(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 766 856**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 84/12 (2009.01)
H04L 29/06 (2006.01)
H04W 88/06 (2009.01)
H04W 4/80 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.09.2016 PCT/CN2016/097948**

(87) Fecha y número de publicación internacional: **06.04.2017 WO17054617**

(96) Fecha de presentación y número de la solicitud europea: **02.09.2016 E 16850241 (7)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2019 EP 3285513**

(54) Título: **Procedimiento, dispositivo y sistema de autentificación de red WiFi**

(30) Prioridad:

29.09.2015 CN 201510634506

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.06.2020

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

HUANG, ZHENGQUAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento, dispositivo y sistema de autentificación de red WiFi

Campo técnico

La presente invención se refiere al campo de las comunicaciones y, en particular, a un procedimiento, un aparato y un sistema para autenticar una red WiFi.

Antecedentes

La tecnología de comunicaciones de fidelidad inalámbrica (WiFi) ha sido promovida y aplicada masivamente debido a su banda de frecuencia de comunicación libre. Con la amplia aplicación de la tecnología de comunicaciones WiFi, la seguridad de una red WiFi se vuelve cada vez más importante.

Debido a que cualquier persona o institución puede establecer o configurar una red WiFi y la red WiFi está abierta a terminales, existen algunas redes ilegales, tal como las redes de fraude electrónico. Las redes de fraude electrónico se enmascaran como ciertas redes WiFi públicas que proporcionan servicios de acceso inalámbrico para el público general, por ejemplo, una red WiFi establecida por un operador o una red WiFi establecida por un gobierno, una escuela u otras instituciones públicas, y engañan a los usuarios para que accedan a redes ilegales, a fin de robar elementos de privacidad personal, información confidencial, y similares. Por ejemplo, una red de fraude electrónico puede usar un identificador de conjunto de servicios (por sus siglas en inglés, SSID) y una pantalla de autenticación de inicio de sesión que son iguales que las de una red WiFi pública, y también requerir que un usuario ingrese un comprobante de inicio de sesión, tal como un nombre de usuario o una contraseña en la pantalla de autenticación. Sin embargo, se usa un modo de acceso abierto cuando el inicio de sesión se implementa dentro de la red de fraude electrónico, es decir, se puede acceder a la red de fraude electrónico sin ningún nombre de usuario o contraseña. Por lo tanto, independientemente de la información ingresada por el usuario, el usuario puede acceder con éxito a la red de fraude electrónico, de modo que el usuario es engañado para acceder a la red de fraude electrónico. Sin embargo, en vista del nombre de SSID o la pantalla de inicio de sesión, el usuario puede creer erróneamente que ha accedido a una red WiFi pública auténtica. Cuando el usuario realiza compras en línea o pagos en línea utilizando la red de fraude electrónico accedida, la privacidad personal y la información confidencial del usuario son bastante vulnerables al robo por parte de la red de fraude electrónico y el usuario es vulnerable a una gran pérdida.

Los motivos de vulnerabilidad de una red WiFi pública a la falsificación son que la red WiFi es abierta y gratuita, y lo que es más importante, es que la red WiFi pública no proporciona un mecanismo de autenticación de acceso perfecto.

Actualmente, para facilitar el uso de la red WiFi pública, normalmente se usan ciertas formas de autenticación de acceso fáciles de operar para acceder a la red WiFi pública. Por ejemplo, la autenticación se realiza usando un código de verificación de mensaje SMS en un teléfono móvil o mediante el barrido de un código de respuesta rápida. Tales formas de autenticación de acceso son generalmente de autenticación unidireccional, es decir, solo una red, tal como una red celular inalámbrica o una red WiFi pública, autentica una terminal. Por lo tanto, dichas formas de autenticación de acceso no pueden evitar que los proveedores de red no autorizados usen una red de suplantación de identidad o una red de fraude electrónico para engañar a un usuario mediante la falsificación de una red WiFi pública auténtica. Una red WiFi pública con accesibilidad abierta es aún más fácil de falsificar.

En conclusión, debido a que una red WiFi pública no proporciona un mecanismo de autenticación de acceso perfecto, no se puede garantizar la seguridad de la información de un usuario de la terminal en un procedimiento de autenticación cuando el usuario accede a la red WiFi pública.

El documento US 2005/0176407 A1 desvela un procedimiento y un sistema para autenticar a un usuario de un dispositivo de transferencia de datos. El sistema de comunicaciones móviles verifica si los datos de identificación de suscriptor móvil ingresados contienen un derecho de acceso al punto de acceso al servicio. Si existe un derecho de acceso válido, se genera una contraseña, que luego se transmite a una terminal de suscriptor (por ejemplo, un teléfono móvil GSM) correspondiente a los datos de identificación del suscriptor móvil.

El documento WO 2005/013582 A2 desvela un mecanismo para mejorar la seguridad y el control de acceso a través de una red, tal como una red de área local inalámbrica (por sus siglas en inglés, "WLAN"), que aprovecha las interacciones del navegador web sin requerir una sesión de comunicación separada explícita entre una red de puntos de acceso y una red de proveedores de servicios.

Sumario

Las realizaciones de la presente invención proporcionan un procedimiento, un aparato y un sistema para autenticar una red WiFi, a fin de resolver el problema de que no se puede garantizar la seguridad de la información de un usuario terminal en un procedimiento de autenticación cuando el usuario accede a una red WiFi. Las soluciones técnicas específicas proporcionadas en las realizaciones de la presente invención son las siguientes:

De acuerdo con un primer aspecto, se proporciona un procedimiento para autenticar una red WiFi, que incluye:

enviar, mediante una terminal cuando se determina que existe una red WiFi en un área en la que se ubica la terminal, un mensaje de solicitud a un centro de autenticación asociado, en el que el mensaje de solicitud porta un primer identificador de usuario, y recibir la información de verificación de acceso enviada por el centro de autenticación asociado y asignada por el centro de autenticación asociado a un usuario representado por el primer identificador de usuario;

enviar, mediante la terminal, una solicitud de inicio de sesión a un centro de autenticación de WiFi en la red WiFi, en el que la solicitud de inicio de sesión porta la información de verificación de acceso, y recibir la información de autenticación retroalimentada por el centro de autenticación de WiFi y usada para responder a la solicitud de inicio de sesión, en el que la información de autenticación porta un segundo identificador de usuario; y

determinar, mediante la terminal cuando el segundo identificador de usuario portado en la información de autenticación es igual que el primer identificador de usuario, que la red WiFi es una red segura.

Con referencia al primer aspecto, en una primera implementación posible del primer aspecto, el identificador de usuario incluye un número ISDN internacional de la estación móvil (Número ISDN internacional de la estación móvil, por sus siglas en inglés MSISDN) o una identidad.

Con referencia al primer aspecto, en una segunda implementación posible del primer aspecto, la determinación, mediante una terminal, de que existe una red WiFi en un área en la que se ubica la terminal incluye:

buscar, mediante la terminal, una red WiFi en el área en la que se ubica la terminal, y determinar, de acuerdo con el resultado de la búsqueda, que existe una red WiFi en el área en la que se ubica la terminal.

De acuerdo con un segundo aspecto, se proporciona un procedimiento para autenticar una red WiFi, que incluye:

recibir, mediante un centro de autenticación de WiFi, una solicitud de inicio de sesión enviada por una terminal para iniciar sesión en una red WiFi en la que se ubica el centro de autenticación de WiFi, en la que la solicitud de inicio de sesión porta información de verificación de acceso;

enviar, mediante el centro de autenticación de WiFi a un centro de autenticación asociado, la información de verificación de acceso portada en la solicitud de inicio de sesión, y

recibir un identificador de usuario correspondiente a la información de verificación de acceso y retroalimentada por el centro de autenticación asociado; y

añadir, mediante el centro de autenticación de WiFi, el identificador de usuario a información de autenticación, y enviar, a la terminal, la información de autenticación que porta el identificador de usuario.

De acuerdo con un tercer aspecto, se proporciona un procedimiento para autenticar una red WiFi, que incluye:

asignar, mediante un centro de autenticación asociado cuando se recibe un mensaje de solicitud que porta un identificador de usuario, información de verificación de acceso al identificador de usuario, y almacenar de forma correspondiente el identificador de usuario y la información de verificación de acceso asignada al identificador de usuario;

notificar, mediante el centro de autenticación asociado, la información de verificación de acceso a una terminal usada por un usuario representado por el identificador de usuario;

recibir, mediante el centro de autenticación asociado, la información de verificación de acceso enviada por el centro de autenticación de WiFi; y

consultar el identificador de usuario almacenado correspondientemente de acuerdo con la información de verificación de acceso, y retroalimentar el identificador de usuario hallado en el centro de autenticación de WiFi.

Con referencia al tercer aspecto, en una primera implementación posible del tercer aspecto, la notificación, mediante el centro de autenticación asociado, de la información de verificación de acceso a una terminal usada por un usuario representado por el identificador de usuario incluye:

notificar, mediante el centro de autenticación asociado, la información de verificación de acceso a la terminal mediante el uso de una red celular inalámbrica en la forma de un mensaje SMS, un código de respuesta rápida o un código de barras.

De acuerdo con un cuarto aspecto, se proporciona un sistema para autenticar una red WiFi, que incluye:

una terminal, configurada para: cuando se determina que existe una red WiFi en un área en la que se ubica la terminal, enviar un mensaje de solicitud a un centro de autenticación asociado, en el que el mensaje de solicitud porta un primer identificador de usuario, y recibir la información de verificación de acceso enviada por el centro de autenticación asociado y asignada por el centro de autenticación asociado a un usuario representado por el primer identificador de

usuario; enviar una solicitud de inicio de sesión a un centro de autenticación de WiFi en la red WiFi, en el que la solicitud de inicio de sesión porta la información de verificación de acceso; recibir información de autenticación retroalimentada por el centro de autenticación de WiFi y usada para responder a la solicitud de inicio de sesión, en el que la información de autenticación porta un segundo identificador de usuario; y cuando el segundo identificador de usuario portado en la información de autenticación es igual que el primer identificador de usuario, determinar que la red WiFi es una red segura;

el centro de autenticación de WiFi, configurado para: recibir la solicitud de inicio de sesión enviada por la terminal para iniciar sesión en la red WiFi en la que se ubica el centro de autenticación de WiFi; enviar, al centro de autenticación asociado, la información de verificación de acceso portada en la solicitud de inicio de sesión, y recibir un identificador de usuario correspondiente a la información de verificación de acceso y retroalimentada por el centro de autenticación asociado; y añadir el identificador de usuario a la información de autenticación, y enviar, a la terminal, la información de autenticación que porta el identificador de usuario; y

el centro de autenticación asociado, configurado para: cuando se recibe el mensaje de solicitud que porta el identificador de usuario, asignar la información de verificación de acceso al identificador de usuario, y almacenar de forma correspondiente el identificador de usuario y la información de verificación de acceso asignada al identificador de usuario; notificar la información de verificación de acceso a la terminal usada por un usuario representado por el identificador de usuario; recibir la información de verificación de acceso enviada por el centro de autenticación de WiFi; y consultar el identificador de usuario almacenado correspondientemente de acuerdo con la información de verificación de acceso, y retroalimentar el identificador de usuario hallado al centro de autenticación de WiFi.

De acuerdo con un quinto aspecto, se proporciona un aparato para autenticar una red WiFi, que incluye:

una primera unidad transceptora, configurada para: cuando se determina que existe una red WiFi en un área en la que se ubica el aparato, enviar un mensaje de solicitud a un centro de autenticación asociado, en el que el mensaje de solicitud porta un primer identificador de usuario, y recibir la información de verificación de acceso enviada por el centro de autenticación asociado y asignada por el centro de autenticación asociado a un usuario representado por el primer identificador de usuario;

una segunda unidad transceptora, configurada para: enviar una solicitud de inicio de sesión a un centro de autenticación de WiFi en la red WiFi, en el que la solicitud de inicio de sesión porta la información de verificación de acceso, y recibir la información de autenticación retroalimentada por el centro de autenticación de WiFi y usada para responder a la solicitud de inicio de sesión, en el que la información de autenticación porta un segundo identificador de usuario; y

una unidad de procesamiento, configurada para: cuando el segundo identificador de usuario portado en la información de autenticación es igual que el primer identificador de usuario, determinar que la red WiFi es una red segura.

