(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 555 169**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 4/20 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.02.2013 E 13707947 (1)**

(97) Fecha y número de publicación de la concesión europea: **30.09.2015 EP 2813054**

(54) Título: **Mecanismo de seguridad para obtener una autorización para un servidor de localización descubierto**

(30) Prioridad:

10.02.2012 US 201261597704 P
07.02.2013 US 201313762231

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.12.2015

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
attn: International IP Administration, 5775 Morehouse Drive
San Diego, California 92121-1714, US

(72) Inventor/es:

HAWKES, PHILIP MICHAEL;
WACHTER, ANDREAS KLAUS;
BURROUGHS, KIRK ALLAN y
EDGE, STEPHEN WILLIAM

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Mecanismo de seguridad para obtener una autorización para un servidor de localización descubierto

ANTECEDENTES

A medida que los servicios relacionados con la localización de dispositivos móviles se vuelven más populares, las soluciones de localización y los servidores de localización asociados que permiten y colaboran en tales soluciones de localización se utilizan de manera más generalizada. Un ejemplo de una solución de localización de este tipo es la solución denominada localización segura en el plano de usuario (SUPL) definida por la Alianza Móvil Abierta (OMA) en documentos disponibles públicamente. Otro ejemplo es la solución de localización del plano de control (CP) definida por el Proyecto de Asociación de Tercera Generación (3GPP) en documentos disponibles públicamente. Debido al siempre creciente predominio de los dispositivos móviles, los servidores de localización pueden restringir algunas veces la capacidad del usuario de obtener acceso al servidor de localización sin alguna forma de autenticación o autorización. Por tanto, los dispositivos móviles visitantes no siempre pueden acceder fácilmente en primera instancia a los servicios proporcionados por el servidor de localización.

Se hace referencia al documento de Tcs Systems titulado: "*SLP Discovery Models and Mechanisms*", 15 de diciembre de 2010 (15/12/2010), paginas 1 a 11, XP55026932, obtenido de la siguiente dirección de Internet: URL:http://member.open-mobilealli-ance.org/ftp/Public_documents/LOC/2010/OMA-LOC-2010-0316-INP_SUPL_3_0_TCS_SLP_Models_and_Discovery_Mechanisms.zip. El documento describe modelos adicionales de implantación de plataformas de localización SUPL y mecanismos de descubrimiento SLP como apoyo a estos modelos.

RESUMEN

Según la presente invención se proporciona un procedimiento, un terminal y un aparato, como se expone respectivamente en las reivindicaciones independientes. Realizaciones preferidas de la invención se describen en las reivindicaciones dependientes.

Estos y otros problemas pueden resolverse según las realizaciones de la presente invención, descritas en el presente documento.

En algunas realizaciones se presenta un procedimiento para obtener un acceso autorizado desde un terminal a un servidor de localización descubierto. El procedimiento puede incluir conmutar desde una primera red, que no soporta un acceso autenticado a un servidor de localización local por medio del terminal, hasta una segunda red que soporta un acceso autenticado al servidor de localización local por medio del terminal. El acceso autenticado al servidor de localización local puede obtenerse usando la segunda red. La autorización para el servidor de localización descubierto puede obtenerse después a partir del servidor de localización local. Después, el terminal puede conmutar desde la segunda red hasta la primera red. Después, el terminal puede acceder al servidor de localización descubierto usando la primera red basándose en la autorización obtenida a partir del servidor de localización local.

En algunas realizaciones, el servidor de localización descubierto incluye una plataforma de localización SUPL descubierta (D-SLP). En algunas realizaciones, el servidor de localización local incluye una plataforma de localización SUPL local (H-SLP). En algunas realizaciones, obtener un acceso autenticado incluye usar al menos uno de un mecanismo de autenticación de cliente alternativo (ACA), certificados de dispositivo y una arquitectura de inicialización genérica (GBA) para autenticar el terminal por medio de la H-SLP.

En algunas realizaciones, la primera red es una red de área local inalámbrica (WLAN). En algunas realizaciones, la segunda red es una red que soporta Evolución a Largo Plazo (LTE), WCDMA, GSM o HRPD cdma2000.

En algunas realizaciones se presenta un terminal para obtener acceso autorizado a un servidor de localización descubierto. El terminal puede incluir un transceptor configurado para conmutar desde una primera red, que no soporta un acceso autenticado a un servidor de localización local por medio del terminal, hasta una segunda red que soporta un acceso autenticado al servidor de localización local por medio del terminal. El transceptor puede conmutar desde la segunda red hasta la primera red después de que el terminal obtenga un acceso autenticado al servidor de localización local usando la segunda red. El terminal también puede incluir un procesador configurado para obtener un acceso autenticado al servidor de localización local usando la segunda red. El procesador también puede estar configurado para obtener una autorización para el servidor de localización descubierto a partir del servidor de localización local y para acceder al servidor de localización descubierto usando la primera red basándose en la autorización obtenida a partir del servidor de localización local.

