAP) y clientes inalámbricos.

Las redes públicas abiertas de zona con cobertura inalámbrica Wi-Fi que se están implementando en la actualidad son operados en general por los ISP (Proveedores de Servicios de Internet), operadores celulares, o por un establecimiento comercial en sí mismo. Habitualmente, estas redes requieren un abono de pago o pueden ser ofrecidas como parte de un plan de datos celular o la compra de acceso durante un periodo de tiempo específico. Habitualmente, tales redes de zona con cobertura inalámbrica Wi-Fi usan una tecnología denominada portales cautivos a través de los cuales los usuarios pueden proporcionar sus credenciales para acceder a la red o para comprar acceso. El enfoque basado en portal cautivo requiere que el usuario lance un navegador web que entonces se redirige a un portal que es gestionado por el operador de la red de zona con cobertura inalámbrica. Este portal proporciona información acerca de los diversos planes de datos que se pueden comprar. Si el usuario tiene un abono con el operador, el portal proporciona una forma para que el usuario introduzca credenciales asignadas y obtenga entonces acceso a Internet. El dispositivo de usuario no tiene conectividad a Internet (más allá del portal cautivo) hasta que se realiza la autenticación. La zona con cobertura inalámbrica Wi-Fi permite que el dispositivo de usuario se asocie con el punto de acceso (AP) Wi-Fi y asigna al dispositivo una dirección de IP. No obstante, la conectividad a Internet más allá del portal cautivo está bloqueada hasta que el usuario se ha autenticado usando credenciales que se asignan como parte de un abono, o el usuario compra acceso durante un periodo de tiempo. Este enfoque se está implementando ampliamente en la actualidad y funciona bien dados los tipos de aplicaciones y servicios usados.

En las redes de zona con cobertura inalámbrica habilitadas para RSN, no es posible el uso del enfoque de redirección de portal cautivo, debido a que las redes habilitadas para RSN requieren que el dispositivo se autentique

usando 802.1x, y la autenticación se realiza antes de que se asigne una dirección de IP al dispositivo. Por lo tanto, no hay forma alguna de que el dispositivo sea redirigido a una página de portal. Si el dispositivo no tiene las credenciales necesarias y la capacidad de autenticarse usando el protocolo de 802.1x, entonces el dispositivo es incapaz de usar la red de zona con cobertura inalámbrica Wi-Fi. 802.1x es un protocolo de seguridad especificado por IEEE para la autenticación del Protocolo de Autenticación Extensible (EAP) (802.1X™, norma IEEE para redes locales y metropolitanas, Control de Acceso de Red Basado en Puertos, 13 de diciembre de 2004).

En general, el uso de 802.1x para autenticarse con una red de zona con cobertura inalámbrica Wi-Fi habilitada para RSN proporciona una experiencia de usuario mejor debido a que el usuario no tiene que abrir un navegador y proporcionar credenciales. No se requiere intervención manual alguna para obtener conectividad a Internet a través de una red de zona con cobertura inalámbrica de este tipo.

El enfoque basado en 802.1x funciona bien cuando el dispositivo/usuario tiene las credenciales que son válidas en una red Wi-Fi. No obstante, dado el gran número de operadores de zona con cobertura inalámbrica Wi-Fi que operan tales redes, el usuario puede no tener credenciales cuando se itinera o en una ubicación dada. Debería ser posible, incluso en redes habilitadas para RSN que utilizan mecanismos de autenticación basados en 802.1x, proporcionar al usuario una oportunidad de comprar un abono. Los operadores de redes de zona con cobertura inalámbrica Wi-Fi pueden generar ingresos al garantizar que proporcionan servicio no solo a usuarios que tengan abonos sino a cualquier otra persona que pueda desear usar la red. Por lo tanto, el operador de zona con cobertura inalámbrica puede tener un interés financiero en ofrecer la capacidad de comprar un abono para acceder a la red.

El grupo de trabajo de Hotspot 2.0 de la Alianza Wi-Fi está centrado en la actualidad en el desarrollo de soluciones que habilitan un acceso ininterrumpido a las redes Wi-Fi de HS2.0 al simplificar los procedimientos de autenticación de acceso. La provisión de capacidades de registro en línea a las redes RSN es un tema de debate.

El documento US 2007/206527 se refiere al establecimiento y la configuración de una WLAN. La tecnología de AP virtual se utiliza para ayudar a la configuración de la red. En particular, se proporcionan al menos dos redes inalámbricas en un AP único, una WLAN de configuración y una WLAN operativa, al utilizar la tecnología de AP virtual. La LAN de configuración se utiliza para proporcionar una comunicación entre el AP y los dispositivos de cliente que está relacionada con el establecimiento, configuración, modificación, etc., de redes, y la WLAN operativa proporciona una comunicación de datos de WLAN normal. Cada una de la WLAN de configuración y la WLAN operativa se puede dotar de sus propios ajustes de seguridad y SSID. El dispositivo de cliente se asocia en primer lugar con la WLAN de configuración. Después de que se haya establecido un canal seguro y autenticado, el AP puede enviar al dispositivo de cliente los ajustes para la WLAN operativa, incluyendo el SSID de operación y otros códigos/claves de cifrado de seguridad asociados, y similares.

El documento EP1615381 divulga un dispositivo de asociación de WLAN y un proceso para asociar una estación nueva a una WLAN, por medio de un aparato central. El proceso comprende: intercambiar señales entre dicha estación y dicho aparato central, dotar automáticamente a dicho aparato central de al menos una clave secreta de central (K), encontrándose disponible al menos una clave secreta de estación (K') que se corresponde con dicha clave secreta de central (K) para dicha estación, y registrar dicha estación como parte de dicha WLAN, bajo intercambios inalámbricos entre dicha estación y dicho aparato central iniciados por una solicitud de asociación enviada por dicha estación y asegurados por medio de dichas claves secretas de central y de estación. La estación se registra solo cuando un usuario ejecuta una acción física de confirmación.

Sumario

La invención se define por la materia objeto de las reivindicaciones independientes. Las realizaciones ventajosas están sujetas a las reivindicaciones dependientes. En un primer aspecto ilustrativo de las realizaciones ilustrativas hay un aparato que comprende al menos un procesador y al menos una memoria que incluye código de programa informático. En este aspecto, la al menos una memoria con el código de programa informático está configurada con el al menos un procesador para dar lugar a que el aparato al menos: reciba al menos una transmisión de baliza de al menos un punto de acceso de red; en respuesta a determinar que el aparato no tiene las credenciales necesarias para acoplarse con un punto de acceso de red seguro del al menos un punto de acceso de red, forme una asociación preliminar con el al menos un punto de acceso de red; durante la asociación preliminar, reciba o cree credenciales necesarias para asociarse con el punto de acceso de red seguro; y forme una asociación con el punto de acceso de red seguro usando las credenciales recibidas o creadas y obtenga conectividad a Internet por medio del punto de acceso de red seguro.

En un segundo aspecto ilustrativo de las realizaciones ilustrativas hay un método que comprende: recibir, en un dispositivo de usuario, al menos una transmisión de baliza de al menos un punto de acceso de red; en respuesta a determinar que el dispositivo de usuario no tiene las credenciales necesarias para acoplarse con un punto de acceso de red seguro del al menos un punto de acceso de red, formar una asociación preliminar con el al menos un punto de acceso de red; durante la asociación preliminar, recibir o crear, el dispositivo de usuario, credenciales necesarias para asociarse con el punto de acceso de red seguro; y formar una asociación entre el dispositivo de usuario y el punto de acceso de red seguro usando las credenciales recibidas o creadas y obtener conectividad a Internet por

medio del punto de acceso de red seguro.

En un tercer aspecto ilustrativo de las realizaciones ilustrativas hay un medio legible por ordenador no transitorio que incluye instrucciones de programa informático. En este aspecto, ejecutar las instrucciones por al menos un procesador de datos da como resultado la realización de operaciones que comprenden: recibir, en un dispositivo de usuario, al menos una transmisión de baliza de al menos un punto de acceso de red; en respuesta a determinar que el dispositivo de usuario no tiene las credenciales necesarias para acoplarse con un punto de acceso de red seguro del al menos un punto de acceso de red, formar una asociación preliminar con el al menos un punto de acceso de red; durante la asociación preliminar, recibir o crear, el dispositivo de usuario, credenciales necesarias para asociarse con el punto de acceso de red seguro; y formar una asociación entre el dispositivo de usuario y el punto de acceso de red seguro usando las credenciales recibidas o creadas y obtener conectividad a Internet por medio del punto de acceso de red seguro.

En un cuarto aspecto ilustrativo de las realizaciones ilustrativas hay un aparato que comprende al menos un procesador y al menos una memoria que incluye código de programa informático. En este cuarto aspecto, la al menos una memoria con el código de programa informático está configurada con el al menos un procesador para dar lugar a que el aparato al menos: envíe al menos una transmisión de baliza que comprende un identificador de conjunto de servicios, y proporcione un servicio de registro para un punto de acceso de red seguro que opera con un identificador de conjunto de servicios que es el mismo que el del aparato.

En un quinto aspecto ilustrativo de las realizaciones ilustrativas hay un método que comprende: enviar desde un punto de acceso de red no de red de seguridad robusta, RSN, al menos una transmisión de baliza que comprende un identificador de conjunto de servicios, y proporcionar, el punto de acceso de red no de red de seguridad robusta, RSN, un servicio de registro para un punto de acceso de red seguro que opera con un identificador de conjunto de servicios que es el mismo que el del punto de acceso de red no de red de seguridad robusta, RSN.

En un sexto aspecto ilustrativo de las realizaciones ilustrativas hay un medio legible por ordenador no transitorio que incluye instrucciones de programa informático. En este aspecto, ejecutar las instrucciones por al menos un procesador de datos da como resultado la realización de operaciones que comprenden: enviar desde un punto de acceso de red no de red de seguridad robusta, RSN, al menos una transmisión de baliza que comprende un identificador de conjunto de servicios, y proporcionar, el punto de acceso de red no de red de seguridad robusta, RSN, un servicio de registro para un punto de acceso de red seguro que opera con un identificador de conjunto de servicios que es el mismo que el del punto de acceso de red no de red de seguridad robusta, RSN.

En un séptimo aspecto ilustrativo de las realizaciones ilustrativas hay un aparato que comprende al menos un procesador y al menos una memoria que incluye código de programa informático. En este séptimo aspecto, la al menos una memoria con el código de programa informático está configurada con el al menos un procesador para dar lugar a que el aparato al menos: transmita al menos una transmisión de baliza; proporcione un identificador de acceso de red, NAI, de registro a un dispositivo de usuario mientras el dispositivo de usuario se encuentra en un estado preasociado al aparato; reciba del dispositivo de usuario una solicitud de asociación que incluye el identificador de acceso de red, NAI, de registro; y conceda al dispositivo de usuario un acceso limitado a una red para fines de creación de credenciales.