Con referencia al quinto aspecto, en una primera implementación posible del quinto aspecto, el identificador de usuario incluye un MSISDN o una identidad.

Con referencia al quinto aspecto, en una segunda implementación posible del quinto aspecto, el aparato también incluye:

una unidad de detección, configurada para: buscar una red WiFi en el área en la que se ubica el aparato, y determinar, de acuerdo con el resultado de la búsqueda, que existe una red WiFi en el área en la que se ubica el aparato.

De acuerdo con un sexto aspecto, se proporciona un aparato para autenticar una red WiFi, que incluye:

una primera unidad transceptora, configurada para recibir una solicitud de inicio de sesión enviada mediante una terminal para iniciar sesión en una red WiFi en la que se ubica el centro de autenticación de WiFi, en la que la solicitud de inicio de sesión porta información de verificación de acceso; y

una segunda unidad transceptora, configurada para: enviar, a un centro de autenticación asociado, la información de verificación de acceso portada en la solicitud de inicio de sesión, y

recibir un identificador de usuario correspondiente a la información de verificación de acceso y retroalimentarlo mediante el centro de autenticación asociado, en el que

la primera unidad transceptora también está configurada para: añadir el identificador de usuario a la información de autenticación, y enviar, a la terminal, la información de autenticación que porta el identificador de usuario.

De acuerdo con un séptimo aspecto, se proporciona un aparato para autenticar una red WiFi, que incluye:

una unidad de asignación, configurada para: cuando se recibe un mensaje de solicitud que porta un identificador de usuario, asignar información de verificación de acceso al identificador de usuario;

una primera unidad transceptora, configurada para: almacenar de forma correspondiente el identificador de usuario y

la información de verificación de acceso asignada al identificador de usuario, y notificar la información de verificación de acceso a una terminal usada por un usuario representado por el identificador de usuario; y

una segunda unidad transceptora, configurada para: recibir la información de verificación de acceso enviada mediante un centro de autenticación de WiFi; y

consultar el identificador de usuario almacenado correspondientemente de acuerdo con la información de verificación de acceso, y retroalimentar el identificador de usuario hallado al centro de autenticación de WiFi.

Con referencia al séptimo aspecto, en una primera implementación posible del séptimo aspecto, la primera unidad transceptora también está configurada para:

notificar la información de verificación de acceso a la terminal mediante el uso de una red celular inalámbrica en la forma de un mensaje SMS, un código de respuesta rápida o un código de barras.

En las realizaciones de la presente invención, la terminal envía el mensaje de solicitud al centro de autenticación asociado para solicitar el acceso a la red WiFi, en el que el mensaje de solicitud porta el primer identificador de usuario. La autenticidad de la red WiFi se verifica indirectamente mediante la determinación de si la red WiFi a la que se accede se puede interconectar a un centro de autenticación asociado de confianza. Es decir, la autenticación se realiza en la red WiFi a la que se accede mediante el uso de la información de autenticación retroalimentada por el centro de autenticación de WiFi y que porta el segundo identificador de usuario. De esta forma, el centro de autenticación asociado examina estrictamente la autenticidad y la seguridad de la red WiFi cuando el centro de autenticación de WiFi está interconectado al centro de autenticación asociado. Esto asegura no solo la autenticidad y seguridad de una red en la que se ubica el centro de autenticación asociado, sino también la autenticidad y seguridad de la red WiFi a la que se accede. Por lo tanto, se puede asegurar la seguridad de la información de un usuario de la terminal.

Breve descripción de los dibujos

La FIG. 1 es un diagrama esquemático de un procedimiento de autenticación de acceso a una red WiFi pública mediante una terminal de WiFi de la técnica anterior;

La FIG. 2 es un diagrama esquemático de una arquitectura del sistema de autenticación de canal dual de acuerdo con una realización de la presente invención;

La FIG. 3 es un diagrama esquemático de un procedimiento de autenticación de una red WiFi de acuerdo con una realización de la presente invención;

La FIG. 4 es un diagrama esquemático de una arquitectura del sistema de autenticación de canal dual en un escenario de aplicación práctica de acuerdo con una realización de la presente invención;

La FIG. 5 es un diagrama esquemático de un procedimiento de autenticación de canal dual en un escenario de aplicación práctica de acuerdo con una realización de la presente invención;

La FIG. 6 es un diagrama esquemático de un procedimiento de autenticación de canal dual en otro escenario de aplicación práctica de acuerdo con una realización de la presente invención;

La FIG. 7 es un diagrama estructural de un primer aparato para autenticar una red WiFi de acuerdo con una realización de la presente invención;

La FIG. 8 es un diagrama estructural de un segundo aparato para autenticar una red WiFi de acuerdo con una realización de la presente invención;

La FIG. 9 es un diagrama estructural de un tercer aparato para autenticar una red WiFi de acuerdo con una realización de la presente invención;

La FIG. 10 es un diagrama estructural de una terminal de acuerdo con una realización de la presente invención;

La FIG. 11 es un diagrama estructural de un primer dispositivo para autenticar una red WiFi de acuerdo con una realización de la presente invención; y

La FIG. 12 es un diagrama estructural de un segundo dispositivo para autenticar una red WiFi de acuerdo con una realización de la presente invención.

Descripción de realizaciones

Lo siguiente describe clara y completamente las soluciones técnicas en las realizaciones de la presente invención con referencia a los dibujos adjuntos en las realizaciones de la presente invención. Evidentemente, las realizaciones descritas simplemente son algunas pero no todas las realizaciones de la presente invención. Todas las otras realizaciones obtenidas por los expertos en la técnica en base a las realizaciones de la presente invención sin esfuerzos creativos están dentro del ámbito de la presente invención.

Con referencia a la FIG. 1, la FIG. 1 muestra un procedimiento de autenticación para acceder a una red WiFi mediante el uso de un código de verificación de mensaje SMS en la técnica anterior. Generalmente, una red WiFi pública establecida por un operador y una red celular inalámbrica se complementan entre sí. La red WiFi pública generalmente incluye una terminal de WiFi 1 y un centro de autenticación de WiFi 3, y la red celular inalámbrica incluye una terminal celular 2 y un centro de autenticación asociado 4. Opcionalmente, el centro de autenticación asociado 4 de la presente memoria puede ser un servidor de suscriptor doméstico (HSS), un registro de ubicación local (HLR) o un centro de autenticación (AuC) que está dispuesto en el lado de la red celular inalámbrica. Cuando un usuario requiere acceder a la red WiFi pública del operador, generalmente se requiere una terminal celular 2 (un teléfono móvil en la presente memoria) para obtener en primer lugar un código de verificación de mensaje SMS del centro de autenticación asociado 4 en la red celular inalámbrica. Luego, el código de verificación del mensaje SMS y un número de teléfono móvil se ingresan en una pantalla de inicio de sesión de red WiFi pública de la terminal de WiFi 1. El centro de autenticación de WiFi 3 en la red WiFi pública transmite el código de verificación de mensaje SMS ingresado y el número de teléfono móvil ingresado al centro de autenticación asociado 4, y el centro de autenticación asociado 4 verifica el código de verificación del mensaje SMS y el número de teléfono móvil. Después de que la verificación tiene éxito, se envía un mensaje de éxito de autenticación al centro de autenticación de WiFi, y la terminal de WiFi 1 puede acceder a la red WiFi pública. Si la verificación falla, se envía un mensaje de falla de autenticación al centro de autenticación de WiFi y se rechaza el acceso de la terminal de WiFi 1 a la red WiFi pública. La FIG. 1 muestra el procedimiento general.

En base al mecanismo de atención y al procedimiento de acceso a una red WiFi usando un código de verificación de mensaje SMS en la técnica anterior, con referencia a la FIG. 2, una realización de la presente invención proporciona un sistema de autenticación de canal dual que incluye una terminal de WiFi 1, un centro de autenticación de WiFi 2, y un centro de autenticación asociado 3.

La terminal de WiFi 1 está configurada para: cuando se determina que existe una red WiFi en un área en la que se ubica la terminal de WiFi, enviar un mensaje de solicitud al centro de autenticación asociado 3, en el que el mensaje de solicitud porta un primer identificador, y recibir la información de verificación de acceso enviada por el centro de autenticación asociado 3 y asignada a un usuario representado por el primer identificador de usuario; enviar una solicitud de inicio de sesión al centro de autenticación de WiFi 2 en la red WiFi, en el que la solicitud de inicio de sesión porta la información de verificación de acceso; recibir la información de autenticación retroalimentada por el centro de autenticación de WiFi 2 y usada para responder a la solicitud de inicio de sesión, en la que la información de autenticación porta un segundo identificador de usuario; y cuando el segundo identificador de usuario portado en la información de autenticación es igual que el primer identificador de usuario, determinar que la red WiFi es una red segura.

El centro de autenticación de WiFi 2 está configurado para: recibir la solicitud de inicio de sesión enviada por la terminal de WiFi 1 para iniciar sesión en la red WiFi en la que se ubica el centro de autenticación de WiFi 2, en la que la solicitud de inicio de sesión porta la información de verificación de acceso; enviar, al centro de autenticación asociado 3, la información de verificación de acceso portada en la solicitud de inicio de sesión, y recibir un identificador de usuario correspondiente a la información de verificación de acceso y retroalimentada por el centro de autenticación asociado 3; y añadir el identificador de usuario a la información de autenticación, y enviar, a la terminal de WiFi 1, la información de autenticación, que porta el identificador de usuario.

El centro de autenticación asociado 3 está configurado para: cuando se recibe el mensaje de solicitud que porta el identificador de usuario, asignar la información de verificación de acceso al identificador de usuario, y almacenar de forma correspondiente el identificador de usuario y la información de verificación de acceso asignada al identificador de usuario; notificar la información de verificación de acceso a la terminal de WiFi 1 usada por un usuario representado por el identificador de usuario; recibir la información de verificación de acceso enviada mediante el centro de autenticación de WiFi 2; y consultar el identificador de usuario almacenado de forma correspondiente de acuerdo con la información de verificación de acceso, y retroalimentar el identificador de usuario hallado al centro de autenticación de WiFi 2.

En base al sistema de autenticación de canal dual que se muestra en la FIG. 2, una realización de la presente invención proporciona un mecanismo de autenticación de red WiFi. El mecanismo de autenticación es una mejora del mecanismo de autenticación de la técnica anterior en el que la autenticación se realiza en una red WiFi a la que se accede mediante el uso de un código de verificación de mensaje SMS. En base a un sistema de autenticación que se muestra en la FIG. 2, en un procedimiento en el que una terminal de WiFi accede a una red WiFi, es decir, la red WiFi puede autenticar la terminal de WiFi, pero lo que es más importante, antes o después de que la terminal de WiFi acceda a la red WiFi, un centro de autenticación de WiFi en la red WiFi proporciona a la terminal de WiFi información de identificación del usuario de la terminal de WiFi que accede a la red WiFi, y la terminal de WiFi autentica la red WiFi de acuerdo con la información de identificación del usuario obtenida. Esto evita la suplantación de identidad de la red WiFi a la que se accede y mejora la seguridad de la red.

Específicamente, los canales duales en el sistema de autenticación de canal dual que se muestran en la FIG. 2 son un canal asociado y un canal de autenticación. El canal asociado es un canal usado mediante el centro de autenticación asociado 3 para transmitir la información de verificación de acceso de la red WiFi a la terminal de WiFi 1 mediante el uso de una red asociada. El canal de autenticación es un canal usado mediante el centro de autenticación de WiFi 2 para transmitir la información de autenticación a la terminal de WiFi 1 mediante el uso de la

red WiFi, después de obtener la información de autenticación del centro de autenticación asociado 3. Cabe señalar que, en la aplicación práctica, el centro de autenticación de WiFi 2 y el centro de autenticación asociado 3 se pueden implementar en forma integrada o separada de acuerdo con un requerimiento real. Para facilitar la descripción, se supone que el centro de autenticación de WiFi 2 y el centro de autenticación asociado 3 se implementan por separado en esta realización de la presente invención.

En base al sistema de autenticación de canal dual que se muestra en la FIG. 2, una realización de la presente invención proporciona un procedimiento para autenticar una red WiFi. La FIG. 3 muestra una relación de interacción entre dispositivos y un procedimiento de autenticación en el sistema de autenticación de canal dual. Un procedimiento de autenticación de una red WiFi incluye dos etapas: una etapa de asociación y una etapa de autenticación. La etapa de asociación incluye el paso 1 al paso 3, y la etapa autenticación indica el paso 4 al paso 9.