En algunas realizaciones se presenta un aparato para obtener un acceso autorizado a un servidor de localización descubierto. El aparato puede incluir medios para conmutar desde una primera red, que no soporta un acceso autenticado a un servidor de localización local por medio de un terminal, hasta una segunda red que soporta un acceso autenticado al servidor de localización local por medio del terminal. El aparato puede incluir además medios

para obtener un acceso autenticado al servidor de localización local usando la segunda red, y medios para obtener una autorización para el servidor de localización descubierto a partir del servidor de localización local. El aparato también puede incluir medios para conmutar desde la segunda red hasta la primera red, y medios para acceder al servidor de localización descubierto usando la primera red en función de la autorización obtenida a partir del servidor de localización local.

En algunas realizaciones se presenta un medio legible por procesador no transitorio. El medio legible por procesador puede incluir instrucciones legibles por procesador configuradas para hacer que un procesador conmute desde una primera red, que no soporta un acceso autenticado a un servidor de localización local por medio de un terminal, hasta una segunda red que soporta un acceso autenticado al servidor de localización local por medio del terminal. Las instrucciones legibles por procesador también pueden hacer que el procesador obtenga un acceso autenticado al servidor de localización local usando la segunda red, obtenga una autorización para un servidor de localización descubierto a partir del servidor de localización local, conmute desde la segunda red hasta la primera red y acceda al servidor de localización descubierto usando la primera red basándose en la autorización obtenida a partir del servidor de localización local.

En algunas realizaciones se presenta un procedimiento para obtener un acceso autorizado desde un terminal a una plataforma de localización segura en el plano de usuario (SUPL). El procedimiento puede incluir conmutar desde una primera red que no soporta una autenticación del terminal hasta a una segunda red que soporta una autenticación del terminal. El acceso autenticado a una primera plataforma SUPL puede obtenerse usando la segunda red. La autorización para una segunda plataforma SUPL puede obtenerse después a partir de la primera plataforma SUPL. Después, el terminal puede conmutar desde la segunda red hasta la primera red. Después, el terminal puede acceder a la segunda plataforma SUPL usando la primera red basándose en la autorización obtenida a partir de la primera plataforma SUPL.

En algunas realizaciones se presenta un aparato. El aparato puede incluir uno o más módulos de comunicación configurados para acceder a una primera red y una segunda red. El aparato puede configurarse para acceder a una primera plataforma de localización segura en el plano de usuario usando la primera red y para acceder a una segunda plataforma de localización segura en el plano de usuario usando la segunda red. La primera plataforma de localización segura en el plano de usuario puede comprender una plataforma de localización local (H-SLP) de localización segura en el plano de usuario (SUPL) y/o la segunda plataforma de localización segura en el plano de usuario puede comprender una plataforma de localización descubierta (D-SLP) de localización segura en el plano de usuario (SUPL). El aparato puede estar configurado para tratar de acceder a la H-SLP usando la segunda red, y para acceder a la H-SLP usando la primera red si falla el acceso a la H-SLP a través de la segunda red.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La naturaleza y las ventajas de varias realizaciones pueden entenderse haciendo referencia a las siguientes figuras. En las figuras adjuntas, componentes o características similares pueden tener la misma etiqueta de referencia. Además, varios componentes del mismo tipo pueden distinguirse añadiendo a la etiqueta de referencia un guión y una segunda etiqueta que distingue los componentes similares. Si solo se usa la primera etiqueta de referencia en la memoria descriptiva, la descripción puede aplicarse a uno cualquiera de los componentes similares que tenga la misma primera etiqueta de referencia, independientemente de la segunda etiqueta de referencia.

La FIG. 1 es una ilustración gráfica de un entorno de red inalámbrica de ejemplo que puede utilizarse junto con los diversos sistemas y procedimientos descritos en el presente documento.

La FIG. 2 ilustra aparatos a modo de ejemplo de varias realizaciones.

Las FIG. 3A, 3B y 3C son ilustraciones a modo de ejemplo de etapas asociadas a varias realizaciones.

Las FIG. 4A, 4B y 4C son ilustraciones a modo de ejemplo de etapas asociadas a otras diversas realizaciones.

Las FIG. 5A, 5B y 5C ilustran diagramas de flujo a modo de ejemplo que describen etapas de varias realizaciones.

La FIG. 6 es un sistema informático a modo de ejemplo de varias realizaciones.

DESCRIPCIÓN DETALLADA

La expresión "a modo de ejemplo" se usa en el presente documento en el sentido de "que sirve como ejemplo, instancia o ilustración". No debe considerarse necesariamente que cualquier realización o diseño descritos en el presente documento como "a modo de ejemplo" son preferidos o ventajosos con respecto a otras realizaciones o diseños.

Las técnicas descritas en el presente documento pueden utilizarse en varias redes de comunicaciones inalámbricas,

tales como redes de acceso múltiple por división de código (CDMA), redes de acceso múltiple por división de tiempo (TDMA), redes de acceso múltiple por división de frecuencia (FDMA), redes FDMA ortogonales (OFDMA), redes FDMA de única portadora (SC-FDMA), etc. Los términos “redes” y “sistemas” se utilizan normalmente de manera intercambiable. Una red CDMA puede implementar una tecnología de radio tal como el Acceso de Radio Terrestre Universal (UTRA), CDMA2000, etc. UTRA incluye CDMA de banda ancha (W-CDMA) y Baja Velocidad de Chip (LCR). CDMA2000 cubre las normas IS-2000, IS-95 e IS-856. Una red TDMA puede implementar una tecnología de radio tal como el Sistema Global de Comunicaciones Móviles (GSM). Una red OFDMA puede implementar una tecnología de radio tal como UTRA Evolucionado (E-UTRA), IEEE 802.11, IEEE 802.16, IEEE 802.20, Flash-OFDM_, etc. UTRA es parte del Sistema Universal de Telecomunicaciones Móviles (UMTS). Evolución a Largo Plazo (LTE) usa E-UTRA. UTRA, E-UTRA, GSM, UMTS y LTE están descritos en documentos de 3GPP. CDMA2000 está descrito en documentos de una organización llamada “2º Proyecto de Asociación de Tercera Generación” (3GPP2). Estas diversas normas y tecnologías de radio son conocidas en la técnica.