En un octavo aspecto ilustrativo de las realizaciones ilustrativas hay un método que comprende: transmitir al menos una transmisión de baliza; proporcionar un identificador de acceso de red, NAI, de registro a un dispositivo de usuario mientras el dispositivo de usuario se encuentra en un estado preasociado; recibir del dispositivo de usuario una solicitud de asociación que incluye el identificador de acceso de red, NAI, de registro; y conceder al dispositivo de usuario un acceso limitado a una red para fines de creación de credenciales.

En un noveno aspecto ilustrativo de las realizaciones ilustrativas hay un medio legible por ordenador no transitorio que incluye instrucciones de programa informático. En este aspecto, ejecutar las instrucciones por al menos un procesador de datos da como resultado la realización de operaciones que comprenden: transmitir al menos una transmisión de baliza; proporcionar un identificador de acceso de red, NAI, de registro a un dispositivo de usuario mientras el dispositivo de usuario se encuentra en un estado preasociado; recibir del dispositivo de usuario una solicitud de asociación que incluye el identificador de acceso de red, NAI, de registro; y conceder al dispositivo de usuario un acceso limitado a una red para fines de creación de credenciales.

Breve descripción de los dibujos

En las figuras de dibujo adjuntas:

La figura 1 muestra un diagrama de bloques simplificado de diversos dispositivos electrónicos que son adecuados para su uso en la puesta en práctica de las realizaciones ilustrativas de la presente invención.

La figura 2 es un diagrama de interacción entre una estación, un punto de acceso y un servidor de portal web de acuerdo con una primera realización de la presente invención.

La figura 3 es un diagrama de interacción entre la estación, el punto de acceso y el servidor de portal web de acuerdo con una segunda realización de la presente invención.

La figura 4 es un diagrama de flujo lógico que ilustra, desde la perspectiva de un dispositivo de usuario, el funcionamiento de un método, y un resultado de la ejecución de instrucciones de programa informático materializadas en una memoria legible por ordenador, de acuerdo con las realizaciones ilustrativas de la presente invención.

Las figuras 5-1 y 5-2 son diagramas de flujo lógico que ilustran, desde la perspectiva de los puntos de acceso de red abierto/seguro respectivos, el funcionamiento de un método, y un resultado de la ejecución de instrucciones de programa informático materializadas en una memoria legible por ordenador, de acuerdo con las realizaciones ilustrativas de la presente invención.

Descripción detallada

Basándose en el análisis anterior, se debería apreciar que un problema que existe es que no hay en la actualidad método alguno mediante el cual un usuario pueda comprar un abono en una red habilitada para RSN. Expuesto de forma sencilla, el usuario no puede acceder a la red debido a que el usuario no tiene las credenciales de red apropiadas, y el usuario no puede crear o comprar las credenciales de red apropiadas debido a que el usuario no tiene acceso a la red. Las prácticas actuales comportan la distribución de un código de acceso en papel a los participantes en un evento, que les permite acceder a la red con ese código de acceso (teniendo todo el mundo el mismo código de acceso, lo que se denomina como WPA_personal en WFA); o generar un testigo separado para cada individuo, lo que se denomina como WPA-Empresa por WFA, y usar métodos tradicionales de distribución (por ejemplo, correo electrónico). Ninguno de estos métodos prevé la creación de una cuenta sobre la marcha, debido a que los mismos requieren que el usuario potencial o bien se registre en el evento, o bien que entre en contacto en persona con un administrador, etc.

Las realizaciones ilustrativas de la presente invención abordan y solucionan estos y otros problemas al proporcionar un método para habilitar capacidades de registro en línea para usuarios ambulantes a redes de zona con cobertura inalámbrica habilitadas para RSN.

Las realizaciones ilustrativas de la presente invención se refieren, al menos en parte, a las redes Wi-Fi de HS2.0, y a proporcionar una capacidad de crear dinámicamente un abono con un operador de una red de zona con cobertura inalámbrica.

Antes de describir con detalle adicional las realizaciones ilustrativas de la presente invención, se hace referencia a la figura 1 para ilustrar un diagrama de bloques simplificado de diversos dispositivos y aparatos electrónicos que son adecuados para su uso en la puesta en práctica de las realizaciones ilustrativas de la presente invención. En la figura 1, una red Wi-Fi está adaptada para la comunicación a través de un enlace inalámbrico 11 con un aparato, tal como un dispositivo de comunicación móvil que puede denominarse en el presente documento estación (STA) o un dispositivo de usuario (UD) 10, por medio de un punto o nodo de acceso de red. En la figura 1, se muestran dos puntos de acceso de red (NWAP), en donde uno representa una red habilitada para RSN 12 y el otro una red abierta 12' (una red no habilitada para RSN). Al menos el NWAP habilitado para RSN (zona con cobertura inalámbrica) 12 proporciona acceso a una o más redes de comunicaciones de datos (por ejemplo, Internet). El UD 10 incluye un controlador, tal como al menos un ordenador o un procesador de datos (DP) 10A, al menos un medio de memoria legible por ordenador no transitorio materializado como una memoria (MEM) 10B que almacena un programa de instrucciones informáticas (PROG) 10C, y al menos un transceptor (par de transmisor y receptor) de radiofrecuencia (RF) adecuado 10D para unas comunicaciones inalámbricas bidireccionales con los puntos o nodos de acceso de red 12, 12' por medio de una o más antenas. El NWAP 12 también incluye un controlador, tal como al menos un ordenador o un procesador de datos (DP) 12A, al menos un medio de memoria legible por ordenador materializado como una memoria (MEM) 12B que almacena un programa de instrucciones informáticas (PROG) 12C, y al menos un transceptor (par de transmisor y receptor) de RF adecuado 12D para la comunicación con el UD 10 por medio de una o más antenas. Se puede suponer que el NWAP 12' se construye de forma similar con el fin de incluir un controlador, tal como al menos un ordenador o un procesador de datos (DP) 12A', al menos un medio de memoria legible por ordenador materializado como una memoria (MEM) 12B' que almacena un programa de instrucciones informáticas (PROG) 12C', y al menos un transceptor (par de transmisor y receptor) de RF adecuado 12D' para la comunicación con el UD 10 por medio de una o más antenas.

Obsérvese que, aunque el NWAP habilitado para RSN 12 y el NWAP abierto (no habilitado para RSN) 12' se muestran como dos puntos de acceso separados, en la práctica la funcionalidad de ambos se podría ubicar conjuntamente dentro de un sistema de hardware/software de punto de acceso.

Para los fines de describir las realizaciones ilustrativas de la presente invención, se puede suponer que el UD 10 también incluye un navegador 10E, un almacén de credenciales 10F y un gestor de conexión (CM) 10G. Aunque se muestran en la figura 1 como elementos separados, en la práctica el navegador 10E y el gestor de conexión 10G

puede formar parte del software de programa 10C, y el almacén de credenciales 10F se puede implementar como una o más ubicaciones de almacenamiento en la memoria 10B. Cada una del NWAP habilitado para RSN 12 y el NWAP abierto (no habilitado para RSN) 12' puede incluir una página de portal 12E, 12E', o de lo contrario tener acceso a un servidor en el que se aloja una página de portal web.

Obsérvese que el UD 10 puede incluir un circuito integrado o chip o módulo de WLAN especializado que materializa la totalidad o al menos parte de la funcionalidad necesaria para las operaciones y conectividad de WLAN.

Se supone que al menos uno de los PROG 10C y 12C incluye instrucciones de programa que, cuando son ejecutadas por el DP asociado, posibilitan que el dispositivo electrónico funcione de acuerdo con las realizaciones ilustrativas de la presente invención, como se analizará posteriormente con mayor detalle. Es decir, las realizaciones ilustrativas de la presente invención se pueden implementar al menos en parte por software informático ejecutable por el DP 10A del UD 10 y/o por el DP 12A del NWAP 12, o por hardware, o por una combinación de software y hardware (y firmware).

En general, las diversas realizaciones del UD 10 pueden incluir, pero no se limitan a, asistentes digitales personales (PDA) que tienen capacidades de comunicación inalámbrica, ordenadores portátiles que tienen capacidades de comunicación inalámbrica, dispositivos de captación de imágenes tales como cámaras digitales que tienen capacidades de comunicación inalámbrica, dispositivos de juegos que tienen capacidades de comunicación inalámbrica, aparatos de almacenamiento y de reproducción de música que tienen capacidades de comunicación inalámbrica, aparatos de Internet que permiten acceso y navegación inalámbricos por Internet, teléfonos celulares que tienen capacidad Wi-Fi, así como terminales o unidades portátiles que incorporan combinaciones de tales funciones.

Las MEM legibles por ordenador 10B y 12B pueden ser de cualquier tipo conveniente para el entorno técnico local y se pueden implementar usando cualquier tecnología de almacenamiento de datos conveniente, tal como dispositivos de memoria basados en semiconductores, memoria de acceso aleatorio, memoria de solo lectura, memoria de solo lectura programable, memoria flash, dispositivos y sistemas de memoria magnéticos, dispositivos y sistemas de memoria ópticos, memoria fija y memoria extraíble. Los DP 10A y 12A pueden ser de cualquier tipo conveniente para el entorno técnico local, y pueden incluir uno o más de ordenadores de propósito general, ordenadores de propósito especial, microprocesadores, procesadores digitales de señales (DSP) y procesadores basándose en arquitecturas de procesador de múltiples núcleos, como ejemplos no limitantes.

De acuerdo con las realizaciones ilustrativas de la presente invención, se proporcionan múltiples soluciones para un registro en línea del UD 10, así como un mecanismo de generación de credenciales simplificado (ininterrumpido para el usuario).

En una primera realización (véase también la figura 2), para una aparición de la red habilitada para RSN 12, también se proporciona la red no habilitada para RSN (es decir, abierta) 12' correspondiente. La red abierta 12' proporciona al menos una capacidad de registro en línea para el UD 10 y, habitualmente, no proporcionaría acceso a Internet o ningún otro servicio.

El procedimiento funciona tal como sigue. La red abierta 12' publicita en sus capacidades (por ejemplo, una capacidad recién definida, o una específica del proveedor) que proporciona solo un servicio de registro en línea para la creación de credenciales que se va a usar con la red RSN 12 (con el mismo SSID). Como es bien sabido, el identificador de conjunto de servicios, o SSID, es un nombre que identifica una LAN inalámbrica de 802.11 particular. Un dispositivo de cliente recibe mensajes de radiodifusión de todos los puntos de acceso dentro de alcance que publicitan sus SSID. El dispositivo de cliente puede seleccionar entonces, de forma o bien manual o bien automática, basándose en la configuración, la red con la que asociarse. La longitud del SSID puede ser de hasta 32 caracteres.