Paso 1: Cuando se determina, mediante barrido, que existe una red WiFi en un área en la que se ubica una terminal de WiFi 1, la terminal de WiFi 1 envía un mensaje de solicitud a un centro de autenticación asociado 3, en el que el mensaje de solicitud porta un primer identificador de usuario.

La terminal de WiFi 1 en esta realización de la presente invención puede ser cualquier terminal con una función WiFi tal como una tableta (dispositivo Android portátil, por sus siglas en inglés PAD), un teléfono inteligente o un ordenador portátil; y el identificador de usuario puede ser uno de los siguientes identificadores: un número de teléfono móvil, una identidad de suscriptor móvil internacional (IMSI), un identificador de tarjeta de identidad, un identificador de tarjeta de seguridad social o un identificador de pasaporte.

El paso 1 se puede realizar después de que la terminal de WiFi 1 determina que la terminal de WiFi 1 ha accedido a la red WiFi, o se puede realizar cuando la terminal de WiFi 1 determina que la terminal de WiFi 1 no ha accedido a la red WiFi.

El enfoque y una forma de solicitud, mediante la terminal de WiFi 1, para obtener información de verificación de acceso del centro de autenticación asociado 3 no están específicamente limitados. Mediante el uso de una red celular inalámbrica, la terminal de WiFi 1 puede solicitar obtener, del centro de autenticación asociado 3, la información de verificación de acceso asignada al primer identificador de usuario. Si la terminal de WiFi 1 tiene una función de comunicación celular, mediante el uso de la red celular inalámbrica, la terminal de WiFi 1 puede solicitar directamente obtener la información de verificación de acceso del centro de autenticación asociado 3. Si la terminal de WiFi 1 no tiene función de comunicación celular, mediante el uso de la red celular inalámbrica, otro dispositivo con la función de comunicación celular puede solicitar obtener, del centro de autenticación asociado 3, la información de verificación de acceso asignada al primer identificador de usuario. Si la terminal de WiFi 1 ha accedido a la red WiFi de antemano, mediante el uso de la red WiFi, la terminal de WiFi 1 alternativamente puede solicitar obtener, del centro de autenticación asociado 3, la información de verificación de acceso asignada al primer identificador de usuario. Incluso se puede usar un servicio dedicado provisto por el centro de autenticación asociado 3 para solicitar obtener, del centro de autenticación asociado 3, la información de verificación de acceso asignada al primer identificador de usuario. Por ejemplo, mediante el uso de un sistema de obtención de información dedicado, y una red IP cableada que se proporcionan mediante el centro de autenticación asociado 3, la terminal de WiFi 1 solicita obtener la información de verificación de acceso asignada al primer identificador de usuario.

Paso 2: Cuando se recibe el mensaje de solicitud usado para obtener la información de verificación de acceso asignada al primer identificador de usuario, el centro de autenticación asociado 3 asigna la información de verificación de acceso al primer identificador de usuario, y almacena de forma correspondiente el primer identificador de usuario y la información de verificación de acceso asignada al primer identificador de usuario. Opcionalmente, antes de asignar información de verificación de acceso al primer identificador de usuario, el centro de autenticación asociado 3 necesita verificar el primer identificador de usuario, y después de que la verificación tiene éxito, genera la información de verificación de acceso correspondiente al primer identificador de usuario, y almacena temporalmente una relación de asociación entre el primer identificador de usuario y la información de verificación de acceso correspondiente para una consulta posterior.

Paso 3: El centro de autenticación asociado 3 notifica la información de verificación de acceso correspondiente al primer identificador de usuario a la terminal de WiFi 1.

Opcionalmente, el centro de autenticación asociado 3 notifica la información de verificación del acceso a la terminal de WiFi 1 mediante el uso de la red celular inalámbrica en la forma de un mensaje SMS, o un código de respuesta rápida, o un código de barras o puede notificar la información de verificación de acceso a la terminal de WiFi 1 por otros medios. Por ejemplo, el centro de autenticación asociado 3 notifica la información de verificación de acceso a la terminal de WiFi 1 mediante el uso de la red IP cableada.

En este caso, las operaciones en la etapa de asociación se completan mediante el uso de un canal asociado. Es decir, la terminal de WiFi 1 ha obtenido la información de verificación de acceso requerida para acceder a la red WiFi, y la transmisión de información entre diferentes dispositivos en los pasos anteriores se implementa mediante el uso de una red asociada. En la etapa de autenticación posterior, la autenticación se realiza en la red WiFi, de acuerdo con los siguientes pasos específicos (se continúan los números de paso).

Paso 4: La terminal de WiFi 1 añade la información de verificación de acceso a una solicitud de inicio de sesión usada para iniciar sesión en la red WiFi, y envía a un centro de autenticación de WiFi 2, la solicitud de inicio de sesión que porta la información de verificación de acceso.

Paso 5: Después de recibir la solicitud de inicio de sesión enviada mediante la terminal de WiFi 1, el centro de autenticación de WiFi 2 envía, al centro de autenticación asociado 3, la información de verificación de acceso portada en la solicitud de inicio de sesión.

Paso 6: Después de recibir la información de verificación de acceso enviada mediante el centro de autenticación de WiFi 2, el centro de autenticación asociado 3 consulta un segundo identificador de usuario almacenado de forma correspondiente de acuerdo con la información de verificación de acceso.

Paso 7: El centro de autenticación asociado 3 añade el segundo identificador de usuario hallado a la información de autenticación, y retroalimenta al centro de autenticación de WiFi 2, la información de autenticación que porta el segundo identificador de usuario hallado.

Paso 8: Después de recibir el segundo identificador de usuario correspondiente a la información de verificación de acceso y retroalimentada por el centro de autenticación asociado 3, el centro de autenticación de WiFi 2 añade el segundo identificador de usuario a la información de autenticación y envía, a la terminal de WiFi 1, la información de autenticación que porta el segundo identificador de usuario.

Paso 9: Después de recibir la información de autenticación retroalimentada por el centro de autenticación de WiFi 2 y usada para responder a la solicitud de inicio de sesión, la terminal de WiFi 1 determina si el segundo identificador de usuario portado en la información de autenticación es consistente con el primer identificador de usuario usado para obtener la información de verificación de acceso del centro de autenticación asociado 3. Si el segundo identificador de usuario es consistente con el primer identificador de usuario, esto indica que la red WiFi es una red segura; o si el segundo identificador de usuario no es consistente con el primer identificador de usuario, esto indica que existe un riesgo de acceso y una amenaza de seguridad en la red WiFi.

En este caso, las operaciones en la etapa de autenticación se completan mediante el uso de un canal de autenticación. Es decir, cuando se accede a la red WiFi, la terminal de WiFi 1 obtiene el identificador de usuario correspondiente a la información de verificación de acceso e intenta autenticar la red WiFi mediante la verificación del identificador de usuario recibido. La transmisión de información entre diferentes dispositivos en los pasos 4 a 8 se implementa mediante el uso del canal de autenticación.

Por lo tanto, en esta realización de la presente invención, la autenticidad de la red WiFi se verifica indirectamente al determinar si la red WiFi a la que se accede se puede interconectar a un centro de autenticación asociado de confianza. Es decir, que la red WiFi que se puede interconectar con éxito al centro de autenticación asociado es confiable y segura. El motivo es que, en un procedimiento de interconexión con el centro de autenticación asociado, el centro de autenticación asociado examina estrictamente la autenticidad y la seguridad de la red a interconectar. Esto asegura no solo la autenticidad y la seguridad de una red en la que se ubica el centro de autenticación asociado, sino también la autenticidad y seguridad de la red WiFi a la que se accede. Una red de suplantación de identidad o una red de fraude electrónico no se pueden interconectar con el centro de autenticación asociado y no pueden obtener el identificador de usuario del centro de autenticación asociado y, por lo tanto, no pueden mostrar al usuario, mediante el uso de la terminal de WiFi, el identificador de usuario correspondiente a la información de verificación de acceso que se ingresa al momento de acceder a la red WiFi. De esta forma, la autenticidad de la red WiFi se verifica mediante la verificación de si la red WiFi puede proporcionar un identificador de usuario correcto correspondiente a la información de verificación de acceso, de modo que la terminal de WiFi pueda distinguir entre una red WiFi auténtica y una red WiFi de suplantación de identidad.

A continuación, se usan dos escenarios de aplicación específicos para describir el procedimiento anterior.

Escenario 1:

Con referencia a la FIG. 4, debido a que la seguridad y la credibilidad de una red de operador son relativamente altas, en el escenario 1 se usa un centro de autenticación tal como HSS/HLR/AuC en la red de operador para implementar en colaboración una función de autenticación de una red WiFi. La red de operador incluye entidades de funciones lógicas tal como una red celular inalámbrica, un centro de autenticación y un centro de SMS. El centro de autenticación y el centro de SMS en la red de operador se pueden integrar como un centro de autenticación asociado para proporcionar funciones tal como autenticación de red y notificación de mensajes.

En la red WiFi, además de una terminal de WiFi, un centro de autenticación de WiFi debe ejecutar la autenticación de un usuario en acceso. El centro de autenticación de WiFi, se puede establecer de forma independiente, o se puede establecer mediante una organización de terceros que se especializa en proporcionar un servicio de autenticación. Por ejemplo, el centro de autenticación de WiFi puede ser un centro de autenticación en la red de operador. Independientemente de la forma del centro de autenticación de WiFi, el centro de autenticación de WiFi puede implementar la autenticación de acceso unidireccional solo en el usuario, y la autenticación en la red WiFi se debe ejecutar en colaboración con un centro de autenticación asociado. Para facilitar la descripción, en el escenario 1, se

supone que un servidor de autenticación, autorización y contabilización (AAA) se implementa de forma independiente como un centro de autenticación de WiFi en la red WiFi.

Para un procedimiento de autenticación de una red WiFi pública mediante el uso de la arquitectura del sistema en la FIG. 4, véase la FIG. 5. Los pasos específicos son los siguientes:

S501. Cuando una terminal de WiFi 1 necesita acceder a una red WiFi pública, una terminal celular 5 en primer lugar usa un primer identificador de usuario (en la presente memoria, un número de teléfono móvil de la terminal celular 5) de un usuario de la terminal de WiFi 1 para solicitar, desde un centro de autenticación 3 en una red de operador mediante el uso de una red celular inalámbrica, información de verificación de acceso a la red WiFi asignada al número de teléfono móvil.

Cabe señalar que, si la terminal de WiFi 1 tiene una función de comunicación de red celular, la terminal de WiFi 1 se puede integrar con la terminal celular 5.

S502. El centro de autenticación 3 en la red de operador verifica la terminal celular 5, y después de que la verificación tiene éxito, asigna la información de verificación de acceso correspondiente (es decir, un código de verificación de acceso WiFi) al número de teléfono móvil de la terminal celular 5, y almacena temporalmente la información de verificación de acceso para una consulta posterior.

S503. El centro de autenticación 3 en la red de operador envía el número de teléfono móvil de la terminal celular 5 y el código de verificación de acceso WiFi correspondiente a un centro de SMS del operador 4.

S504. El centro de SMS del operador 4 envía el código de verificación de acceso WiFi recibido correspondiente al número de teléfono móvil de la terminal celular 5 a la terminal celular 5 usando la red celular inalámbrica.

Opcionalmente, el centro de SMS del operador 4 notifica el código de verificación de acceso WiFi a la terminal celular 5 mediante el uso de la red celular inalámbrica en forma de un mensaje SMS, un código de respuesta rápida o un código de barras, o puede notificar la información de verificación de acceso a la terminal celular 5 por otros medios.

S505. El usuario ingresa el código de verificación de acceso WiFi recibido por la terminal celular 5 en la terminal de WiFi 1 del usuario. Este paso se puede omitir si la terminal de WiFi 1 se puede integrar con la terminal celular 5.

S506. La terminal de WiFi 1 añade el código de verificación de acceso WiFi a una solicitud de inicio de sesión mediante el uso de una red WiFi pública, y transmite, a un centro de autenticación de WiFi 2, la solicitud de inicio de sesión que porta el código de verificación de acceso WiFi, en el que el centro de autenticación de WiFi 2 de la presente memoria es un centro de autenticación o un servidor AAA (AuC/AAA) establecido por la red WiFi.