El acceso múltiple por división de frecuencia de única portadora (SC-FDMA), el cual utiliza modulación de única portadora y ecualización en el dominio de frecuencia, es una técnica. SC-FDMA puede tener un funcionamiento y complejidad global similares a los del sistema OFDMA. Una señal SC-FDMA puede tener una relación de potencia pico a promedio (PAPR) más baja debido a su estructura intrínseca de única portadora. SC-FDMA ha acaparado gran atención, especialmente en las comunicaciones de enlace ascendente, donde una PAPR más baja beneficia en gran medida al terminal móvil en lo que respecta a la eficacia de la potencia de transmisión. Actualmente es un proyecto para el esquema de acceso múltiple de enlace ascendente en la Evolución a Largo Plazo (LTE) de 3GPP, o en UTRA Evolucionado.

En el presente documento se describen varias realizaciones en relación con un terminal de acceso. Un terminal de acceso también puede denominarse sistema, unidad de abonado, estación de abonado, estación móvil, móvil, estación remota, terminal remoto, dispositivo móvil, terminal de usuario, terminal, dispositivo de comunicaciones inalámbricas, agente de usuario, dispositivo de usuario, equipo de usuario (UE) o, en el caso de que se soporte SUPL, terminal con capacidad SUPL (SET). Un terminal de acceso puede ser un teléfono celular, un teléfono sin cables, un teléfono de protocolo de inicio de sesión (SIP), una estación de bucle local inalámbrico (WLL), un asistente digital personal (PDA), un dispositivo manual con capacidad de conexión inalámbrica, un dispositivo informático, un teléfono inteligente, una tableta, un ordenador portátil u otro dispositivo de procesamiento conectado a o que contiene un módem, por ejemplo un módem inalámbrico. Además, en el presente documento se describen varias realizaciones en relación con una estación base. Una estación base puede utilizarse para comunicaciones con uno o más terminales de acceso y también puede denominarse punto de acceso, nodo B, nodo B evolucionado (eNodoB), estación base de punto de acceso, punto de acceso WiFi, femtocélula, estación base local, nodo B local, nodo B evolucionado local o utilizando otra terminología.

Haciendo referencia a la FIG. 1, se ilustra un sistema de comunicaciones inalámbricas de acceso múltiple según algunas realizaciones. En una realización, un punto de acceso (AP) 100 incluye grupos de múltiples antenas, uno que incluye la 104 y la 106, otro que incluye la 108 y la 110, y otro adicional que incluye la 112 y la 114. En la FIG. 1 solo se muestran dos antenas para cada grupo de antenas, aunque puede utilizarse un número mayor o menor de antenas para cada grupo de antenas. Por ejemplo, solo una o dos antenas totales pueden estar incluidas o acopladas al AP 100. El terminal de acceso (AT) 116 se comunica con las antenas 112 y 114, mientras que las antenas 112 y 114 transmiten información al terminal de acceso 116 a través del enlace directo 120 y reciben información desde el terminal de acceso 116 a través del enlace inverso 118. Ejemplos de los AT pueden incluir SET, teléfonos móviles, PDA, tabletas inalámbricas y similares. El terminal de acceso 122 se comunica con las antenas 106 y 108, mientras que las antenas 106 y 108 transmiten información al terminal de acceso 122 a través del enlace directo 126 y reciben información desde el terminal de acceso 122 a través del enlace inverso 124. En un sistema de duplexación por división de frecuencia (FDD), los enlaces de comunicaciones 118, 120, 124 y 126 pueden usar diferentes frecuencias para las comunicaciones. Por ejemplo, el enlace directo 120 puede usar una frecuencia diferente a la usada por el enlace inverso 118.

Cada grupo de antenas y/o el área en la que están diseñados para comunicarse puede denominarse sector del punto de acceso. En la realización, cada grupo de antenas está diseñado para comunicarse con terminales de acceso en un sector de las áreas cubiertas por el punto de acceso 100.

En la comunicación a través de los enlaces directos 120 y 126, las antenas de transmisión del punto de acceso 100 pueden utilizar conformación de haz para mejorar la relación de señal a ruido de enlaces directos para los diferentes terminales de acceso 116 y 122. Además, un punto de acceso que utiliza conformación de haz para la transmisión a terminales de acceso dispersados de manera aleatoria en su área de cobertura puede generar menos interferencias en los terminales de acceso de células vecinas que un punto de acceso que transmite a través de una única antena a todos sus terminales de acceso. En algunas realizaciones no se lleva a cabo la conformación de haz.