Cuando el UD 10 realiza un procedimiento de Descubrimiento y Selección de Red (NDS) y halla tanto la red abierta 12' como la red habilitada para RSN 12, con el mismo SSID, este comprueba en primer lugar si tiene credenciales válidas con la red habilitada para RSN 12. Si el UD 10 determina que no tiene las credenciales habilitadas para RSN apropiadas, este detecta la capacidad de la red abierta 12' con el mismo SSID. Si la capacidad de la red 12' indica que soporta solo el procedimiento de registro, el UD 10 se asocia con la red abierta 12', lanza el navegador 10E y genera algo de tráfico http (por ejemplo, ficticio) (por ejemplo, al realizar una solicitud http a una cierta dirección de IP tal como páginadeinicioficticia.net). El NWAP de red abierta 12' redirige ese tráfico http a la página de portal 12E (y ofrece su certificado al UD 10 de una forma convencional). Después de que el terminal haya autenticado la página de portal usando la credencial proporcionada, en la página de portal 12E se ofrecen al UD 10 las tasas de los planes y se le pide seleccionar una e introducir la información de tarificación (por ejemplo, de tarjeta de crédito). Al UD 10 también se le puede ofrecer la posibilidad de crear credenciales para el usuario, o hacer que la página de portal 12E cree las credenciales (véase posteriormente para la creación de credenciales).

Cuando el navegador 10E recibe las credenciales, puede almacenarlas temporalmente en el almacén de credenciales 12F e iniciar un mensaje de desasociación (por ejemplo, mediante el uso de las interfaces de programa de aplicación (API) de un chip de WLAN disponible a través de una interfaz de línea de comandos). El dispositivo UD

10 inicia entonces un mensaje de conexión a la red habilitada para RSN 12 al especificar el SSID para el que se acababan de crear las credenciales (por ejemplo, a través de la interfaz de línea de comandos del chip de WLAN). Como alternativa, si no se especifica el SSID, el UD 10 puede comenzar un nuevo procedimiento de NDS, hallar el SSID para el que se crearon las credenciales y conectarse con el mismo. Cuando se le piden las credenciales, el gestor de conexión 10G en el UD 10 suministra las credenciales recién creadas. Después de que la autenticación haya tenido éxito, el gestor de conexión 10G considerará las credenciales verificadas y actualizará su estado en consecuencia en el almacén de credenciales 10F.

En el caso de que no se pueda operar con las credenciales o que estas no sean válidas, o que estas caduquen, la autenticación no tendrá éxito. En lugar de proporcionar un mensaje de error al usuario, en su lugar el UD 10 se puede reasociar automáticamente al NWAP abierto 12' con el mismo SSID, generar tráfico http con el fin de redirigirse a la página de portal 12E' que, a su vez, visualiza qué etapa o etapas debería emprender a continuación el usuario (por ejemplo, visualizar un número de teléfono de un departamento de soporte técnico) cuando este identifica que el UD 10 (con su dirección de MAC única) intentó crear credenciales pero no tuvo éxito por alguna razón.

A continuación, haciendo referencia más concretamente al diagrama de interacción ilustrativo de la figura 2, en 2A una Baliza: SSID X, Abierto, solo Registro en Línea se recibe del NWAP abierto 12'. En 2B, se recibe una Baliza: SSID X, habilitado para RSN. Obsérvese que, en algunas situaciones, se puede invertir el orden de recepción de las balizas en 2A y 2B. Debido a que 2A solo indica un registro en línea (lo que quiere decir que no se proporciona acceso a Internet alguno más allá de la página/páginas de registro), el UD 10 continúa buscando una red que proporciona acceso a Internet. En respuesta a una determinación de que el anfitrión (el UD 10) no tiene las credenciales para acoplarse por medio del AP habilitado para RSN, se envía un Asociar (SSID X, Abierto) al NWAP 12' para fines de creación de credenciales. El UD 10 inicia el navegador 10E y, en 2D, envía una Solicitud de HTTP al NWAP 12' (este es el tráfico http ficticio al que se ha hecho referencia anteriormente). En 2E, el UD 10 recibe en respuesta una Respuesta de HTTP (Redirección) y, en 2F, se establece una conexión HTTPS con la página de portal 12E, con lo que el UD 10 autentica la red y se dota de las credenciales necesarias una vez que este ha suministrado la información de pago. En 2F, el UD 10 envía el Desasociar (SSID X, Abierto) al NWAP 12'. En 2H, el UD 10 envía un Asociar (SSID X, habilitado para RSN) y se autentica con el NWAP habilitado para RSN 12 usando las credenciales proporcionadas por el servidor de registro de portal web 12E durante la conexión HTTPS 2F. Obsérvese, en 2G y 2H, que el SSID X es el mismo SSID recibido en 2A y 2B. En 21, el UD 10 queda conectado a Internet más allá de la página o páginas de registro por medio del NWAP habilitado para RSN 12, y las credenciales recibidas durante la conexión HTTPS en 2F se pueden guardar en el almacén de credenciales 10F para su uso posterior.

En una segunda realización (véase también la figura 3), cuando hay una red habilitada para RSN 12 para la que el UD 10 no tiene credenciales, el UD 10 comprueba en primer lugar la capacidad de la red habilitada para RSN 12. Si se soporta la capacidad de registro en línea (como se define actualmente en la tabla 7-43bo de 802.11u), de acuerdo con un aspecto ilustrativo de la presente invención la red habilitada para RSN 12 proporciona un Identificador de Acceso de Red (NAI, por ejemplo, véase RFC4282) de registro especial en un estado preasociado. Un NAI de este tipo se podría definir en la tabla 7-43bn de 802.11u, o este se podría definir como un elemento de lista específico del proveedor de Protocolo de Consulta de Red de Acceso (ANQP) de tal modo que, cuando la capacidad de registro en línea es soportada por la red habilitada para RSN 12, se ha de proporcionar el NAI de registro. El UD 10 puede usar entonces, por ejemplo, el ANQP (definido en 802.11u) con, por ejemplo, el nombre de Info recién definido para solicitar el NAI de registro de la red habilitada para RSN 12, mientras se encuentra en el estado preasociado. Cuando se recibe este NAI de registro, el UD 10 usa este NAI como su Identidad del Protocolo de Autenticación Extensible (EAP) durante el procedimiento de autenticación de 802.1x. Cuando la red habilitada para RSN 12 recibe un mensaje de Identidad de Respuesta de EAP del UD 10 con el NAI de registro como la identidad del usuario, la red habilitada para RSN 12 sabrá que el usuario desea registrarse. En este caso, la autenticación es solo de lado de servidor, y la red habilitada para RSN 12 no debería pedir las credenciales de usuario (este es el fin de este NAI de registro que se va a definir, debido a que el usuario no tiene credenciales). Una vez que el UD 10 ha autenticado con éxito la red habilitada para RSN 12 y se ha establecido una asociación (con unas claves de sesión de 802.1x generadas), el UD 10 inicia el navegador 10E y genera algo de tráfico http (por ejemplo, ficticio). La red habilitada para RSN 12 redirigirá ese tráfico http a su página de portal 12E. Obsérvese que, incluso aunque se habilite la seguridad de capa de enlace, la presente realización supone que la página de portal 12 presenta un certificado al UD 10 y se establece una conexión https (http seguro) con el fin de evitar que la red habilitada para RSN 12 vea las credenciales que genera el usuario o de las que es dotada por la página de portal. Se ofrecen entonces al usuario las tasas de los planes y se le pide seleccionar una e introducir la información de tarificación. Al usuario también se le puede ofrecer la posibilidad de crear credenciales para el usuario o hacer que la página de portal 12 cree las credenciales (véase posteriormente para la creación de credenciales). Cuando el navegador 10E recibe las credenciales, puede almacenarlas temporalmente en el almacén de credenciales 10F, iniciar el mensaje de desasociación, e iniciar entonces un mensaje de conexión a la misma red habilitada para RSN 12 al especificar el SSID para el que se acababan de crear las credenciales. Cuando la red habilitada para RSN 12 envía una Solicitud de Identidad de EAP, el UD 10 suministra la identidad recién creada (parte del conjunto de credenciales recién creadas), y no el NAI de registro.

A continuación, haciendo referencia más concretamente al diagrama de interacción ilustrativo de la figura 3, en 3A el UD 10 recibe del NWAP habilitado para RSN 12 una Baliza: SSID X, habilitado para RSN, indicándose el soporte de registro en línea. En el caso en el que se descubre que el anfitrión (el UD 10) no tiene las credenciales necesarias, se realiza una determinación de usar el NAI de registro. En 3B, el UD 10 envía una Solicitud, en un estado preasociado, del NAI de registro y, en 3C, recibe el NAI de registro (en el estado preasociado) del NWAP habilitado para RSN 12. En 3D, el UD 10 y el NWAP habilitado para RSN 12 se asocian (usando una autenticación solo de lado de servidor). El UD 10 inicia entonces el navegador 10E. En 3E, se envía la Solicitud de HTTP (tráfico http ficticio) y, en 3F, el NWAP 12 envía la Respuesta de HTTP (redirección). En 3F, el UD 10 recibe en respuesta una Respuesta de HTTP (Redirección) y, en 3G, se establece una conexión HTTPS con la página de portal 12E, con lo que el UD 10 autentica la página de portal y genera o se dota de las credenciales necesarias. En 3H, el UD 10 envía el Desasociar (SSID X, habilitado para RSN, SU-NAI) y, en 31, el UD 10 envía un Asociar (SSID X, habilitado para RSN) y se autentica con el NWAP habilitado para RSN 12 usando las credenciales proporcionadas por el servidor de registro de portal web 12E durante la conexión HTTPS 3G. En 3J, el UD 10 queda conectado a Internet por medio del NWAP habilitado para RSN 12, y las credenciales recibidas durante la conexión HTTPS en 3G se pueden guardar en el almacén de credenciales 10F para su uso posterior.

A continuación se describe el procedimiento de creación de credenciales. Hay dos tipos de credenciales que se pueden crear en línea para usuarios "ambulantes": nombre de usuario/contraseña y certificado. Estas pueden ser o bien permanentes o bien limitadas en el tiempo (por ejemplo, un bono). Si las mismas son permanentes, lo más probable es que haya una línea de crédito asociada a la credencial. Cuando caduca la línea de crédito, el usuario necesitará comprar crédito adicional con el fin de usar las credenciales.