S507. El centro de autenticación de WiFi envía, al centro de autenticación 3 en la red de operador para verificación, el código de verificación de acceso WiFi portado en la solicitud de inicio de sesión.

S508. El centro de autenticación 3 en la red de operador verifica, de acuerdo con el código de verificación de acceso WiFi recibido, si existe el identificador de usuario correspondiente (es decir, el número de teléfono móvil), y si existe el número de teléfono móvil correspondiente, se retroalimenta el número de teléfono móvil correspondiente al centro de autenticación de WiFi 2 en la red WiFi pública, o si el número de teléfono móvil correspondiente no existe, se retroalimenta la información de falla al centro de autenticación de WiFi 2 en la red WiFi pública.

S509. El centro de autenticación de WiFi 2 en la red WiFi pública transmite, a la terminal de WiFi 1, el número de teléfono móvil obtenido del centro de autenticación 3 en la red de operador, para demostrar que la red WiFi pública conoce una relación de asociación entre el identificador de usuario y la información de verificación de acceso, y demostrar adicionalmente la autenticidad de la red WiFi pública.

S510. El usuario determina si un número de teléfono móvil que se muestra en la terminal de WiFi 1 es consistente con el número de teléfono móvil usado al momento de solicitar el código de verificación de acceso WiFi. Si el número de teléfono móvil que se muestra en la terminal de WiFi 1 es consistente con el número de teléfono móvil usando al momento de solicitar el código de verificación de acceso WiFi, esto indica que la red WiFi pública es auténtica y confiable y se puede acceder de forma segura; o si el número de teléfono móvil que se muestra en la terminal de WiFi 1 no es consistente con el número de teléfono móvil usado al momento de solicitar el código de verificación de acceso WiFi, esto indica que la red WiFi pública es una red de suplantación de identidad y existe un riesgo de acceso y una amenaza de seguridad.

Escenario 2:

Un canal asociado en un sistema de autenticación de canal dual se implementa mediante el uso de una red cableada. La red cableada usada puede ser una red IP cableada o una red de nombre de punto de acceso de línea (APN) dedicada. La red cableada no está específicamente limitada, a condición de que se pueda establecer una relación de asociación entre la información de verificación de acceso de una red WiFi y un identificador de usuario, tal como un identificador de tarjeta de identidad o un identificador de pasaporte, mediante el uso de la red cableada. Por ejemplo, un sistema de gestión de credenciales para tarjetas de identidad, pasaportes, tarjetas de seguridad social y similares

se puede usar como un centro de autenticación asociado, para asignar la información de verificación de acceso correspondiente (es decir, un código de verificación de acceso WiFi) a un identificador de usuario ingresado (es decir, un número de credenciales) y establecer una relación de asociación entre el número de las credenciales y el código de verificación de acceso WiFi. Luego, el centro de autenticación asociado se interconecta con un centro de autenticación de WiFi de la red WiFi a autenticar. El número de credenciales correspondiente al código de verificación de acceso WiFi se obtiene del centro de autenticación asociado de acuerdo con el código de verificación de acceso WiFi, y el número de credenciales se retroalimenta al centro de autenticación de WiFi. El centro de autenticación de WiFi envía el número de credenciales recibido a una terminal de WiFi correspondiente para demostrar su autenticidad. En la presente memoria, con referencia a la FIG. 6, se utiliza un sistema de gestión de identidad como un centro de autenticación asociado para la descripción.

Como se ilustra en la FIG. 6, en el escenario 2, el procedimiento en el que la terminal de WiFi obtiene la información de verificación de acceso es diferente al del escenario 1. Un primer identificador de usuario de un usuario que usa la terminal de WiFi, es decir, un identificador de tarjeta de identidad de la presente memoria, se ingresa en un sistema de obtención de información establecido por el sistema de gestión de tarjetas de identidad. El identificador de la tarjeta de identidad obtenido del sistema de obtención de información se transmite al sistema de gestión de la tarjeta de identidad mediante el uso de una red IP cableada. El sistema de gestión de la tarjeta de identidad asigna la información de verificación de acceso correspondiente, es decir, un código de verificación de acceso WiFi, al identificador de la tarjeta de identidad, y almacena temporalmente el identificador de la tarjeta de identidad y el código de verificación de acceso WiFi correspondiente para una consulta posterior. Luego, el sistema de gestión de la tarjeta de identidad notifica el código de verificación de acceso asignado al identificador de la tarjeta de identidad. Una forma de notificación específica no está limitada. Opcionalmente, el código de verificación de acceso se notifica a la terminal de WiFi mediante el uso de una red celular en forma de un mensaje SMS, un código de respuesta o un código de barras; o el código de verificación de acceso WiFi asignado se puede mostrar en el sistema de obtención de información, y la terminal de WiFi obtiene el código de verificación de acceso WiFi correspondiente del sistema de obtención de información; o el sistema de gestión de la tarjeta de identidad puede mostrar directamente el código de verificación de acceso a la terminal de WiFi por medio de impresión en papel. Después de que la terminal de WiFi obtiene el código de verificación de acceso WiFi, un procedimiento posterior de autenticación de la red WiFi es básicamente igual que el procedimiento de autenticación en el escenario 1, y no se describe nuevamente en la presente memoria.

En base a la realización anterior, como se muestra en la FIG. 7, un primer aparato 7 para autenticar una red WiFi proporcionado en una realización de la presente invención incluye:

una primera unidad transceptora 70, configurada para: cuando se determina que existe una red WiFi en un área en que se ubica el aparato, enviar un mensaje de solicitud a un centro de autenticación, en el que el mensaje de solicitud porta un primer identificador de usuario, y recibir la información de verificación de acceso enviada por el centro de autenticación asociado y asignada a un usuario representado por el primer identificador de usuario;

una segunda unidad transceptora 71, configurada para: enviar una solicitud de inicio de sesión a un centro de autenticación de WiFi en la red WiFi, en el que la solicitud de inicio de sesión porta la información de verificación de acceso, y recibir la información de autenticación retroalimentada por el centro de autenticación de WiFi y usada para responder a la solicitud de inicio de sesión, en el que la información de autenticación porta un segundo identificador de usuario; y

una unidad de procesamiento 72, configurada para: cuando el segundo identificador de usuario portado en la información de autenticación es igual que el primer identificador de usuario, determinar que la red WiFi es una red segura.

Opcionalmente, el identificador de usuario incluye un MSISDN o una identidad.

Opcionalmente, el aparato además incluye:

una unidad de detección 73, configurada para: buscar una red WiFi en un área en que se ubica el aparato, y determinar, de acuerdo con un resultado de la búsqueda, que existe una red WiFi en el área en que se ubica el aparato.

En base a la realización anterior, como se muestra en la FIG. 8, un segundo aparato 8 para autenticar una red WiFi proporcionada en una realización de la presente invención incluye:

una primera unidad transceptora 80, configurada para recibir una solicitud de inicio de sesión enviada por una terminal para iniciar sesión en una red WiFi en la que se ubica el centro de autenticación, en la que la solicitud de inicio de sesión porta la información de verificación de acceso; y

una segunda unidad transceptora 81, configurada para: enviar, a un centro de autenticación asociado, la información de verificación de acceso portada en la solicitud de inicio de sesión, y

recibir un identificador de usuario correspondiente a la información de verificación de acceso y retroalimentada por el centro de autenticación asociado, en el que

la primera unidad transceptora 80 también está configurada para: añadir el identificador de usuario a la información de autenticación, y enviar, a la terminal, la información de autenticación que porta el identificador de usuario.

En base a la realización anterior, como se muestra en la FIG. 9, un tercer aparato 9 para autenticar una red WiFi proporcionado en una realización de la presente invención incluye:

una unidad de asignación 90, configurada para: cuando se recibe un mensaje de solicitud que porta un identificador de usuario, asignar la información de verificación de acceso al identificador de usuario;

una primera unidad transceptora 91, configurada para: almacenar de forma correspondiente el identificador de usuario y la información de verificación de acceso asignada al identificador de usuario y notificar la información de verificación de acceso a una terminal usada por un usuario representado por el identificador de usuario; y

una segunda unidad transceptora 92, configurada para: recibir la información de verificación de acceso mediante un centro de autenticación de WiFi; y

consultar el identificador de usuario almacenado correspondientemente de acuerdo con la información de verificación de acceso, y retroalimentar el identificador de usuario hallado al centro de autenticación de WiFi.

Opcionalmente, la primera unidad transceptora 91 también está configurada para:

notificar la información de verificación de acceso a la terminal mediante el uso de una red celular inalámbrica en la forma de un mensaje SMS, un código de respuesta rápida o un código de barras.

En base a la realización anterior, como se muestra en la FIG. 10, una realización de la presente invención proporciona una terminal 100, y la terminal 100 incluye:

un transceptor 101, un procesador 102, una memoria 103, y un bus 104, en la que el transceptor 101, el procesador 102, y la memoria 103 se conectan al bus 104.

El transceptor 101 está configurado para: cuando se determina que existe una red WiFi en un área en la que se ubica la terminal, enviar un mensaje de solicitud a un centro de autenticación asociado, en el que el mensaje de solicitud porta un primer identificador de usuario, y recibir información de verificación de acceso por el centro de autenticación asociado y asignada a un usuario representado por el primer identificador de usuario.

El transceptor 101 también está configurado para: enviar una solicitud de inicio de sesión al centro de autenticación de WiFi en la red WiFi, en el que la solicitud de inicio de sesión porta la información de verificación de acceso, y recibir la información de autenticación retroalimentada por el centro de autenticación de WiFi y usada para responder a la solicitud de inicio de sesión, en el que la información de autenticación porta un segundo identificador de usuario.

La memoria 103 está configurada para almacenar un grupo de programas.

El procesador 102 está configurado para invocar los programas almacenados en la memoria 103, para ejecutar el siguiente procedimiento:

cuando el segundo identificador de usuario portado en la información de autenticación es igual que el primer identificador de usuario, determinar que la red WiFi es una red segura.

Opcionalmente, el identificador de usuario incluye MSISDN o una identidad.

Opcionalmente, el procesador 102 también está configurado para: buscar una red WiFi en el área en la que se ubica la terminal, y determinar, de acuerdo con un resultado de la búsqueda, que existe una red WiFi en el área en que se ubica la terminal.

En base a la realización anterior, como se muestra en la FIG. 11, una realización de la presente invención proporciona un primer dispositivo 110 para autenticar una red WiFi, configurado para implementar las funciones del de autenticación de WiFi en las realizaciones que se muestran en la FIG. 2 a FIG. 6. El dispositivo de autenticación 110 incluye: un transceptor 111, una memoria 112, y un bus 113. El transceptor 111 y la memoria 112 se conectan al bus 113.

La memoria 112 está configurada para almacenar una solicitud de inicio de sesión enviada mediante una terminal para iniciar sesión en la red WiFi en la que se ubica el centro de autenticación de WiFi, en el que la solicitud de inicio de sesión porta la información de verificación de acceso.

El transceptor 111 está configurado para: enviar, a un centro de autenticación asociado, la información de verificación de acceso portada en la solicitud de inicio de sesión almacenada en la memoria 112, y

recibir un identificador de usuario correspondiente a la información de verificación de acceso y retroalimentada por el centro de autenticación asociado.

El transceptor 111 también está configurado para: añadir el identificador de usuario a la información de autenticación, y enviar, a la terminal, la información de autenticación que porta el identificador de usuario.

En base a la realización anterior, como se muestra en la FIG. 12, una realización de la presente invención proporciona un segundo dispositivo 120 para autenticar una red WiFi, configurado para implementar las funciones del centro de autenticación asociado en las realizaciones que se muestran en la FIG. 2 a FIG. 6. El dispositivo de autenticación 120 incluye: un transceptor 121, una memoria 122, un procesador 123, y un bus 124. El transceptor 121, la memoria 122, y el procesador 123 se conectan al bus 124.

La memoria 122 almacena un grupo de programas.

El procesador 123 está configurado para invocar los programas almacenados en la memoria 122, para ejecutar el siguiente procedimiento:

cuando el transceptor 121 recibe un mensaje de solicitud que porta un identificador de usuario, asignar información de verificación de acceso al identificador.

La memoria 122 también está configurada para almacenar de forma correspondiente el identificador de usuario y la información de verificación de acceso asignada al identificador de usuario.