Pueden utilizarse otros puntos de acceso o estaciones de transmisión. Por ejemplo, una estación base puede usarse además o en lugar del AP 100. En algunas realizaciones, un primer transmisor tal como el AP 100 puede proporcionar acceso a una primera red, mientras que un segundo transmisor, por ejemplo una estación base celular, puede proporcionar acceso a una segunda red. En algunas realizaciones, las áreas en las que puede accederse al

primer transmisor y al segundo transmisor están solapadas.

La FIG. 2 es un diagrama de bloques de una realización de un sistema transmisor 210 (que puede implementar, por ejemplo, el punto de acceso 100) y de un sistema receptor 250 (que puede implementar, por ejemplo, el terminal de acceso 116) en un sistema MIMO 200. Sin embargo, debe observarse que aunque se describe un sistema MIMO 200 de ejemplo, en algunas realizaciones no se usa MIMO, ya que pueden usarse otros sistemas (por ejemplo, SISO, MISO, SIMO, etc.). En el sistema transmisor 210, los datos de tráfico para una pluralidad de flujos de datos se proporcionan desde una fuente de datos 212 a un procesador de datos de transmisión (TX) 214.

En algunas realizaciones, cada flujo de datos se transmite a través de una antena de transmisión respectiva. El procesador de datos TX 214 formatea, codifica y entrelaza los datos de tráfico para cada flujo de datos basándose en un esquema de codificación particular seleccionado para que ese flujo de datos proporcione datos codificados.

Los datos codificados para cada flujo de datos pueden multiplexarse con datos piloto utilizando técnicas OFDM. Los datos piloto son normalmente un patrón de datos conocido que se procesa de una manera conocida y que puede utilizarse en el sistema receptor para estimar la respuesta de canal. Los datos piloto multiplexados y los datos codificados para cada flujo de datos se modulan después (es decir, se mapean con símbolos) en función de un esquema de modulación particular (por ejemplo, BPSK, QPSK, M-PSK, o M-QAM) seleccionado para que ese flujo de datos proporcione símbolos de modulación. La velocidad de transferencia de datos, la codificación y la modulación de cada flujo de datos puede determinarse mediante instrucciones llevadas a cabo por un procesador 230.

Los símbolos de modulación para todos los flujos de datos se proporcionan después a un procesador MIMO TX 220, que puede procesar adicionalmente los símbolos de modulación (por ejemplo, para OFDM). El procesador MIMO TX 220 proporciona después NT flujos de símbolos de modulación a NT transmisores (TMTR) 222a a 222t. En determinadas realizaciones, el procesador MIMO TX 220 aplica pesos de conformación de haz a los símbolos de los flujos de datos y a la antena desde la cual se está transmitiendo el símbolo.

Cada transmisor 222 recibe y procesa un flujo de símbolos respectivo para proporcionar una o más señales analógicas y acondiciona adicionalmente (por ejemplo, amplifica, filtra y convierte de manera ascendente) las señales analógicas para proporcionar una señal modulada adecuada para su transmisión a través del canal MIMO. Después, NT señales moduladas de los transmisores 222a a 222t se transmiten desde NT antenas 224a a 224t, respectivamente.

En el sistema receptor 250, las señales moduladas transmitidas se reciben por NR antenas 252a a 252r y la señal recibida desde cada antena 252 se proporciona a un receptor respectivo (RCVR) 254a a 254r. Cada receptor 254 acondiciona (por ejemplo, filtra, amplifica y convierte de manera descendente) una señal recibida respectiva, digitaliza la señal acondicionada para proporcionar muestras y procesa adicionalmente las muestras para proporcionar un flujo de símbolos "recibido" correspondiente.

Después, un procesador de datos RX 260 recibe y procesa los NR flujos de símbolos recibidos desde los NR receptores 254 basándose en una técnica de procesamiento de receptor particular para proporcionar NT flujos de símbolos "detectados". Después, el procesador de datos RX 260 desmodula, desentrelaza y descodifica cada flujo de símbolos detectado para recuperar los datos de tráfico para el flujo de datos. El procesamiento del procesador de datos RX 260 es complementario al realizado por el procesador MIMO TX 220 y el procesador de datos TX 214 en el sistema transmisor 210.

Un procesador 270 puede determinar periódicamente qué matriz de precodificación utilizar. El procesador 270 puede formular un mensaje de enlace inverso que comprende una parte de índice de matriz y una parte de valor de rango.

El mensaje de enlace inverso puede comprender varios tipos de información relacionados con el enlace de comunicación y/o con el flujo de datos recibido. Después, el mensaje de enlace inverso se procesa mediante un procesador de datos TX 238, que también recibe datos de tráfico para una pluralidad de flujos de datos desde una fuente de datos 236, se modula por un modulador 280, se acondiciona por los transmisores 254a a 254r y se envía al sistema transmisor 210. Dos o más receptores, transmisores y grupos de antenas pueden estar configurados para acceder a redes diferentes, por ejemplo una red WLAN y una red LTE, WCDMA, o HPRD cdma2000. En algunas realizaciones, un único receptor, transmisor y grupo de antenas puede estar configurado para acceder a al menos dos redes diferentes. Asimismo, una pluralidad de procesadores puede incluirse para procesar comunicaciones y/o datos para una pluralidad de redes. Además, un único procesador puede configurarse para procesar comunicaciones y/o datos para una pluralidad de redes.