Un certificado de cliente es generado por software, pero un nombre de usuario/contraseña también puede ser generado por el usuario. No hay, no obstante, razón alguna para exigir al usuario que introduzca un nombre de usuario/contraseña. El software también podría generar cadenas aleatorias para ambos del par nombre de usuario/contraseña, como en Hotspot 2.0, uno de los requisitos es que el UD 10 no debería solicitar que el usuario introduzca credenciales. Es decir, estas credenciales no son para el usuario, sino para el consumo del dispositivo.

Por lo tanto, de acuerdo adicionalmente con las realizaciones ilustrativas cuando el usuario se redirige a una página de portal (12, 12'), la página de portal debería tener una opción para que el usuario seleccione una generación de credenciales o bien automática o bien manual, siendo el valor por defecto la generación de credenciales automática (independientemente de si la red requiere un nombre de usuario/contraseña o un certificado como la credencial). Con la generación de credenciales automática, la página de portal 12, 12' genera las credenciales requeridas (o bien un nombre de usuario/contraseña o bien un certificado de cliente) y proporciona las credenciales generadas al UD 10. Una vez que el UD 10 ha recibido las credenciales, este las almacena en el almacén de credenciales 12F y las usa cuando sea apropiado. Debido a que el UD 10 suministra automáticamente las credenciales al NWAP 12, 12' el usuario no necesita tener conocimiento de las credenciales. Por lo tanto, las credenciales no necesitan encontrarse en una forma legible por un ser humano. Además, el usuario no necesita saber el tipo de credenciales que se reciben, (ya sea este un nombre de usuario/contraseña o un certificado de cliente).

En el lado del UD 10, la implementación de las realizaciones ilustrativas puede ser parte del cliente o demonio del gestor de conexión 10G. Cuando el UD 10 percibe la disponibilidad de la red de zona con cobertura inalámbrica Wi-Fi de HS2.0 habilitada para RSN 12, y reconoce que no tiene credenciales para su uso con esa red, este puede proporcionar las mejoras de lógica y de interfaz de usuario que permiten que el usuario compre un acceso en esa red.

Hay una serie de ventajas y efectos técnicos que se pueden obtener mediante el uso de las realizaciones ilustrativas. Por ejemplo, su uso proporciona un método mediante el cual un usuario final/consumidor puede comprar acceso a una red de zona con cobertura inalámbrica Wi-Fi habilitada para RSN de HS2.0. También a modo de ejemplo, el uso de las realizaciones ilustrativas satisface un interés comercial de un operador de zona con cobertura inalámbrica Wi-Fi para proporcionar la capacidad mediante la cual los abonos pueden ser comprados por cualquiera que se encuentre en las proximidades de esa red. Además, las realizaciones ilustrativas proporcionan un medio seguro mediante el cual se intercambian la información de pago y credenciales. Además, las realizaciones ilustrativas se pueden implementar al utilizar protocolos previamente existentes. Estos protocolos se implementan en la mayoría de los UD 10, y no es necesaria mejora alguna en los protocolos y/o el software del gestor de conexión 10G.

Basándose en lo anterior, debería ser evidente que las realizaciones ilustrativas de la presente invención proporcionan un método, aparato y programa o programas informáticos para posibilitar la conectividad con diversos tipos de los tipos de comunicaciones inalámbricas locales de dispositivos y estaciones y terminales, tales como los conformes con los tipos de sistemas de comunicación según IEEE 802.

La figura 4 es un diagrama de flujo lógico que ilustra, desde la perspectiva del UD 10, el funcionamiento de un método, y un resultado de la ejecución de instrucciones de programa informático, de acuerdo con las realizaciones ilustrativas de la presente invención. De acuerdo con estas realizaciones ilustrativas, un método realiza, en el bloque 4A, una etapa de recibir, en un dispositivo de usuario, al menos una transmisión de baliza de al menos un punto de

acceso de red. En una realización, se recibe una primera transmisión de baliza de un punto de acceso de red no seguro que indica solo registro RSN y también se recibe una segunda baliza de un punto de acceso seguro, en la que la primera y la segunda balizas comprenden un mismo identificador de conjunto de servicios. En otra realización, se recibe solo una baliza del punto de acceso de red seguro. En respuesta a una determinación en el bloque 4A de que el dispositivo de usuario no tiene las credenciales necesarias para acoplarse con el punto de acceso de red seguro, en el bloque 4B una etapa de formar una asociación preliminar con uno de los puntos de acceso de red seguros y no seguros de acuerdo con las diferentes realizaciones anteriores. A modo de ejemplo, en una de esas realizaciones, el UD 10 obtiene en primer lugar un NAI de registro del punto de acceso RSN mientras se encuentra en un estado preasociado al mismo antes de realizar la asociación preliminar del bloque 4B con el punto de acceso RSN. En el bloque 4C hay una etapa de enviar tráfico http hacia el punto de acceso asociado en el bloque 4B. Como se ha hecho notar anteriormente, este tráfico http puede ser tráfico ficticio o tráfico ordinario (genuino). En el bloque 4D hay una etapa de redirigirse a, y formar una conexión http segura con, una página de portal. En el bloque 4E hay una etapa de, el dispositivo de usuario, autenticar la página de portal y recibir, de la página de portal, credenciales necesarias para asociarse con el punto de acceso de red seguro. Como alternativa, el dispositivo de usuario puede crear las credenciales como también se expone en el bloque 4E. En el bloque 4F hay una etapa de terminar la asociación preliminar y, en el bloque 4G, hay una etapa de formar una asociación con el punto de acceso de red seguro usando las credenciales recibidas y obtener conectividad a Internet por medio del punto de acceso de red seguro.

El método como en la figura 4, en donde la primera baliza del bloque 4A se recibe del punto de acceso no seguro que es un punto de acceso de red no habilitado para RSN que publicita solo una capacidad de registro, y en donde el punto de acceso de red seguro es un punto de acceso habilitado para RSN diferente. En otra realización, los puntos de acceso de red seguros y no seguros se materializan en el mismo nodo físico que opera funcionalmente sobre una red segura y sobre una red no segura, respectivamente.

El método del párrafo anterior, en donde el dispositivo de usuario forma la asociación preliminar en el bloque 4B con el punto de acceso de red no habilitado para RSN, envía el tráfico http (por ejemplo, ficticio) al punto de acceso de red no habilitado para RSN, termina la asociación preliminar con el punto de acceso no habilitado para RSN, y forma la asociación con el punto de acceso habilitado para RSN usando las credenciales recibidas.

El método como en la figura 4, en donde la baliza se recibe de un punto de acceso de red no habilitado para red de seguridad robusta (RSN) que proporciona la conectividad a Internet, indicando la baliza que el punto de acceso de red habilitado para RSN soporta una capacidad de registro para el dispositivo de usuario, y que comprende adicionalmente enviar una solicitud de un identificador de acceso de red (NAI) de registro, en un estado preasociado del dispositivo de usuario, al punto de acceso de red habilitado para RSN; recibir el NAI de registro solicitado y, usando autenticación de lado de servidor, asociarse con el punto de acceso habilitado para RSN.

El método del párrafo anterior, en donde el dispositivo de usuario envía el tráfico http (por ejemplo, ficticio) al punto de acceso de red habilitado para RSN, termina la asociación preliminar en el bloque 4F que usó el NAI de registro con el punto de acceso habilitado para RSN, y forma la asociación con el punto de acceso de red habilitado para RSN usando las credenciales recibidas.

El método de la figura 4 y cualquiera de los párrafos anteriores, en el que, cuando está conectado con la página de portal, un usuario está habilitado para seleccionar una generación de credenciales o bien automática o bien manual.

El método del párrafo anterior, en donde, con la generación de credenciales automática, la página de portal 12 genera las credenciales como o bien un nombre de usuario/contraseña o bien un certificado de cliente y proporciona las credenciales generadas al dispositivo de usuario que almacena y proporciona automáticamente las credenciales al punto de acceso de red habilitado para RSN sin requerir que el usuario sea consciente del contenido de las credenciales. O, en una realización, el usuario puede introducir las credenciales generadas de forma manual.

La figura 5-1 es un diagrama de flujo lógico que ilustra, desde la perspectiva del AP no RSN 12', el funcionamiento de un método, y un resultado de la ejecución de instrucciones de programa informático, de acuerdo con las realizaciones ilustrativas de la presente invención. De acuerdo con estas realizaciones ilustrativas, un método realiza, en el bloque 5A, una etapa de enviar desde un punto de acceso de red (no RSN) al menos una transmisión de baliza que comprende un identificador de conjunto de servicios y, en el bloque 5B, proporcionar, el punto de acceso de red (no RSN), un servicio de registro para un punto de acceso de red seguro que opera con el mismo identificador de conjunto de servicios. En una realización, la al menos una transmisión de baliza también incluye una indicación de capacidad que indica que el punto de acceso de red no RSN solo es capaz de registro RSN.

En una realización ilustrativa, el registro puede proceder tal como sigue. En el bloque 5C hay una etapa de asociarse, el punto de acceso no RSN, con el dispositivo de usuario tal como al aceptar una solicitud de asociación procedente del dispositivo de usuario y, en el bloque 5D, hay una etapa de recibir, el punto de acceso no RSN, tráfico http del dispositivo de usuario. Como anteriormente, este tráfico http puede ser tráfico ficticio o cualquier tráfico. En el bloque 5E hay una etapa de redirigir el tráfico a una página de portal y, para una realización específica, en la etapa 5F hay una etapa de formar una conexión http segura con el dispositivo de usuario para establecer

credenciales mediante las cuales el dispositivo de usuario puede acceder al punto de acceso de red seguro. En el bloque 5G hay, en una alternativa, una etapa de autenticar el dispositivo de usuario con la página de portal en la que el dispositivo de usuario crea las credenciales. En el bloque 5H hay, en otra alternativa, una etapa de autenticar el dispositivo de usuario con la página de portal en la que credenciales necesarias para asociarse con el punto de acceso (RSN) seguro se envían de la página de portal al dispositivo de usuario. Puede haber una asociación preliminar con el punto de acceso no seguro como se ha hecho notar anteriormente a continuación de la descripción de la figura 4. Y, en el bloque 51, hay una etapa de desasociarse, el punto de acceso no RSN, del dispositivo de usuario.