El transceptor 121 también está configurado para: notificar la información de verificación de acceso almacenada en la memoria 122 a una terminal usada por un usuario representado por el identificador de usuario;

recibir la información de verificación de acceso enviada por un centro de autenticación de WiFi, y

consultar el identificador de usuario almacenado correspondientemente de acuerdo con la información de verificación de acceso, y retroalimentar el identificador de usuario hallado en el centro de autenticación de WiFi.

Opcionalmente, el transceptor 121 también está configurado para:

notificar, la información de verificación de acceso a la terminal mediante el uso de una red celular inalámbrica en la forma de un mensaje SMS, un código de respuesta rápida o un código de barras.

En conclusión, en las realizaciones de la presente invención, cuando se determina que existe una red WiFi en el área en que se ubica la terminal, la terminal envía el mensaje de solicitud al centro de autenticación asociado, en el que el mensaje de solicitud porta el primer identificador de usuario; y recibe la información de verificación de acceso enviada por el centro de autenticación asociado y asignada al usuario representado por el primer identificador de usuario. La terminal envía la solicitud de inicio de sesión al centro de autenticación de WiFi en la red WiFi, en el que la solicitud de inicio de sesión porta la información de verificación de acceso; y recibe la información de autenticación retroalimentada por el centro de autenticación de WiFi y usada para responder a la solicitud de inicio de sesión, en el que la información de autenticación porta el segundo identificador de usuario. Cuando el segundo identificador de usuario portado en la información de autenticación es igual que el primer identificador de usuario, la terminal determina que la red WiFi es una red segura. De esta forma, la autenticidad de la red WiFi se verifica indirectamente mediante la determinación de si la red WiFi a la que se accede se puede interconectar a un centro de autenticación asociado de confianza, es decir, que la autenticación se ejecuta en la red WiFi a la que se accede mediante el uso de la información de autenticación que es retroalimentada por el centro de autenticación de WiFi y que porta el segundo identificador de usuario. El centro de autenticación asociado examina estrictamente la autenticidad y seguridad de la red WiFi cuando el centro de autenticación de WiFi está interconectado al centro de autenticación asociado. Esto asegura no solo la autenticidad y la seguridad de una red en la que está ubicado el centro de autenticación asociado, sino también la autenticidad y seguridad de la red WiFi a la que se accede. Por lo tanto, se puede garantizar la seguridad de la información de un usuario de la terminal.

Los expertos en la técnica deben comprender que las realizaciones de la presente invención se pueden proporcionar como un procedimiento, un sistema o un producto de programa de ordenador. Por lo tanto, la presente invención puede usar una forma de realizaciones solo de hardware, realizaciones solo de software o realizaciones con una combinación de software y hardware. Además, la presente invención puede usar una forma de un producto de programa de ordenador que se implementa en uno o más medios de almacenamiento utilizables por ordenador (que incluyen, pero no se limitan a, una memoria de disco, un CD-ROM, una memoria óptica y similares) que incluye un código de programa utilizable por ordenador.

La presente invención se describe con referencia a los diagramas de flujo y/o diagramas de bloques del procedimiento, el dispositivo (sistema), y el producto de programa de ordenador de acuerdo con las realizaciones de la presente invención. Se debe entender que las instrucciones del programa de ordenador se pueden usar para implementar cada procedimiento y/o cada bloque en los diagramas de flujo y/o los diagramas de bloques y una combinación de un procedimiento y/o un bloque en los diagramas de flujo y/o los diagramas de bloques. Estas instrucciones del programa de ordenador se pueden proporcionar a un ordenador de propósito general, un ordenador dedicado, un procesador incorporado o un procesador de cualquier otro dispositivo de procesamiento de datos programable para generar una máquina, de modo que las instrucciones ejecutadas por un ordenador o un procesador de cualquier otro dispositivo

de procesamiento de datos programable generan un aparato para implementar una función específica en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones del programa de ordenador se pueden almacenar en una memoria legible por ordenador que puede instruir al ordenador o cualquier otro dispositivo de procesamiento de datos programable que trabaje de una forma específica, de modo que las instrucciones almacenadas en la memoria legible por ordenador generen un artefacto que incluya un aparato de instrucciones. El aparato de instrucciones implementa una función específica en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones del programa de ordenador se pueden cargar en un ordenador u otro dispositivo de procesamiento de datos programable, de modo de ejecutar una serie de operaciones y pasos en el ordenador u otro dispositivo programable, generando de este modo el procesamiento implementado por el ordenador. Por lo tanto, las instrucciones ejecutadas en el ordenador u otro dispositivo programable proporcionan pasos para implementar una función específica en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Aunque se han descrito algunas realizaciones de la presente invención, las personas expertas en la técnica pueden ejecutar cambios y modificaciones a estas realizaciones una vez aprendido el concepto inventivo básico. Por lo tanto, se debe interpretar que las siguientes reivindicaciones abarcan las realizaciones preferidas y todos los cambios y modificaciones que se hallan dentro del ámbito de la presente invención.

Evidentemente, los expertos en la técnica pueden hacer varias modificaciones y variaciones a las realizaciones de la presente invención sin apartarse del alcance de las realizaciones de la presente invención. La presente invención está destinada a abarcar estas modificaciones y variaciones a condición de que se hallen dentro del ámbito de protección definido por las siguientes reivindicaciones y sus tecnologías equivalentes.

REIVINDICACIONES

1. Un procedimiento para autenticar una red WiFi, que comprende:

enviar (1, S501), mediante una terminal, al determinar que existe una red WiFi en un área en la que se ubica la terminal, un mensaje de solicitud a un centro de autenticación asociado, en el que el mensaje de solicitud porta un identificador de usuario, y recibir (3, S504) la información de verificación de acceso enviada por el centro de autenticación asociado y asignada por el centro de autenticación asociado (3) a un usuario representado por el identificador de usuario;

enviar (4, 506), mediante la terminal, una solicitud de inicio de sesión a un centro de autenticación de WiFi en la red WiFi, en el que la solicitud de inicio de sesión porta la información de verificación de acceso, y recibir (8, S509) la información de autenticación retroalimentada por el centro de autenticación de WiFi y usada para responder la solicitud de inicio de sesión, en el que la información de autenticación porta un identificador de usuario que corresponde a la información de verificación de acceso y se obtiene mediante el centro de autenticación de WiFi desde el centro de autenticación asociado; y

determinar (9, S510), mediante la terminal cuando el identificador de usuario portado en la información de autenticación es igual que el identificador de usuario portado en el mensaje de solicitud, que la red WiFi es una red segura.

2. El procedimiento de acuerdo con la reivindicación 1, en donde el identificador de usuario comprende un número ISDN internacional de la estación móvil, MSISDN, o una identidad.

3. El procedimiento de acuerdo con la reivindicación 1, en donde la determinación, mediante una terminal, de que existe una red WiFi en un área en la que se ubica la terminal comprende:

buscar, mediante la terminal, una red WiFi en el área en la que se ubica la terminal, y determinar, de acuerdo con un resultado de la búsqueda, que existe una red WiFi en el área en la que se ubica la terminal.

4. Un procedimiento para autenticar una red WiFi, que comprende:

recibir (4, S506), mediante un centro de autenticación de WiFi, una solicitud de inicio de sesión enviada mediante una terminal para iniciar sesión en una red WiFi en la que se ubica el centro de autenticación de WiFi, en donde la solicitud de inicio de sesión porta información de verificación de acceso;

enviar (5, S507), mediante el centro de autenticación de WiFi a un centro de autenticación asociado, la información de verificación de acceso portada en la solicitud de inicio de sesión, y

recibir (7, S508), un identificador de usuario correspondiente a la información de verificación de acceso y retroalimentada por el centro de autenticación asociado; y

añadir (8, S509), mediante el centro de autenticación de WiFi, el identificador de usuario a la información de autenticación, y enviar, a la terminal, la información de autenticación que porta el identificador de usuario.

5. Un procedimiento para autenticar una red WiFi, que comprende:

asignar (2, S502), mediante un centro de autenticación asociado cuando se recibe un mensaje de solicitud que porta un identificador de usuario, la información de verificación de acceso al identificador de usuario, y almacenar de forma correspondiente el identificador de usuario y la información de verificación de acceso asignada al identificador de usuario;

notificar (3, S504), mediante el centro de autenticación asociado, la información de verificación de acceso a una terminal usada por un usuario representado por el identificador de usuario;

recibir (5, S507), mediante el centro de autenticación asociado, información de verificación de acceso enviada por un centro de autenticación de WiFi; y

consultar (6, S508) el identificador de usuario almacenado correspondientemente de acuerdo con la información de verificación de acceso recibida, y retroalimentar (7, S508) el identificador de usuario hallado al centro de autenticación de WiFi.

6. El procedimiento de acuerdo con la reivindicación 5, en donde la notificación (3, S504), mediante el centro de autenticación asociado, de la información de verificación de acceso a una terminal usada por un usuario representado por el identificador de usuario comprende:

notificar (3, S504), mediante el centro de autenticación asociado, la información de verificación de acceso a la terminal mediante el uso de una red celular inalámbrica en la forma de un mensaje SMS, un código de respuesta rápida o un código de barras.

7. Un sistema para autenticar una red WiFi, que comprende:

una terminal (1), configurada para: cuando se determina que existe una red WiFi en un área en la que se ubica la terminal, enviar un mensaje de solicitud a un centro de autenticación asociado (3), en donde el mensaje de solicitud porta un identificador de usuario, y recibir la información de verificación de acceso enviada por el centro de autenticación asociado (3) y asignada por el centro de autenticación asociado (3) a un usuario representado por el identificador de usuario; enviar una solicitud de inicio de sesión a un centro de autenticación de WiFi (2) en la red WiFi, en donde la solicitud de inicio de sesión porta la información de verificación de acceso; recibir la información de autenticación retroalimentada por el centro de autenticación de WiFi (2) y usada para responder a la solicitud de inicio de sesión, en la que la información de autenticación porta un identificador de usuario que corresponde a la información de verificación de acceso y se obtiene mediante el centro de autenticación de WiFi (2) desde el centro de autenticación asociado (3); y cuando el identificador de usuario portado en la información de autenticación es igual que el identificador de usuario portado en el mensaje de solicitud, determinar que la red WiFi es una red segura;

el centro de autenticación de WiFi (2), configurado para: recibir la solicitud de inicio de sesión enviada por la terminal (1) para iniciar sesión en la red WiFi en la que se ubica en el centro de autenticación de WiFi (2); enviar, al centro de autenticación asociado (3), la información de verificación de acceso portada en la solicitud de inicio de sesión, y recibir un identificador de usuario correspondiente a la información de verificación de acceso y retroalimentada por el centro de autenticación asociado (3); y añadir el identificador de usuario a la información de autenticación, y enviar, a la terminal (1), la información de autenticación que porta el identificador de usuario; y

el centro de autenticación asociado (3), configurado para: cuando se recibe el mensaje de solicitud que porta el identificador de usuario, asignar la información de verificación de acceso al identificador de usuario, y almacenar de forma correspondiente el identificador de usuario y la información de verificación de acceso asignada al identificador de usuario; notificar la información de verificación de acceso a la terminal usada por un usuario representado por el identificador de usuario; recibir la información de verificación de acceso enviada por el centro de autenticación de WiFi (2); y consultar el identificador de usuario almacenado correspondientemente de acuerdo con la información de verificación de acceso, y retroalimentar el identificador de usuario hallado al centro de autenticación de WiFi (2).

8. Un aparato para autenticar una red WiFi, que comprende:

una primera unidad transceptora (70), configurada para: cuando se determina que existe una red WiFi en un área en la que se ubica el aparato, enviar un mensaje de solicitud a un centro de autenticación asociado, en donde el mensaje de solicitud porta un identificador de usuario, y recibir la información de verificación de acceso enviada por el centro de autenticación asociado y asignada por el centro de autenticación asociado a un usuario representado por el identificador de usuario;

una segunda unidad transceptora (71), configurada para: enviar una solicitud de inicio de sesión a un centro de autenticación de WiFi en la red WiFi, en la que la solicitud de inicio de sesión porta la información de verificación de acceso, y recibir información de autenticación retroalimentada por el centro de autenticación de WiFi y usada para responder a la solicitud de inicio de sesión, en la que la información de autenticación porta un identificador de usuario que corresponde a la información de verificación de acceso y se obtiene mediante el centro de autenticación de WiFi desde el centro de autenticación asociado; y

una unidad de procesamiento (72), configurada para: cuando el identificador de usuario portado en la información de autenticación es igual que el identificador de usuario portado en el mensaje de solicitud, determinar que la red WiFi es una red segura.