En el sistema transmisor 210, las señales moduladas del sistema receptor 250 se reciben por las antenas 224, se acondicionan por los receptores 222, se desmodulan por un desmodulador 240 y se procesan por un procesador de datos RX 242 para extraer el mensaje de enlace inverso transmitido por el sistema receptor 250. Después, el procesador 230 determina qué matriz de precodificación utilizar para determinar los pesos de conformación de haz y después procesa el mensaje extraído.

Se presentan aparatos, procedimientos, sistemas y medios legibles por ordenador para obtener conexiones seguras con un servidor de localización descubierto. A medida que los servicios relacionados con la localización de dispositivos móviles se vuelven más populares, las soluciones de localización y los servidores de localización asociados que permiten y colaboran en tales soluciones de localización se utilizan de manera más generalizada. Un ejemplo de una solución de localización de este tipo es la solución SUPL definida por la OMA. Otro ejemplo es la solución de localización CP definida por 3GPP. En el caso de la solución de localización SUPL y otras determinadas soluciones de localización, por ejemplo definidas por el Grupo de Tareas sobre Ingeniería de Internet (IETF), los servidores de localización pueden estar limitados algunas veces a soportar la localización de dispositivos móviles en áreas geográficas de tamaño pequeño o mediano (por ejemplo, un centro comercial, un aeropuerto, un pueblo o una ciudad). En tales casos, un servidor de localización puede necesitar primero ser descubierto por un dispositivo móvil y después estar autorizado para usarse por alguna entidad fiable tal como una red local de un dispositivo móvil o un servidor de localización de red local. En este caso, un posible problema puede ser la incapacidad de obtener acceso a la red local o al servidor de localización de red local de tal manera que la red local o el servidor de localización de red local puede autenticar el dispositivo móvil antes de proporcionar o autorizar las direcciones de uno o más servidores de localización locales autorizados para proporcionar servicios de localización al dispositivo móvil. Este problema puede producirse particularmente cuando un dispositivo móvil usa alguna intranet local (por ejemplo, una red WiFi) para acceder a un servidor de localización local, ya que la intranet local no puede permitir el acceso o autenticar el acceso a la red local del dispositivo móvil o al servidor de localización de red local.

Según algunas realizaciones, para ilustrar estos y otros problemas, un terminal de acceso (AT), por ejemplo un dispositivo móvil y/o el AT 116, puede descubrir un servidor de localización accesible a través de alguna red A que el AT está usando actualmente. Por ejemplo, la dirección del servidor de localización puede proporcionarse (por ejemplo, difundirse) por estaciones base y puntos de acceso, por ejemplo el AP 100, que pertenecen a la red A y, por tanto, a los que el AT puede acceder libremente. Como alternativa, el AT puede consultar alguna entidad de la red A para determinar la dirección (por ejemplo, puede realizar una consulta usando el protocolo de configuración dinámica de *host* (DHCP) de IETF) o el AT puede conseguir la dirección cuando se acopla a la red A o puede conseguir la dirección de algún otro modo. El AT puede desear acceder al servidor de localización descubierto por varios motivos, por ejemplo para servicios de localización, en lugar de a cualquier servidor de localización local que el AT pueda tener. Esto puede deberse a que el servidor de localización descubierto puede proporcionar mejor servicio en el área particular en que el AT está actualmente ubicado (por ejemplo, el AT puede estar desplazándose en un área remota al servidor local, o puede estar dentro de un edificio u otra estructura de la que el servidor local tiene poca o ninguna información), o por cualquier otro motivo o diversidad de motivos. Antes de acceder al servidor de localización descubierto, el AT puede necesitar que el servidor de localización descubierto esté autorizado por el servidor de localización local, por ejemplo, con el fin de ajustarse a organismos de normalización y garantizar que el AT puede confiar en el servidor de localización descubierto para proporcionar los servicios y para no proporcionar un acceso o información no autorizados del AT a otras partes. Además, el AT puede recibir información desde su servidor de localización local (por ejemplo, certificados de seguridad) antes de acceder al servidor de localización descubierto para permitir al servidor de localización descubierto autenticar el AT y, por tanto, cobrar de manera fiable al usuario o la red local del AT por cualquier servicio, si se ha establecido un acuerdo comercial de este tipo.