La figura 5-2 es un diagrama de flujo lógico que ilustra, desde la perspectiva del AP RSN 12', el funcionamiento de un método, y un resultado de la ejecución de instrucciones de programa informático, de acuerdo con las realizaciones ilustrativas de la presente invención. El nodo de acceso RSN se puede ubicar conjuntamente con el nodo de acceso no RSN tal como materializándose ambos en el mismo nodo pero realizando funciones marcadamente diferentes. En el bloque 5J, el nodo de acceso RSN transmite al menos una transmisión de baliza y, en el bloque 5K, en esta realización particular se encuentra la etapa de proporcionar, el punto de acceso RSN, un NAI de registro al dispositivo de usuario mientras el dispositivo de usuario se encuentra en un estado preasociado al punto de acceso RSN. En el bloque 5L se encuentra la etapa de recibir del dispositivo de usuario una solicitud de asociación que incluye el NAI de registro y, en el bloque 5M, hay una etapa de conceder al dispositivo de usuario un acceso (limitado) a la red para fines de creación de credenciales. Los bloques 5D a 5H de la figura 5-2 son los mismos que se han descrito anteriormente para los mismos bloques de la figura 5-1. Entonces, el punto de acceso RSN termina, en el bloque 5N, la asociación preliminar que se concedió en el bloque 5M, y forma, en el bloque 5O, una asociación con el dispositivo de usuario usando las credenciales y concede al dispositivo de usuario conectividad a Internet por medio del punto de acceso RSN.

Las realizaciones ilustrativas también abarcan un medio legible por ordenador no transitorio que contiene instrucciones de programa de software, en donde la ejecución de las instrucciones de programa de software por al menos un procesador de datos da como resultado la realización de operaciones que comprenden la ejecución de las etapas de método de las figuras 4 y 5-1 y 5-2 y sus varios párrafos anteriores relacionados.

Los diversos bloques mostrados en las figuras 4, 5-1 y 5-2 se pueden ver, por lo tanto, como etapas de método, y/o como operaciones que resultan del funcionamiento de código de programa informático, y/o como una pluralidad de elementos de circuito lógico acoplados construidos para llevar a cabo la función o funciones asociadas.

Las realizaciones ilustrativas también se refieren a un aparato que comprende un procesador y una memoria que incluye código de programa informático. La memoria y el código de programa informático están configurados para, con el procesador, dar lugar a que el aparato al menos reciba, en un dispositivo de usuario, al menos una transmisión de baliza de al menos un punto de acceso de red, y en respuesta a una determinación de que el dispositivo de usuario no tiene las credenciales necesarias para acoplarse con el punto de acceso de red, para formar una asociación preliminar con el punto de acceso de red, para enviar tráfico http (por ejemplo, ficticio) hacia el punto de acceso de red y en respuesta a redirigirse a, y formar una conexión http segura con, una página de portal, para autenticar el dispositivo de usuario con la página de portal y recibir, de la página de portal, credenciales necesarias para asociarse con el punto de acceso de red. La memoria y el código de programa informático están configurados adicionalmente, con el procesador, para terminar la asociación preliminar con el punto de acceso de red y para formar una asociación con el punto de acceso de red usando las credenciales recibidas con el fin de obtener conectividad a Internet por medio del punto de acceso de red.

En general, las diversas realizaciones ilustrativas pueden implementarse en hardware o circuitos de propósito especial, software, lógica, conjuntos de chips, por ejemplo, un conjunto de chips o conjuntos de chips de WLAN o cualquier combinación de los mismos. Por ejemplo, algunos aspectos pueden implementarse en hardware, mientras que otros aspectos pueden implementarse en firmware o software que puede ejecutarse por un controlador, microprocesador u otro dispositivo informático, aunque la invención no está limitada a lo mismo. Aunque pueden ilustrarse y describirse diversos aspectos de las realizaciones ilustrativas de la presente invención como diagramas de bloques, diagramas de flujo o usando alguna otra representación gráfica, se entiende bien que estos bloques, aparatos, sistemas, técnicas o métodos descritos en el presente documento pueden implementarse en, como ejemplos no limitantes, hardware, software, firmware, circuitos o lógica de propósito especial, hardware o controlador de propósito general u otros dispositivos informáticos, o alguna combinación de los mismos.

En ese sentido, se debería apreciar por lo tanto que al menos algunos aspectos de las realizaciones ilustrativas de las invenciones se pueden poner en práctica en diversos componentes tales como módulos y chips de circuito integrado, y que las realizaciones ilustrativas de la presente invención se pueden concretar en un aparato que se materializa como un circuito integrado. El circuito o circuitos integrados pueden comprender conjuntos de circuitos (así como posiblemente firmware) para materializar al menos uno o más de un procesador o procesadores de datos, un procesador o procesadores digitales de señales, conjuntos de circuitos de banda base y conjuntos de circuitos de radiofrecuencia que son configurables con el fin de operar de acuerdo con las realizaciones ilustrativas de la presente invención.

Diversas modificaciones y adaptaciones a las realizaciones ilustrativas anteriores de la presente invención pueden hacerse evidentes para los expertos en las materias pertinentes en vista de la descripción anterior, cuando se leen en conjunto con los dibujos adjuntos. No obstante, todas y cada una de las modificaciones seguirán cayendo dentro del alcance de las realizaciones no limitantes e ilustrativas de la presente invención.

Por ejemplo, aunque las realizaciones ilustrativas se han descrito anteriormente en el contexto de los sistemas de tipo IEEE 802, se debería apreciar que las realizaciones ilustrativas de la presente invención no están limitadas para su uso únicamente con este tipo particular de sistema de comunicación inalámbrica, y que estas se pueden aprovechar en otros sistemas de comunicación inalámbrica.

Se debería hacer notar que los términos "conectado", "acoplado", o cualquier variante de los mismos, quieren decir cualquier conexión o acoplamiento, o bien directo o bien indirecto, entre dos o más elementos, y pueden abarcar la presencia de uno o más elementos intermedios entre dos elementos que están "conectados" o "acoplados" entre sí. El acoplamiento o conexión entre los elementos puede ser físico, lógico, o una combinación de los mismos. Como se emplea en el presente documento, se puede considerar que dos elementos están "conectados" o "acoplados" entre sí mediante el uso de uno o más hilos, cables y/o conexiones eléctricas impresas, así como mediante el uso de energía electromagnética, tal como energía electromagnética que tiene unas longitudes de onda en la región de radiofrecuencia, la región de microondas y la región óptica (tanto visible como invisible), como varios ejemplos no limitantes y no exhaustivos.

Además, los diversos nombres usados para los parámetros descritos (por ejemplo, SSID, etc.) no pretenden ser limitantes a ningún respecto, debido a que estos parámetros se pueden identificar mediante cualquier nombre adecuado. Además, los diversos nombres asignados a diferentes comunicaciones de red (por ejemplo, HTTP, HTTPS, etc.) no pretenden ser limitantes a ningún respecto, debido a que estas diversas comunicaciones se pueden identificar mediante cualquier nombre adecuado.

Además, algunas de las características de las diversas realizaciones no limitantes e ilustrativas de la presente invención se pueden aprovechar sin el uso correspondiente de otras características. En ese sentido, la descripción anterior se debería considerar como meramente ilustrativa de los principios, enseñanzas y realizaciones ilustrativas de la presente invención, como se define por las reivindicaciones, y no como limitación de los mismos.

REIVINDICACIONES

1. Un aparato (10) que comprende:

al menos un procesador; y
al menos una memoria que incluye código de programa informático;

en el que la al menos una memoria con el código de programa informático está configurada con el al menos un procesador para dar lugar a que el aparato al menos:

reciba (4A) al menos una transmisión de baliza de al menos un punto de acceso de red (12, 12');
en respuesta a determinar que el aparato no tiene las credenciales necesarias para acoplarse con un punto de acceso de red seguro del al menos un punto de acceso de red, forme (4B) una asociación preliminar con una red indicada para proporcionar una capacidad de registro en línea;
durante la asociación preliminar, reciba o cree (4E) credenciales necesarias para asociarse al punto de acceso de red seguro; y
forme (4G) una asociación con el punto de acceso de red seguro usando las credenciales recibidas o creadas y obtenga conectividad a Internet por medio del punto de acceso de red seguro.

2. El aparato de acuerdo con la reivindicación 1, en el que la al menos una memoria con el código de programa informático está configurada con el al menos un procesador para dar lugar adicionalmente a que el aparato al menos:

envíe (4C) tráfico http hacia el al menos un punto de acceso con el que se forma la asociación preliminar; y
forme (4D) una conexión http segura con una página de portal a la que se redirige el aparato en respuesta a enviar el tráfico http;

en el que el aparato está configurado para recibir o crear las credenciales necesarias para asociarse al punto de acceso de red seguro mientras se encuentra en la conexión http segura con la página de portal.

3. El aparato de acuerdo con la reivindicación 2, donde, cuando está conectado con la página de portal, un usuario está habilitado para seleccionar, por medio del aparato, una generación de credenciales o bien automática o bien manual.

4. El aparato de acuerdo con la reivindicación 3, donde, con la generación de credenciales automática, el aparato recibe, de la página de portal, las credenciales generadas que comprenden uno de un nombre de usuario, una contraseña y un certificado de cliente; el aparato está configurado para almacenar las credenciales recibidas en la al menos una memoria, y el aparato está configurado para proporcionar automáticamente las credenciales almacenadas al punto de acceso de red seguro sin requerir que el usuario sea consciente del contenido de las credenciales.

5. El aparato de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en el que el al menos un punto de acceso de red comprende un punto de acceso de red no seguro que es un punto de acceso de red habilitado para red de seguridad no robusta, RSN, y el punto de acceso de red seguro que es un punto de acceso habilitado para RSN diferente;
en el que la al menos una transmisión de baliza recibida del al menos un punto de acceso de red comprende una primera transmisión de baliza recibida del punto de acceso de red no seguro que indica solo registro de red de seguridad robusta, RSN, y también una segunda baliza recibida del punto de acceso de red seguro, en el que la primera y la segunda balizas comprenden un mismo identificador de conjunto de servicios; y
la asociación preliminar se forma con el punto de acceso de red no seguro.

6. El aparato de acuerdo con la reivindicación 5, en el que el punto de acceso de red seguro y el punto de acceso de red no seguro se materializan en el mismo nodo físico que opera funcionalmente sobre una red segura y sobre una red no segura, respectivamente.

7. El aparato de acuerdo con la reivindicación 5, en el que la al menos una memoria con el código de programa informático está configurada con el al menos un procesador para dar lugar adicionalmente a que el aparato al menos:
termine (4F) la asociación preliminar formada con el punto de acceso de red no seguro, antes de formar (4G) la asociación entre el aparato y el punto de acceso de red seguro.

8. El aparato de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en el que el al menos un punto de acceso de red comprende solo el punto de acceso de red seguro, y la al menos una transmisión de baliza que se recibe comprende una baliza recibida solo del punto de acceso de red seguro que indica que el punto de acceso de red seguro soporta un registro en línea.