9. El aparato de acuerdo con la reivindicación 8, que además comprende:

una unidad de detección (73), configurada para: buscar una red WiFi en el área en la que se ubica el aparato, y determinar, de acuerdo con el resultado de la búsqueda, que existe una red WiFi en el área en la que se ubica el aparato.

10. Un aparato para autenticar una red WiFi, en donde el aparato implementa la función de un centro de autenticación de WiFi, el aparato comprende:

una primera unidad transceptora (80), configurada para recibir una solicitud de inicio de sesión enviada mediante una terminal para iniciar sesión en una red WiFi en la que se ubica el centro de autenticación de WiFi, en la que la solicitud de inicio de sesión porta información de verificación de acceso; y

una segunda unidad transceptora (81), configurada para: enviar, a un centro de autenticación asociado, la información de verificación de acceso portada en la solicitud de inicio de sesión, y

recibir un identificador de usuario correspondiente a la información de verificación de acceso y retroalimentada por el centro de autenticación asociado, en donde

la primera unidad transceptora (80) también está configurada para: añadir el identificador de usuario a la información de autenticación, y enviar, a la terminal, la información de autenticación que porta el identificador de usuario.

11. Un aparato para autenticar una red WiFi, en donde el aparato implementa la función de un centro de autenticación asociado, el aparato comprende:

una unidad de asignación (90), configurada para: cuando se recibe el mensaje de solicitud que porta un identificador de usuario, asignar la información de verificación de acceso al identificador de usuario;

una primera unidad transceptora (91), configurada para: almacenar de forma correspondiente el identificador de usuario y la información de verificación de acceso asignada al identificador de usuario, y notificar la información de verificación de acceso a una terminal usada por un usuario representada por el identificador de usuario; y

una segunda unidad transceptora (92), configurada para: recibir información de verificación de acceso enviada por un centro de autenticación de WiFi; y

consultar el identificador de usuario almacenado correspondientemente de acuerdo con la información de verificación de acceso recibida, y retroalimentar el identificador de usuario hallado al centro de autenticación de WiFi.

12. El aparato de acuerdo con la reivindicación 11, en donde la primera unidad transceptora (91) también está configurada para:

notificar la información de verificación de acceso a la terminal mediante el uso de una red celular inalámbrica en la forma de un mensaje SMS, un código de respuesta rápida o un código de barras.

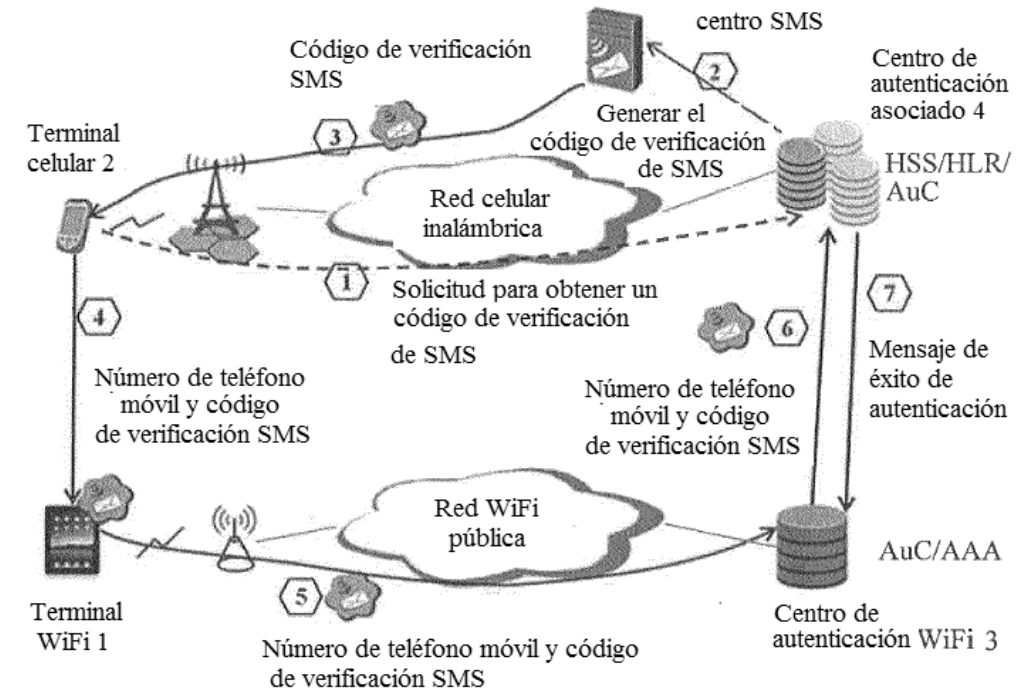
centro SMS
Código de verificación SMS
Centro de autenticación asociado 4
Terminal celular 2
Generar el código de verificación de SMS
HSS/HLR/ AuC
Red celular inalámbrica
Solicitud para obtener un código de verificación de SMS
Mensaje de éxito de autenticación
Número de teléfono móvil y código de verificación SMS
Número de teléfono móvil y código de verificación SMS
Red WiFi pública
AuC/AAA
Terminal WiFi 1
Número de teléfono móvil y código de verificación SMS
Centro de autenticación WiFi 3

FIG. 1

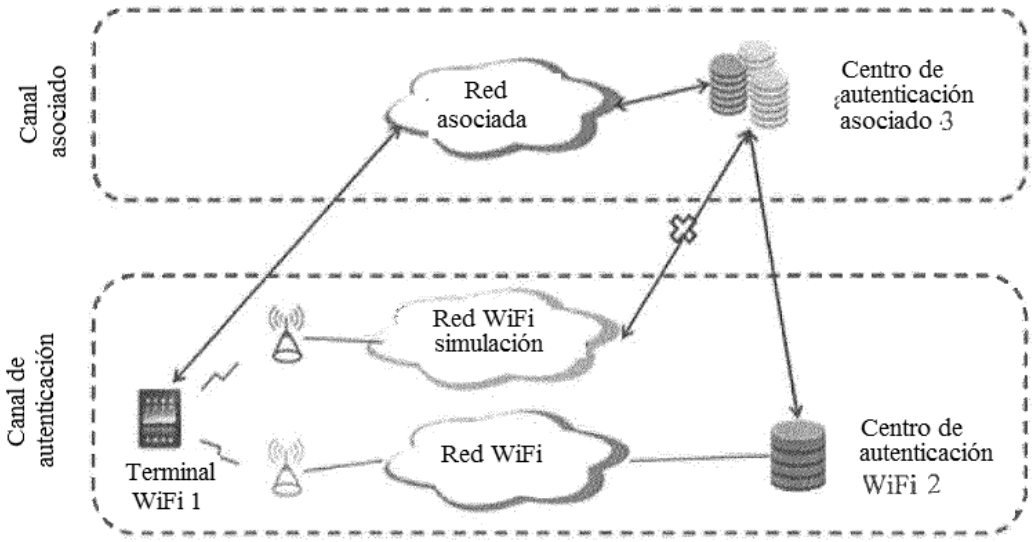
Canal asociado
Red asociada
Centro de autenticación asociado 3
Canal de autenticación
Red WiFi simulación
Terminal WiFi 1
Red WiFi
Centro de autenticación WiFi 2

FIG. 2

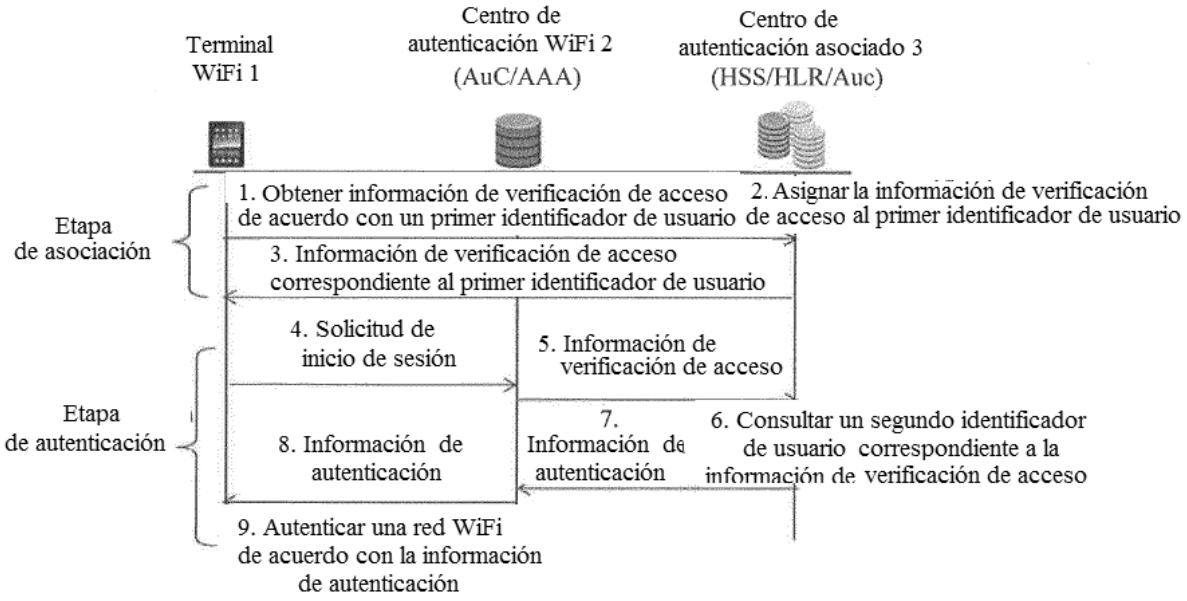
Terminal WiFi 1
Centro de autenticación WiFi 2 (AuC/AAA)
Centro de autenticación asociado 3 (HSS/HLR/Auc)
Etapa de asociación
1. Obtener información de verificación de acceso de acuerdo con un primer identificador de usuario
2. Asignar la información de verificación de acceso al primer identificador de usuario
3. Información de verificación de acceso correspondiente al primer identificador de usuario
Etapa de autenticación
4. Solicitud de inicio de sesión
5. Información de verificación de acceso
6. Consultar un segundo identificador de usuario correspondiente a la información de verificación de acceso
7. Información de autenticación
8. Información de autenticación
9. Autenticar una red WiFi de acuerdo con la información de autenticación

FIG. 3

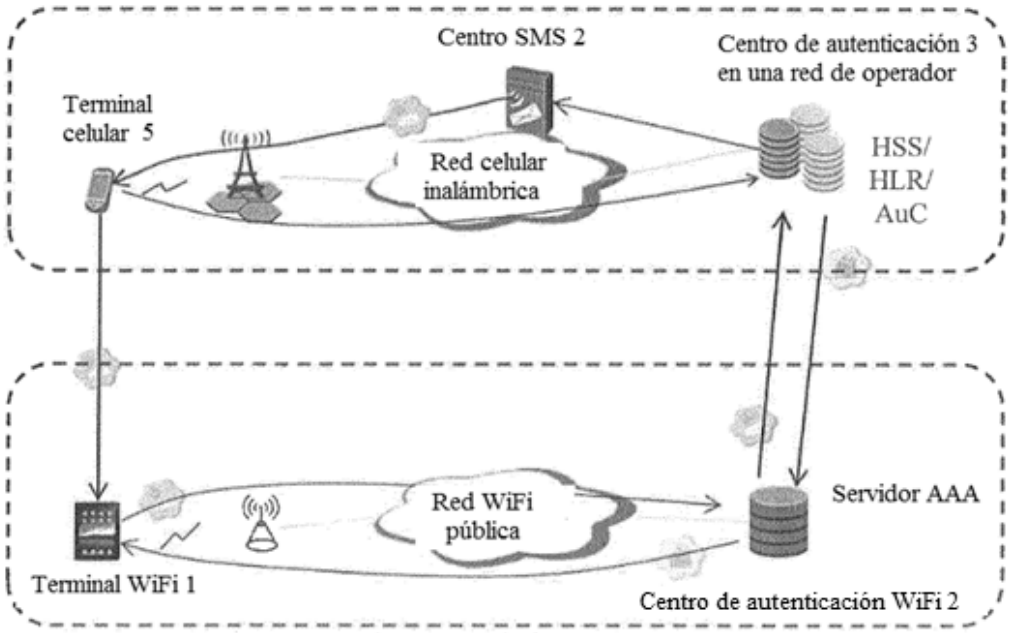
Centro SMS 2
Centro de autenticación 3 en una red de operador
Terminal celular 5
Red celular inalámbrica
HSS/ HLR/ AuC
Red WiFi pública
Servidor AAA
Terminal WiFi 1
Centro de autenticación WiFi 2