Sin embargo, puede ser imposible o muy difícil que el AT pueda acceder a su servidor de localización local usando la red A. Por ejemplo, la red A puede ser una intranet interna de alguna organización o lugar de celebración de eventos y no tener acceso a una red pública, o la red A puede tener acceso a una red pública y permitir que el AT se comunique con su servidor de localización local, pero el servidor de localización local puede no ser capaz de autenticar el AT. Por ejemplo, si la red A es una red de área local inalámbrica (WLAN) con acceso a red pública, la dirección IP del AT puede asignarse por la WLAN y no sería conocida o no podría verificarse por el servidor de localización local o por la red local del usuario del AT. Esto podría significar que cualquier mecanismo de autenticación usado normalmente para autenticar el AT podría no ser utilizado por el servidor de localización local para autenticar el AT, y el servidor de localización local podría rechazar entonces cualquier solicitud para la autorización del servidor de localización descubierto recibida desde el AT. Un ejemplo de un mecanismo de autenticación de este tipo usado por la solución SUPL y definido por la OMA se conoce como autenticación de cliente alternativo (ACA) y usa la capacidad de un servidor de localización local, conocida como plataforma de localización SUPL local (H-SLP), para asociar una dirección IP pública de un SET con una identidad global única del SET, tal como el número de red digital de servicios integrados de estación móvil (MSISDN) o la identidad internacional de abonado móvil (IMSI). Además, el estado de la red A puede impedir que el AT acceda al servidor de localización local. Por ejemplo, la red A, la red local del AT o encaminadores, pasarelas o redes intermedios pueden imponer restricciones en la comunicación con la red local del AT o el AT puede no estar autorizado en la red A para efectuar tal comunicación. Como alternativa, la red A puede estar congestionada o tener una baja disponibilidad de ancho de banda, ocasionando en el AT demasiadas interrupciones, retardos o colisiones. Además, puede no ser posible que el AT autentique el servidor de localización local si el procedimiento de autenticación que va a usarse necesita algún tipo de ayuda de la red local del AT.

Para resolver estos problemas, el AT puede conmutar desde la red A hasta otra red B (por ejemplo, una red LTE, WCDMA o de datos por paquetes de alta velocidad (HRPD) cdma2000) que permita comunicaciones con el servidor de localización local y que permita la autenticación del AT por medio del servidor de localización local. Por ejemplo,

los mecanismos de autenticación pueden usarse por un servidor de localización local en algunas realizaciones cuando un AT accede al mismo desde una red LTE, WCDMA o HRPD ya que el servidor local puede verificar la identidad del AT a partir de la dirección IP que el AT usa para acceder al servidor local. Esta verificación puede ser posible ya que la red local del AT puede conocer la dirección IP asignada al AT (por ejemplo, a partir de una asociación con una dirección global para un AT tal como una IMSI o una MSISDN) o puede realizar una consulta para obtener la identidad del AT (por ejemplo, una IMSI o una MSISDN) conociendo la dirección IP.

Las FIG. 3A, 3B y 3C ilustran los mecanismos anteriormente mencionados según algunas realizaciones. Con referencia a estas figuras y a las figuras y descripción subsiguientes, los términos "servidor de localización descubierto" y "servidor descubierto" se usan como sinónimos, así como los términos "servidor de localización local" y "servidor local". Haciendo referencia a la FIG. 3A, un escenario de red 300 de ejemplo muestra un AT, por ejemplo el AT 116, dentro de la cobertura de la red A. Aquí, el AT ha descubierto un servidor descubierto pero aún no tiene un acceso autorizado al mismo. En este ejemplo, el AT no puede acceder al servidor descubierto para obtener soporte para servidores de localización tal como (i) obtener datos de asistencia desde el servidor descubierto para permitir que el AT se localice a sí mismo a partir de mediciones realizadas por el AT de puntos de acceso que pertenecen a la red A o (ii) hacer que el servidor descubierto localice el AT a partir de mediciones realizadas por el AT y/o por la red A del AT. Por ejemplo, las mediciones pueden comprender mediciones de temporización y de intensidad de señal de estaciones base cercanas (por ejemplo, el AP 100), mediciones de temporización para satélites de navegación global, mediciones de tiempo de ida y vuelta (RTT), mediciones del indicador de intensidad de señal recibida (RSSI), mediciones asistidas del sistema global de navegación por satélite (GNSS) y similares. Esta incapacidad de acceder al servidor descubierto puede producirse debido a que la red A no soporta los medios de autenticación para el AT y, por tanto, no puede señalizar al servidor descubierto ninguna información de autenticación suficiente para el AT ni, por tanto, permitir que el servidor descubierto autentique el AT (por ejemplo, para permitir una facturación subsiguiente del AT o de la red local del AT en relación con cualquier servicio de localización proporcionado al AT por el servidor descubierto). Además, el AT puede obtener tal información de autenticación (para permitir la autenticación del AT por medio del servidor descubierto) a través de su servidor local, pero la red A puede no proporcionar ningún medio para acceder al servidor local o ningún medio para que el servidor local autentique el AT si puede accederse al servidor local. Además, incluso cuando el servidor descubierto puede autenticar el AT a través de la red A o no necesita autenticar el AT (por ejemplo, porque los servicios de localización se proporcionan libremente para el acceso a través de la red A), el AT puede no ser capaz de acceder al servidor local desde la red A para obtener autorización del servidor descubierto o puede ser capaz de acceder al servidor local a través de la red A pero ser incapaz de autenticar el servidor local o no poder ser autenticado por el servidor local. Como se ha descrito anteriormente, tales impedimentos pueden deberse a varias razones, incluyendo que la red A no tenga acceso a una red pública tal como Internet, que la red local no tenga medios para verificar una dirección IP asignada por la red A, restricciones en la comunicación impuestas por la red A, la red local o entidades intermedias, que haya demasiado tráfico en la red A, que no haya configuraciones de red apropiadas para acceder al servidor local u otros impedimentos.