9. El aparato de acuerdo con la reivindicación 8, en el que la al menos una memoria con el código de programa informático está configurada con el al menos un procesador para dar lugar adicionalmente a que el aparato al menos:

mientras el aparato se encuentra en un estado preasociado, envíe una solicitud de un identificador de acceso de red de registro al punto de acceso de red seguro;
reciba el identificador de acceso de red de registro solicitado; y posteriormente
forme la asociación preliminar con el punto de acceso de red seguro usando el identificador de acceso de red y una autenticación solo de lado de servidor.

10. Un método que comprende:

recibir (4A), en un dispositivo de usuario (10), al menos una transmisión de baliza de al menos un punto de acceso de red (12, 12');
en respuesta a determinar que el dispositivo de usuario no tiene las credenciales necesarias para acoplarse con un punto de acceso de red seguro del al menos un punto de acceso de red, formar (4B) una asociación preliminar con una red indicada para proporcionar una capacidad de registro en línea;
durante la asociación preliminar, recibir o crear (4E), el dispositivo de usuario, credenciales necesarias para asociarse al punto de acceso de red seguro; y
formar (4G) una asociación entre el dispositivo de usuario y el punto de acceso de red seguro usando las credenciales recibidas o creadas y obtener conectividad a Internet por medio del punto de acceso de red seguro.

11. Un medio legible por ordenador no transitorio que incluye instrucciones de programa informático que, cuando son ejecutadas por al menos un procesador de datos, dan como resultado la realización de operaciones que comprenden:

recibir (4A), en un dispositivo de usuario (10), al menos una transmisión de baliza de al menos un punto de acceso de red (12, 12');
en respuesta a determinar que el dispositivo de usuario no tiene las credenciales necesarias para acoplarse con un punto de acceso de red seguro del al menos un punto de acceso de red, formar (4B) una asociación preliminar con una red indicada para proporcionar una capacidad de registro en línea;
durante la asociación preliminar, recibir o crear (4E), el dispositivo de usuario, credenciales necesarias para asociarse con el punto de acceso de red seguro; y
formar (4G) una asociación entre el dispositivo de usuario y el punto de acceso de red seguro usando las credenciales recibidas o creadas y obtener conectividad a Internet por medio del punto de acceso de red seguro.

12. Un aparato (12, 12') que comprende:

al menos un procesador; y
al menos una memoria que incluye código de programa informático;

en el que la al menos una memoria con el código de programa informático está configurada con el al menos un procesador para dar lugar a que el aparato al menos:

transmita (5J) al menos una transmisión de baliza;
indique una capacidad de registro en línea;
proporcione (5K) un identificador de acceso de red de registro a un dispositivo de usuario (10) mientras el dispositivo de usuario se encuentra en un estado preasociado al aparato;
reciba (5L) del dispositivo de usuario una solicitud de asociación que incluye el identificador de acceso de red de registro; y
conceda (5M) al dispositivo de usuario un acceso limitado a una red para fines de creación de credenciales.

13. El aparato de acuerdo con la reivindicación 12, en el que conceder al dispositivo de usuario un acceso limitado a la red para fines de creación de credenciales comprende:

establecer una asociación preliminar con el dispositivo de usuario;
redirigir (5E) tráfico http recibido del dispositivo de usuario a una página de portal;
formar (5F) una conexión http segura con el dispositivo de usuario para establecer las credenciales; y terminar (5N) la asociación preliminar con el dispositivo de usuario.

14. El aparato de acuerdo con las reivindicaciones 12 o 13, en donde el aparato comprende un punto de acceso de red de red de seguridad robusta, y la al menos una memoria con el código de programa informático está configurada con el al menos un procesador para dar lugar adicionalmente a que el aparato al menos:
forme (5O) una asociación con el dispositivo de usuario usando las credenciales y posteriormente conceda al dispositivo de usuario conectividad a Internet por medio del aparato.

15. Un método que comprende:

transmitir (5J) al menos una transmisión de baliza;
indicar una capacidad de registro en línea;
proporcionar (5K) un identificador de acceso de red de registro a un dispositivo de usuario (10) mientras el dispositivo de usuario se encuentra en un estado preasociado;
recibir (5L) del dispositivo de usuario una solicitud de asociación que incluye el identificador de acceso de red de registro; y
conceder (5M) al dispositivo de usuario un acceso limitado a una red para fines de creación de credenciales.

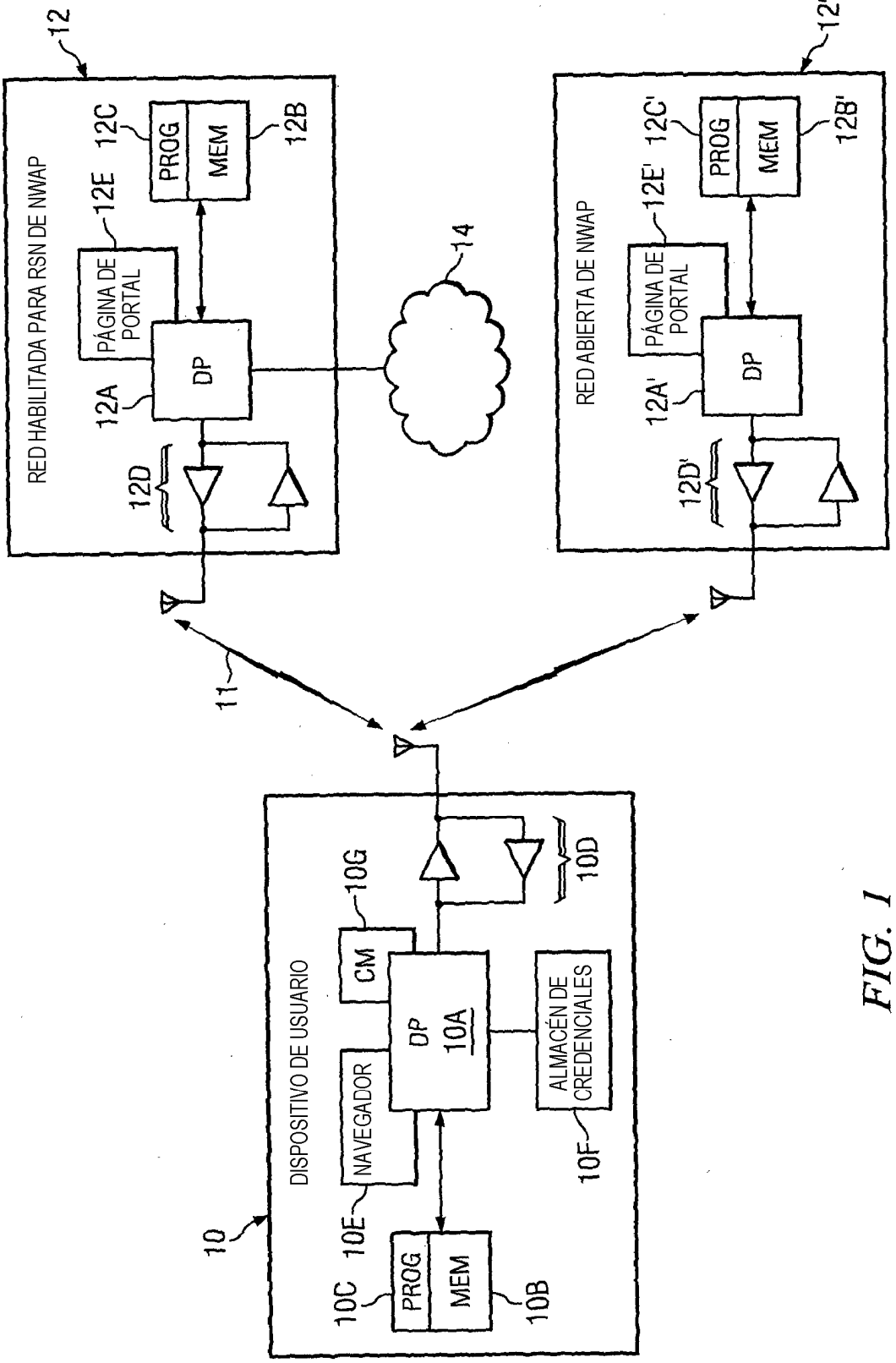
12
RED HABILITADA PARA RSN DE NWAP
12C
PROG
MEM
12B
12E
PÁGINA DE PORTAL
12A
DP
12D
14
12'
RED ABIERTA DE NWAP
12C'
PROG
MEM
12B'
12E'
PÁGINA DE PORTAL
12A'
DP
12D'
11
10
DISPOSITIVO DE USUARIO
10G
CM
10D
NAVEGADOR
DP
10A
ALMACÉN DE CREDENCIALES
10F
10E
10C
PROG
MEM
10B