FIG. 4

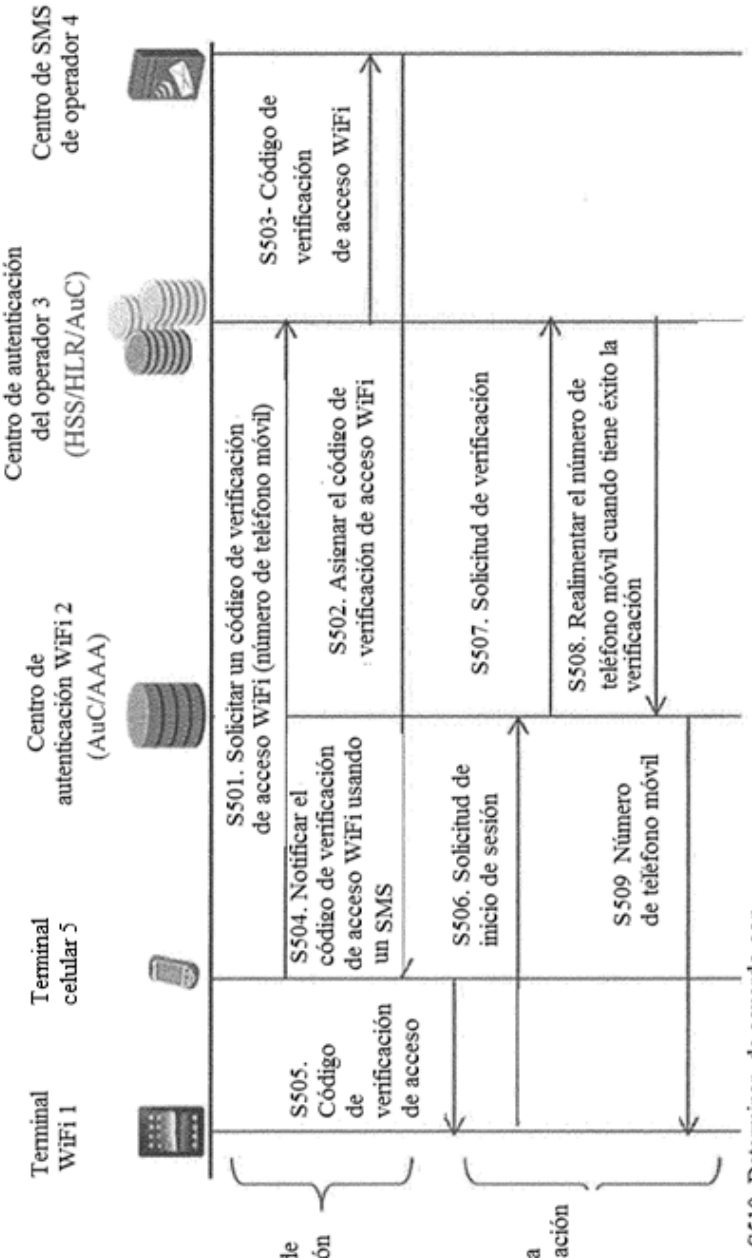
Terminal WiFi 1
Terminal celular 5
Centro de autenticación WiFi 2 (AuC/AAA)
Centro de autenticación del operador 3 (HSS/HLR/AuC)
Centro de SMS de operador 4
S501. Solicitar un código de verificación de acceso WiFi (número de teléfono móvil)
S502. Asignar el código de verificación de acceso WiFi
S503- Código de verificación de acceso WiFi
S504. Notificar el código de verificación de acceso WiFi usando un SMS
S505. Código de verificación de acceso
S506. Solicitud de inicio de sesión
S507. Solicitud de verificación
S508. Realimentar el número de teléfono móvil cuando tiene éxito la verificación
S509 Número de teléfono móvil
S510. Determinar. de acuerdo con el número de teléfono móvil si una red WiFi es auténtica
Etapa de asociación
Etapa de autenticación

FIG. 5

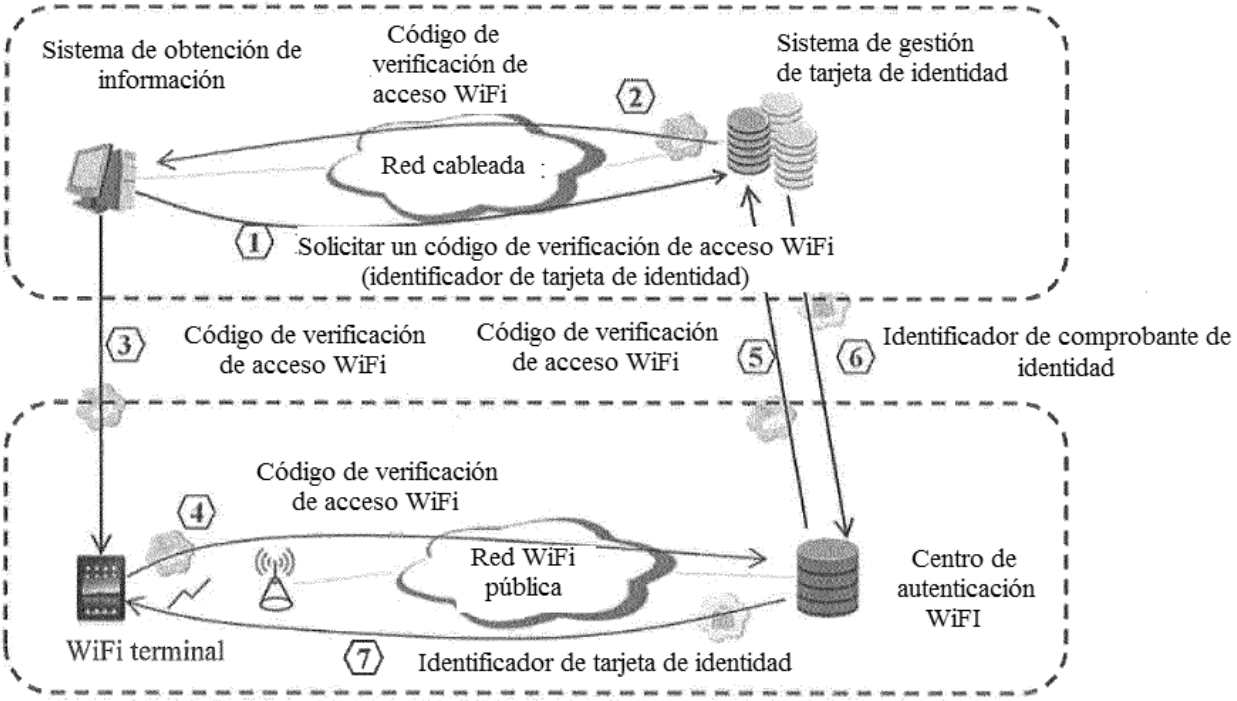
Sistema de obtención de información
Código de verificación de acceso WiFi
Sistema de gestión de tarjeta de identidad
2
Red cableada
1
Solicitar un código de verificación de acceso WiFi (identificador de tarjeta de identidad)
3
Código de verificación de acceso WiFi
Código de verificación de acceso WiFi
5
6
Identificador de comprobante de identidad
Código de verificación de acceso WiFi
4
Red WiFi pública
Centro de autenticación WiFI
WiFi terminal
7
Identificador de tarjeta de identidad

FIG. 6

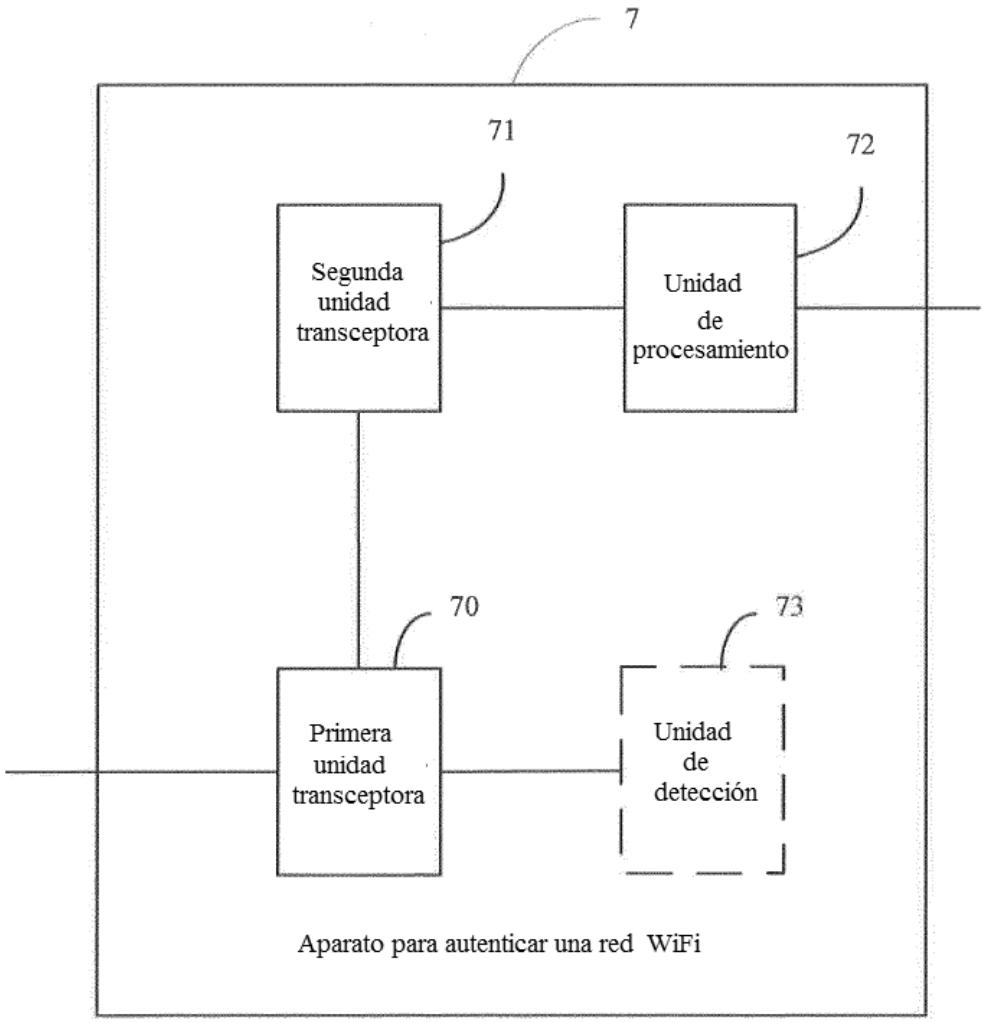
7
71
72
Segunda unidad transceptora
Unidad de procesamiento
70
73
Primera unidad transceptora
Unidad de detección
Aparato para autenticar una red WiFi

FIG. 7

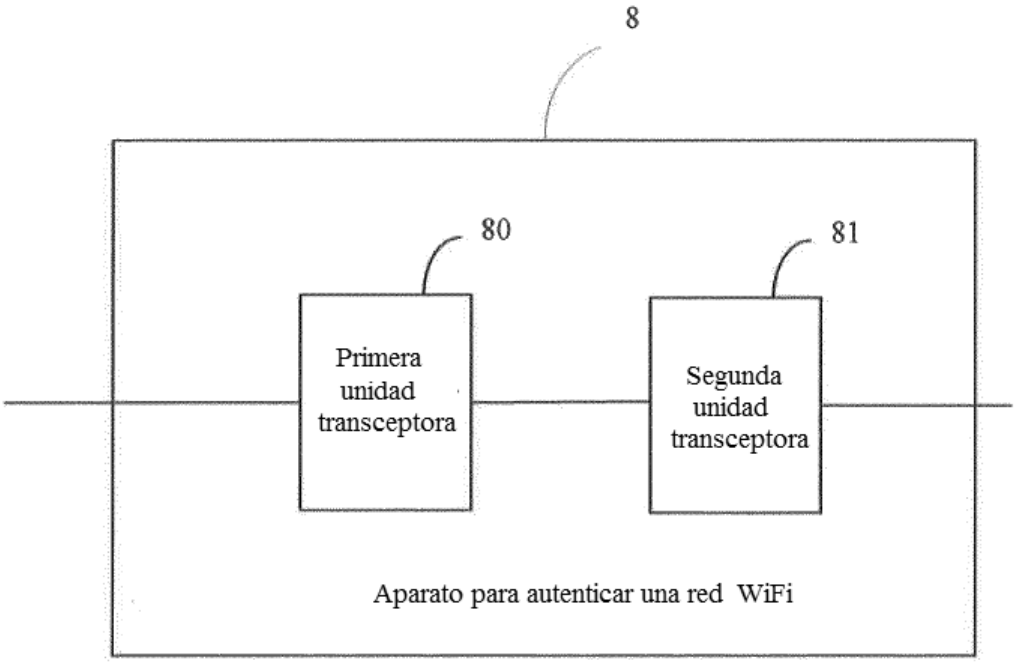
8
80
81
Primera unidad transceptora
Segunda unidad transceptora
Aparato para autenticar una red WiFi