Haciendo referencia a la FIG. 3B, en algunas realizaciones, siguiendo con el escenario presentado en la FIG. 3A, el AT puede conmutar después a una segunda red, la red B, que permite un acceso autenticado al servidor local, como se muestra en el escenario de red 325 de ejemplo. Después, el AT puede conectarse al servidor local en un esfuerzo por conectarse en última instancia al servidor descubierto encontrado en la red A. En el escenario ejemplificado en la FIG. 3B, la red B puede permitir una o más de las siguientes capacidades: (i) acceso al servidor local mediante el AT; (ii) autenticación del AT por medio del servidor local; (iii) autenticación del servidor local por medio del AT; (iv) descubrimiento del servidor descubierto por medio del AT a partir del servidor local; (v) autorización del servidor descubierto por medio del servidor local incluyendo información que indica al AT bajo qué circunstancias (por ejemplo, en qué ubicaciones o desde qué redes) puede acceder al servidor descubierto; (vi) provisión de información desde el servidor local al AT para permitir la autenticación del AT por medio del servidor descubierto; y (vii) provisión de información por medio del servidor local al AT para permitir que la autenticación del servidor descubierto por medio del AT. Estas capacidades habilitadas pueden no ser soportadas por la red A en el escenario mostrado en la FIG. 3A, impidiendo así inicialmente que el AT acceda al servidor descubierto.

Haciendo referencia a la FIG. 3C, siguiendo con este escenario, en algunas realizaciones, el AT conmuta a la red A, habiendo usado ahora cualquiera de las capacidades (i), (ii), (iii), (iv), (v), (vi) y (vii) descritas anteriormente y poseyendo cualquier información obtenida como consecuencia de estas capacidades, tal como información de autenticación o autorización para acceder al servidor descubierto. Después, el AT puede acceder al servidor descubierto a través de la red A para obtener servicios de localización. El acceso al servidor descubierto a través de la red A en lugar de la red B puede ser preferido o incluso necesario, por ejemplo porque el servidor descubierto está en una intranet privada no accesible desde una red pública, tal como la red A, o porque el servidor descubierto solo proporciona servicios de localización en asociación con el acceso desde la red A o porque los costes de uso para el usuario del AT cuando usa la red A son inferiores a los costes cuando se usa la red B. Cuando el AT accede al servidor descubierto a través de la red A, puede usar información recibida desde el servidor local a través de la red B para (a) permitir la autenticación del AT por medio del servidor descubierto (por ejemplo, utilizando certificados de dispositivo proporcionados por el servidor local para este fin), (b) permitir la autenticación del servidor descubierto por medio del AT y/o (c) determinar cuándo el AT puede acceder y cuándo no al servidor descubierto, por ejemplo.

Haciendo referencia a las FIG. 4A, 4B y 4C se presenta un determinado escenario según otras realizaciones. Haciendo referencia a la FIG. 4A, un AT de ejemplo, por ejemplo el AT 116, puede ser un terminal (SET) con capacidad de localización segura en el plano de usuario (SUPL), que puede estar dentro del alcance de transmisión de la red A. Aquí, en el escenario de red 400, el SET puede haber descubierto un tipo de ejemplo de servidor descubierto, tal como una plataforma de localización SUPL descubierta (D-SLP). Sin embargo, el SET puede ser incapaz de acceder en primera instancia a la D-SLP ya que el SET no puede obtener una autorización para la D-SLP y/o información de autenticación para la D-SLP a partir de la SLP local (H-SLP) del SET, en la que el SET puede confiar para proporcionar información segura relacionada con la autorización y autenticación para la D-SLP. Como un ejemplo, la red A puede no proporcionar acceso a la H-SLP del SET o la red A puede proporcionar acceso pero no soportar o permitir la autenticación del SET por medio de la H-SLP del SET usando un procedimiento tal como el mecanismo de autenticación de cliente alternativo (ACA) de SUPL. Tales impedimentos pueden deberse a varias razones, incluyendo que la red A no tenga acceso a una red pública tal como Internet, que la red local no tenga medios para verificar una dirección IP asignada por la red A, restricciones en la comunicación impuestas por la red A, la red local o entidades intermedias, que haya demasiado tráfico en la red A, que no haya configuraciones de red apropiadas para acceder a la H-SLP u otros impedimentos.

Haciendo referencia a la FIG. 4B, en algunas realizaciones, siguiendo con el escenario presentado en la FIG. 4A, el SET puede conmutar después a una segunda red, la red B, que soporta un acceso a la H-SLP a partir del SET y la autenticación del SET por medio de la H-SLP usando, en este ejemplo, el procedimiento de autenticación ACA, como se muestra en el escenario de red 425 de ejemplo. El SET puede conectarse después a la H-SLP en un intento por conectarse en última instancia a la D-SLP encontrada en la red A. En algunas realizaciones, la red A podría ser una WLAN y, en algunas realizaciones, la red B podría ser una red LTE, WCDMA o HRPD, por ejemplo. Evidentemente, las redes A y B podrían ser otros tipos de red. Cuando el SET se conecta a la H-SLP a través de la red B, la H-SLP puede autenticar el SET usando el procedimiento ACA o algún otro procedimiento definido por la OMA para SUPL, tal como usar certificados de dispositivo o usar la arquitectura de inicialización genérica (GBA). Además, el SET puede autenticar la H-SLP usando, por ejemplo, un certificado de clave pública proporcionado por la H-SLP. Estos procedimientos de autenticación pueden ser posibles usando la red B, pero no ser posibles o estar limitados de alguna manera usando la red A. La H-SLP puede proporcionar después la dirección de la D-SLP al SET, puede autorizar la D-SLP para el SET y/o puede proporcionar información (a) que indica al SET bajo qué condiciones puede accederse a la D-SLP y/o (b) que permite que la D-SLP autentique el SET o que el SET autentique la D-SLP.