FIG. 1

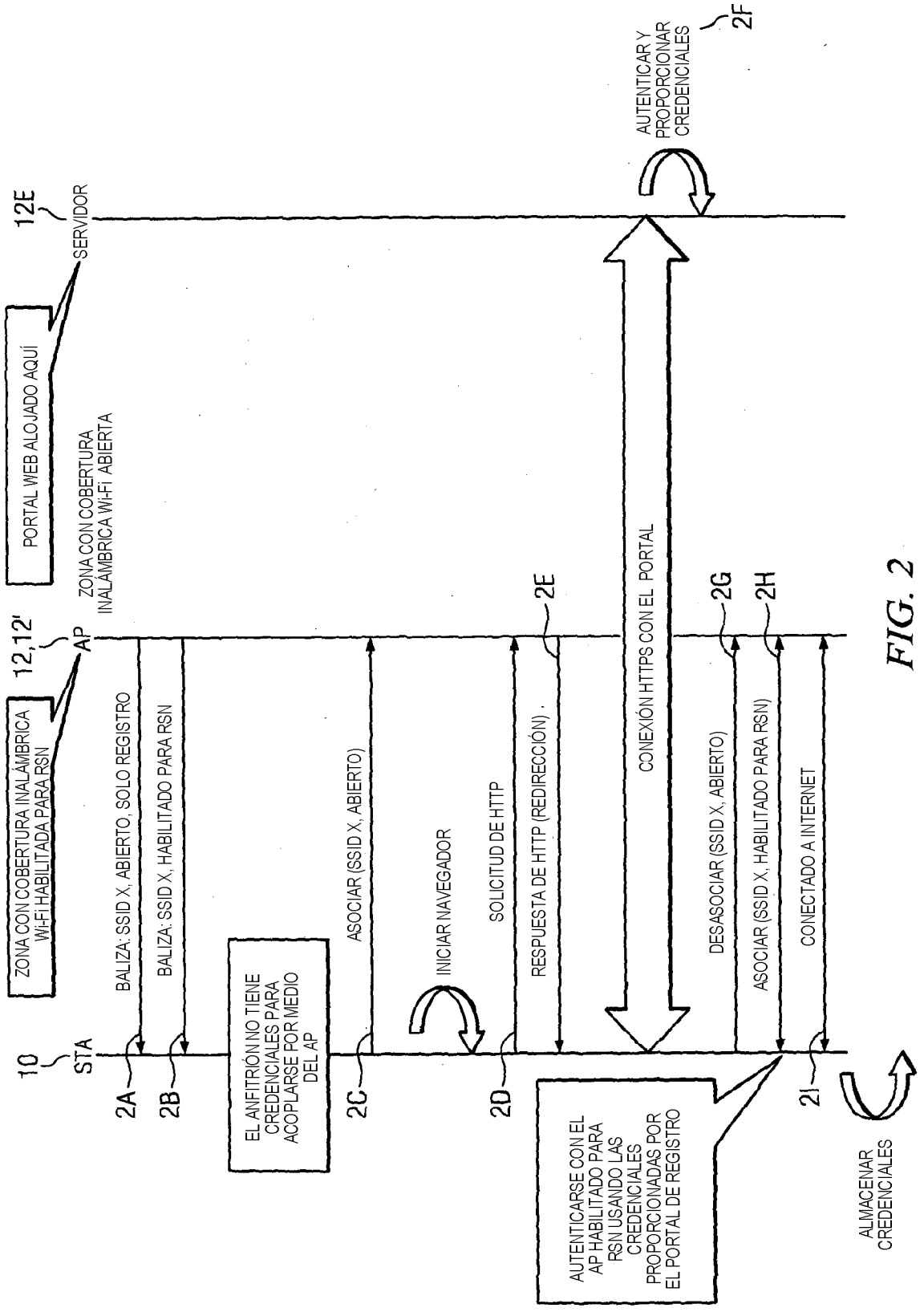
10
STA
12,12'
AP
12E
SERVIDOR
ZONA CON COBERTURA INALÁMBRICA Wi-Fi HABILITADA PARA RSN
PORTAL WEB ALOJADO AQUÍ
ZONA CON COBERTURA INALÁMBRICA Wi-Fi ABIERTA
2A
BALIZA: SSID X, ABIERTO, SOLO REGISTRO
2B
BALIZA: SSID X, HABILITADO PARA RSN
EL ANFITRIÓN NO TIENE CREDENCIALES PARA ACOPLARSE POR MEDIO DEL AP
2C
ASOCIAR (SSID X, ABIERTO)
INICIAR NAVEGADOR
2D
SOLICITUD DE HTTP
2E
RESPUESTA DE HTTP (REDIRECCIÓN)
CONEXIÓN HTTPS CON EL PORTAL
AUTENTICAR Y PROPORCIONAR CREDENCIALES
2F
2G
DESASOCIAR (SSID X, ABIERTO)
2H
ASOCIAR (SSID X, HABILITADO PARA RSN)
CONECTADO A INTERNET
AUTENTICARSE CON EL AP HABILITADO PARA RSN USANDO LAS CREDENCIALES PROPORCIONADAS POR EL PORTAL DE REGISTRO
2I
ALMACENAR CREDENCIALES

FIG. 2

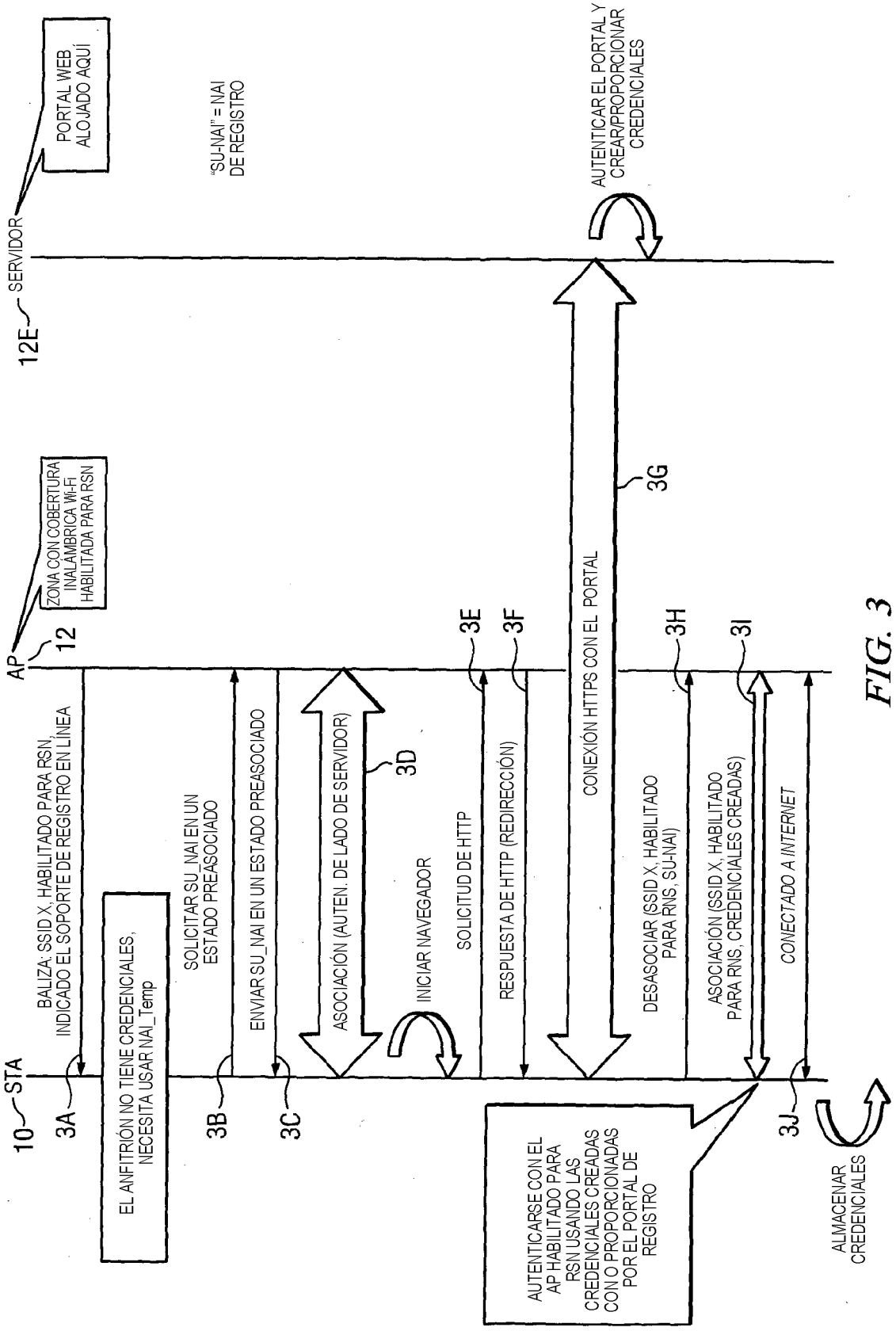
STA
10
AP
12
SERVIDOR
12E
PORTAL WEB ALOJADO AQUÍ
"SU-NAI" = NAI DE REGISTRO
ZONA CON COBERTURA INALÁMBRICA Wi-Fi HABILITADA PARA RSN
AUTENTICAR EL PORTAL Y CREAR/PROPORCIONAR CREDENCIALES
3A
BALIZA: SSID X, HABILITADO PARA RSN, INDICADO EL SOPORTE DE REGISTRO EN LÍNEA
EL ANFITRIÓN NO TIENE CREDENCIALES, NECESITA USAR NAI_Temp
3B
SOLICITAR SU_NAI EN UN ESTADO PREASOCIADO
3C
ENVIAR SU_NAI EN UN ESTADO PREASOCIADO
3D
ASOCIACIÓN (AUTEN. DE LADO DE SERVIDOR)
INICIAR NAVEGADOR
3E
SOLICITUD DE HTTP
3F
RESPUESTA DE HTTP (REDIRECCIÓN)
3G
CONEXIÓN HTTPS CON EL PORTAL
3H
DESASOCIAR (SSID X, HABILITADO PARA RNS, SU-NAI)
3I
ASOCIACIÓN (SSID X, HABILITADO PARA RNS, CREDENCIALES CREADAS)
CONECTADO A INTERNET
AUTENTICARSE CON EL AP HABILITADO PARA RSN USANDO LAS CREDENCIALES CREADAS CON O PROPORCIONADAS POR EL PORTAL DE REGISTRO
3J
ALMACENAR CREDENCIALES