FIG. 8

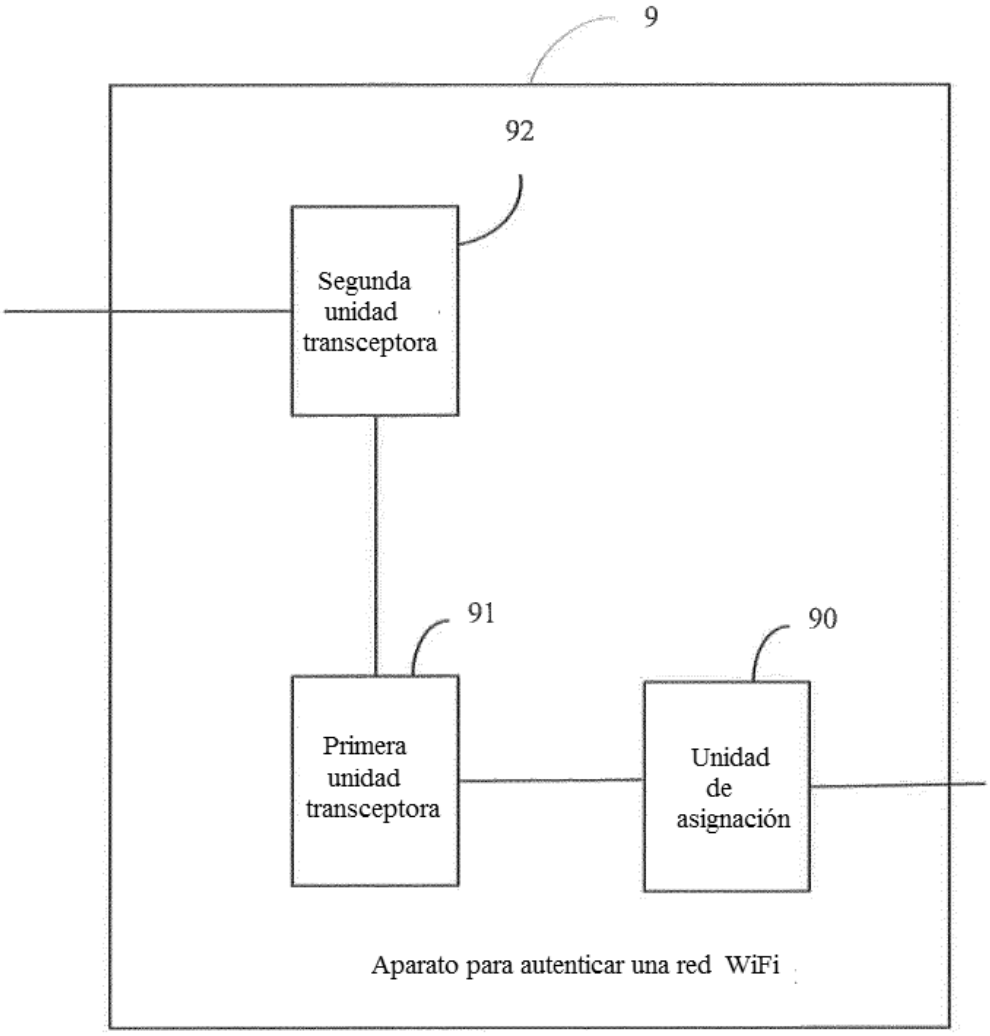
9
92
Segunda unidad transceptora
91
90
Primera unidad transceptora
Unidad de asignación
Aparato para autenticar una red WiFi

FIG. 9

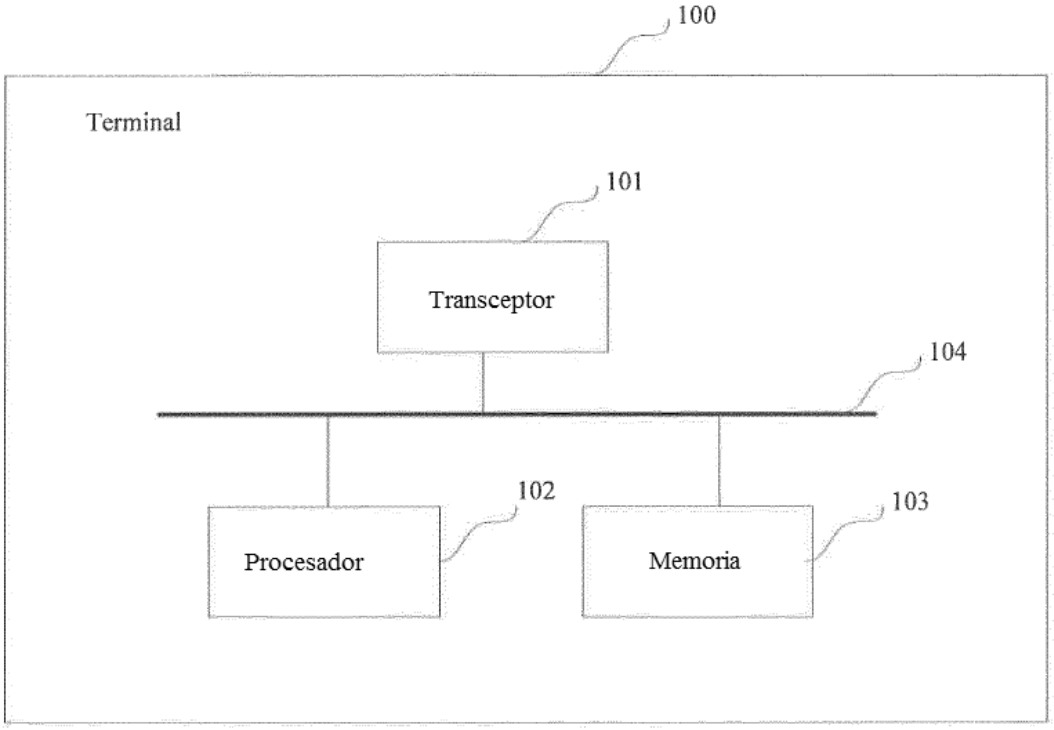
100
Terminal
101
Transceptor
104
102
Procesador
103
Memoria

FIG. 10

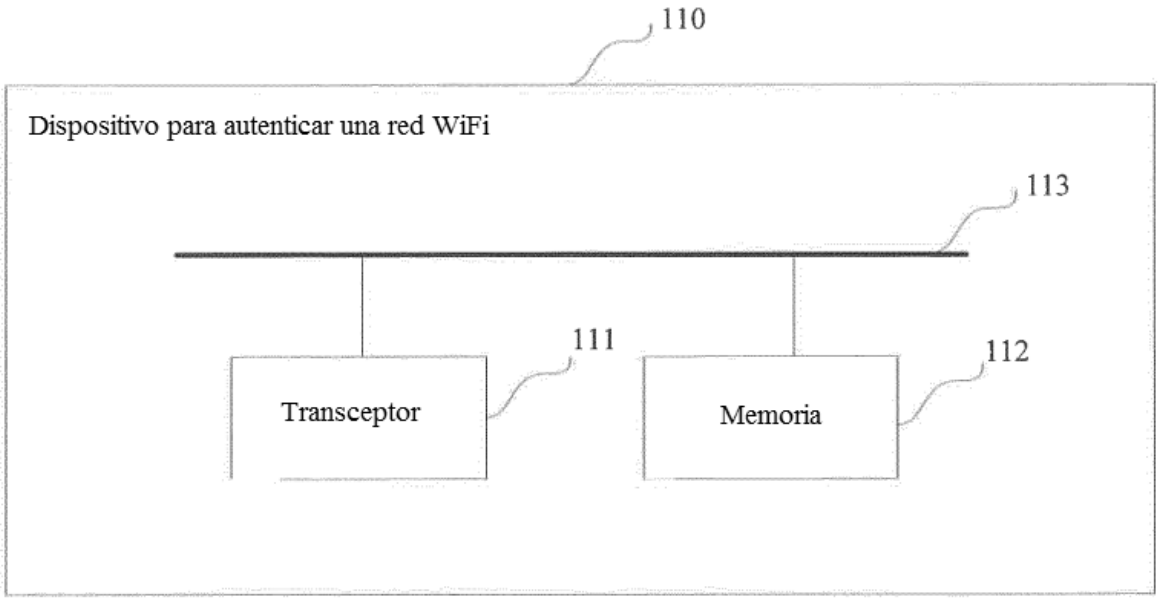
110
Dispositivo para autenticar una red WiFi
113
111
112
Transceptor
Memoria

FIG. 11

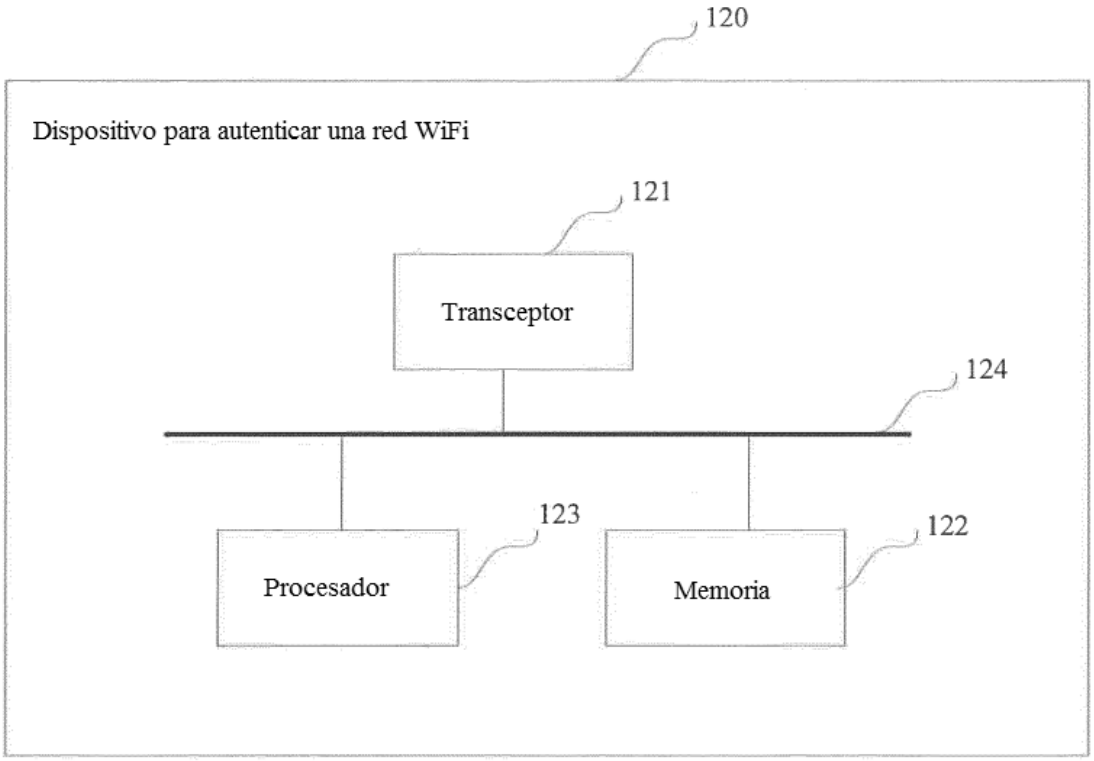
120
Dispositivo para autenticar una red WiFi
121
Transceptor
124
123
Procesador
122
Memoria

FIG. 12