FIG. 3

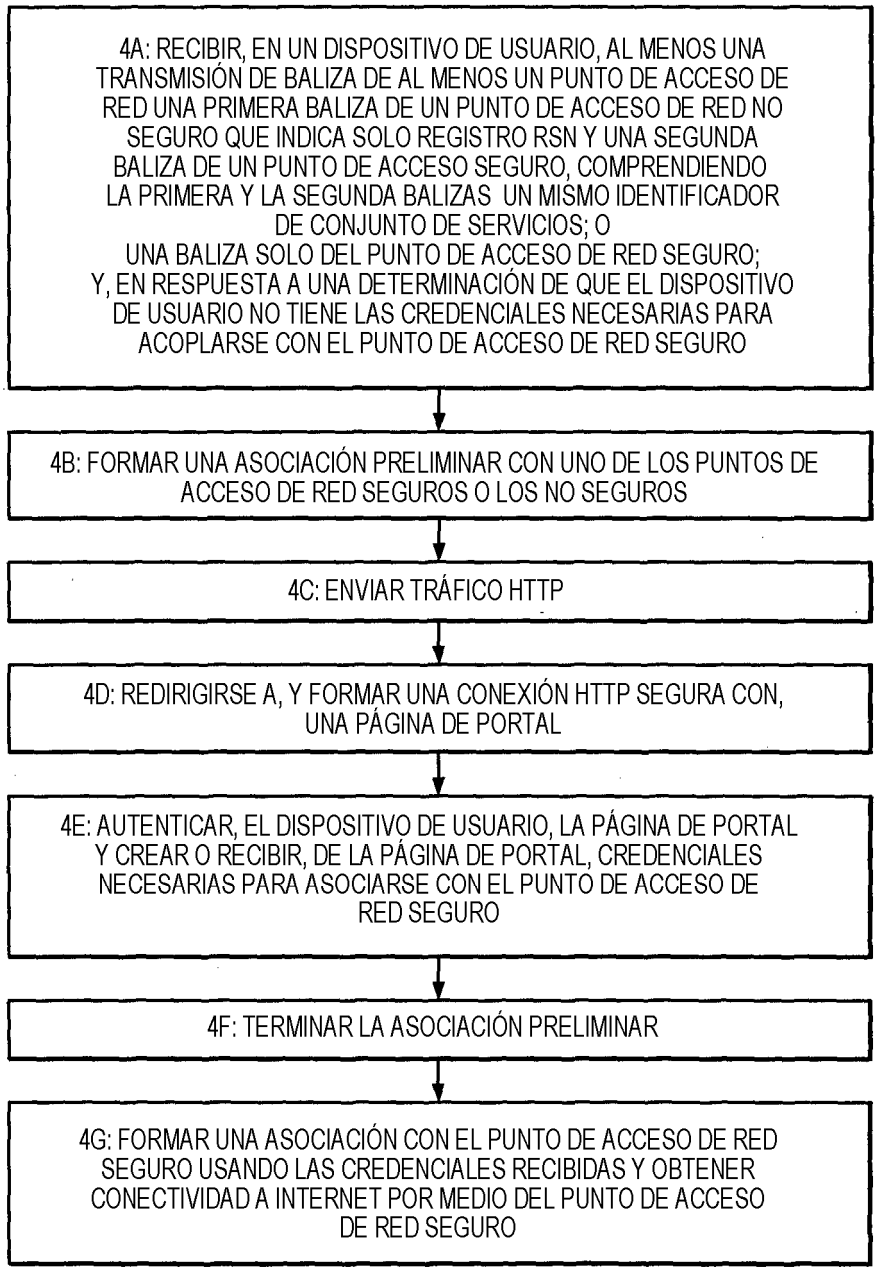
4A: RECIBIR, EN UN DISPOSITIVO DE USUARIO, AL MENOS UNA TRANSMISIÓN DE BALIZA DE AL MENOS UN PUNTO DE ACCESO DE RED UNA PRIMERA BALIZA DE UN PUNTO DE ACCESO DE RED NO SEGURO QUE INDICA SOLO REGISTRO RSN Y UNA SEGUNDA BALIZA DE UN PUNTO DE ACCESO SEGURO, COMPRENDIENDO LA PRIMERA Y LA SEGUNDA BALIZAS UN MISMO IDENTIFICADOR DE CONJUNTO DE SERVICIOS; O UNA BALIZA SOLO DEL PUNTO DE ACCESO DE RED SEGURO; Y, EN RESPUESTA A UNA DETERMINACIÓN DE QUE EL DISPOSITIVO DE USUARIO NO TIENE LAS CREDENCIALES NECESARIAS PARA ACOPLARSE CON EL PUNTO DE ACCESO DE RED SEGURO
4B: FORMAR UNA ASOCIACIÓN PRELIMINAR CON UNO DE LOS PUNTOS DE ACCESO DE RED SEGUROS O LOS NO SEGUROS
4C: ENVIAR TRÁFICO HTTP
4D: REDIRIGIRSE A, Y FORMAR UNA CONEXIÓN HTTP SEGURA CON, UNA PÁGINA DE PORTAL
4E: AUTENTICAR, EL DISPOSITIVO DE USUARIO, LA PÁGINA DE PORTAL Y CREAR O RECIBIR, DE LA PÁGINA DE PORTAL, CREDENCIALES NECESARIAS PARA ASOCIARSE CON EL PUNTO DE ACCESO DE RED SEGURO
4F: TERMINAR LA ASOCIACIÓN PRELIMINAR
4G: FORMAR UNA ASOCIACIÓN CON EL PUNTO DE ACCESO DE RED SEGURO USANDO LAS CREDENCIALES RECIBIDAS Y OBTENER CONECTIVIDAD A INTERNET POR MEDIO DEL PUNTO DE ACCESO DE RED SEGURO

FIG. 4

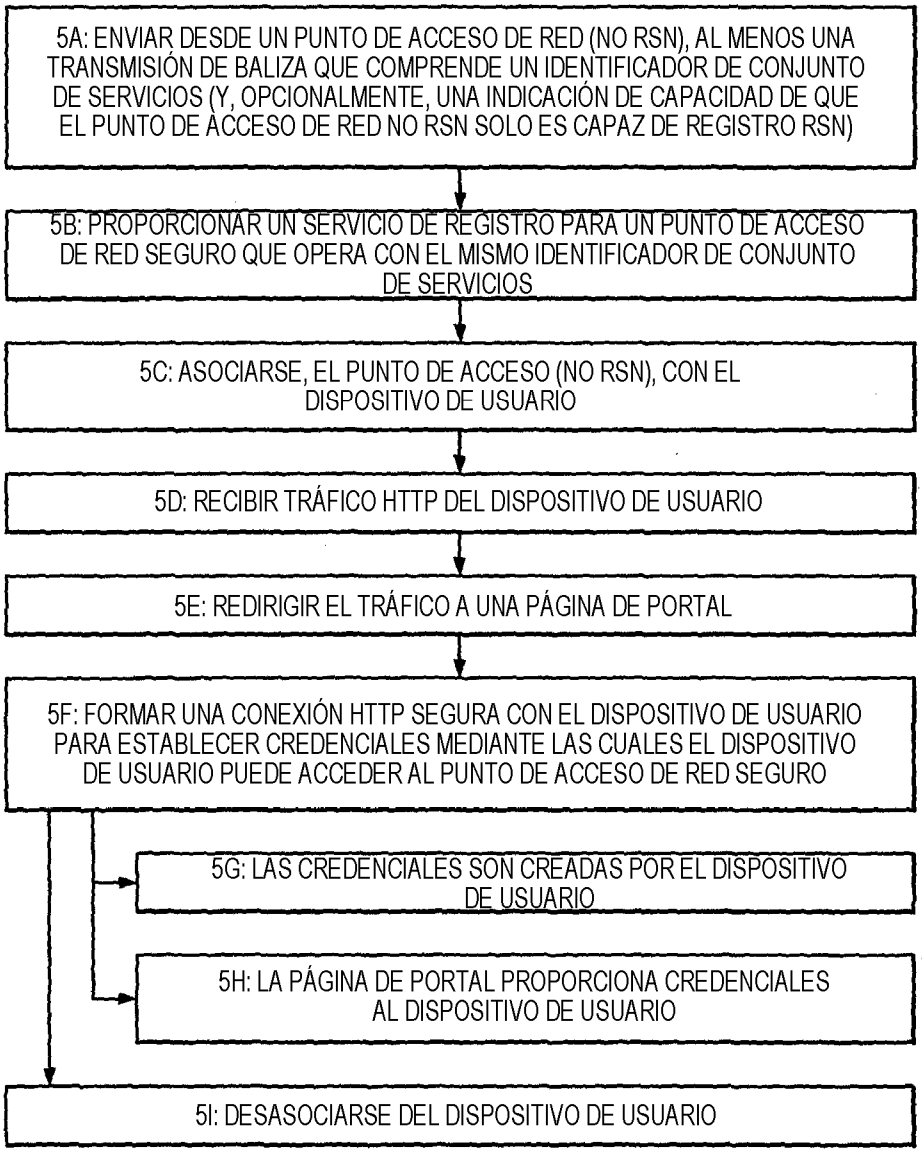
5A: ENVIAR DESDE UN PUNTO DE ACCESO DE RED (NO RSN), AL MENOS UNA TRANSMISIÓN DE BALIZA QUE COMPRENDE UN IDENTIFICADOR DE CONJUNTO DE SERVICIOS (Y, OPCIONALMENTE, UNA INDICACIÓN DE CAPACIDAD DE QUE EL PUNTO DE ACCESO DE RED NO RSN SOLO ES CAPAZ DE REGISTRO RSN)
5B: PROPORCIONAR UN SERVICIO DE REGISTRO PARA UN PUNTO DE ACCESO DE RED SEGURO QUE OPERA CON EL MISMO IDENTIFICADOR DE CONJUNTO DE SERVICIOS
5C: ASOCIARSE, EL PUNTO DE ACCESO (NO RSN), CON EL DISPOSITIVO DE USUARIO
5D: RECIBIR TRÁFICO HTTP DEL DISPOSITIVO DE USUARIO
5E: REDIRIGIR EL TRÁFICO A UNA PÁGINA DE PORTAL
5F: FORMAR UNA CONEXIÓN HTTP SEGURA CON EL DISPOSITIVO DE USUARIO PARA ESTABLECER CREDENCIALES MEDIANTE LAS CUALES EL DISPOSITIVO DE USUARIO PUEDE ACCEDER AL PUNTO DE ACCESO DE RED SEGURO
5G: LAS CREDENCIALES SON CREADAS POR EL DISPOSITIVO DE USUARIO
5H: LA PÁGINA DE PORTAL PROPORCIONA CREDENCIALES AL DISPOSITIVO DE USUARIO
5I: DESASOCIARSE DEL DISPOSITIVO DE USUARIO

FIG .5-1


5J: TRANSMITIR (EL PUNTO DE ACCESO RSN) AL MENOS UNA TRANSMISIÓN DE BALIZA
5K: PROPORCIONAR UN NAI DE REGISTRO A UN DISPOSITIVO DE USUARIO MIENTRAS EL DISPOSITIVO DE USUARIO SE ENCUENTRA EN UN ESTADO PREASOCIADO
5L: RECIBIR, DEL DISPOSITIVO DE USUARIO, UNA SOLICITUD DE ASOCIACIÓN CON EL NAI DE REGISTRO
5M: CONCEDER AL DISPOSITIVO DE USUARIO UN ACCESO A LA RED PARA FINES DE CREACIÓN DE CREDENCIALES
5D: RECIBIR TRÁFICO HTTP DEL DISPOSITIVO DE USUARIO
5E: REDIRIGIR EL TRÁFICO A UNA PÁGINA DE PORTAL
5F: FORMAR UNA CONEXIÓN HTTP SEGURA CON EL DISPOSITIVO DE USUARIO PARA ESTABLECER CREDENCIALES MEDIANTE LAS CUALES EL DISPOSITIVO DE USUARIO PUEDE ACCEDER AL PUNTO DE ACCESO DE RED SEGURO
5G: LAS CREDENCIALES SON CREADAS POR EL DISPOSITIVO DE USUARIO
5H: LA PÁGINA DE PORTAL PROPORCIONA CREDENCIALES AL DISPOSITIVO DE USUARIO
5N: TERMINAR LA ASOCIACIÓN PRELIMINAR CON EL DISPOSITIVO DE USUARIO
5O: FORMAR UNA ASOCIACIÓN CON EL DISPOSITIVO DE USUARIO USANDO LAS CREDENCIALES Y CONCEDER, AL DISPOSITIVO DE USUARIO, CONECTIVIDAD A INTERNET (POR MEDIO DEL PUNTO DE ACCESO RSN)

FIG. 5-2