Haciendo referencia a la FIG. 4C, siguiendo con este escenario, en algunas realizaciones, el SET conmuta a la red A, poseyendo ahora suficiente información y/o autorización de la H-SLP para acceder a la D-SLP, en el escenario de red 450. Después, el SET puede acceder a la D-SLP a través de la red A para obtener servicios de localización. El acceso a la D-SLP a través de la red A en lugar de la red B puede ser preferido o incluso necesario en algunas realizaciones, por ejemplo porque la D-SLP está en una intranet privada no accesible desde una red pública o porque la D-SLP solo proporciona servicios de localización en asociación con el acceso desde la red A o porque los costes de uso para el usuario del SET en la red A son inferiores a los del acceso desde la red B. Cuando el SET accede a la D-SLP a través de la red A, puede usar información recibida desde la H-SLP a través de la red B para (a) permitir la autenticación del SET por medio de la D-SLP (por ejemplo, utilizando certificados de dispositivo proporcionados por la H-SLP para este fin), (b) permitir la autenticación de la D-SLP por medio del SET y/o (c) determinar cuándo el SET puede acceder y cuándo no a la D-SLP, por ejemplo.

Haciendo referencia a la FIG. 5A, un diagrama de flujo 500 describe varias etapas de procedimiento según algunas realizaciones. Estas pueden describirse en los siguientes procesos y pueden ser compatibles con los diagramas ilustrados y descritos en cualquiera de las FIG. 1, 2, 3A, 3B, 3C, 4A, 4B y 4C. Un SET puede necesitar acceder a un servidor de localización descubierto usando una primera red para obtener servicios de localización en su ubicación actual. El SET puede ser consciente (por ejemplo, a partir de información de configuración) de que necesita información de autorización y/o de autenticación para acceder al servidor de localización descubierto a partir de un servidor de localización local.

Sin embargo, el SET puede no ser capaz de obtener un acceso autenticado al servidor de localización local desde la primera red y, por lo tanto, puede ser incapaz de obtener la información de autorización y/o de autenticación usando la primera red, por ejemplo por uno o más motivos relacionados con cualquiera de las razones descritas en la divulgación del presente documento. La primera red puede ser cualquier tipo de red digital y puede ser compatible con lo descrito en relación con la red A en la descripción anterior, por ejemplo.

En el bloque 502, el SET puede conmutar desde la primera red hasta una segunda red que soporta un acceso autenticado del SET al servidor de localización local. Una segunda red de ejemplo que puede ajustarse a esta descripción puede ser la red B según las descripciones anteriores. El SET puede implementarse por el AT 116 y/o el sistema 250, por ejemplo. En tales realizaciones, el bloque 502 puede llevarse a cabo, por ejemplo, por al menos el transceptor 252.

En el bloque 504, el SET puede obtener un acceso autenticado al servidor de localización local usando la segunda red, por ejemplo con el procesador 270 cuando el SET está implementado por el sistema 250. El servidor de

localización local puede ser una H-SLP y puede ser compatible con las descripciones de las FIG. 3A, 3B, 3C, 4A, 4B y 4C.

En el bloque 506, el SET puede obtener del servidor de localización local información de autorización y/o de autenticación para el servidor de localización descubierto, por ejemplo con el procesador 270 cuando el SET está implementado por el sistema 250. Debe recordarse que la autorización desde el servidor de localización local puede producirse cuando está usándose la segunda red. El servidor de localización descubierto puede ser una D-SLP y puede ser compatible con las descripciones de las FIG. 3A, 3B, 3C, 4A, 4B y 4C.

En el bloque 508, el SET puede conmutar desde la segunda red hasta la primera red, por ejemplo con el transceptor 252 cuando el SET está implementado por el sistema 250. En este momento, el SET puede haber obtenido una autorización para el servidor de localización descubierto. En el bloque 510, el SET puede acceder al servidor de localización descubierto usando la autenticación obtenida del servidor de localización local mientras usa la segunda red, por ejemplo con el procesador 270 cuando el SET está implementado por el sistema 250.

Haciendo referencia a la FIG. 5B, el diagrama de flujo 530 puede representar una conjunto alternativo de etapas de procedimiento según otras realizaciones. Estas descripciones pueden ser compatibles con cualquiera de las descripciones de las FIG. 1, 2, 3A, 3B, 3C, 4A, 4B y 4C.

En el bloque 532, en algunas realizaciones, un AT puede usar una WLAN y descubrir un servidor descubierto (por ejemplo, descubrir la dirección de un servidor no conocido anteriormente difundida desde la WLAN). El AT usado en este ejemplo puede ser compatible con el AT 116 y/o el sistema 250, por ejemplo. En tales realizaciones, el bloque 532 puede llevarse a cabo, por ejemplo, por al menos el transceptor 252.

En el bloque 534, el AT necesita una autorización para el servidor descubierto a partir del servidor local y trata de acceder al servidor local usando una primera red (por ejemplo, una WLAN). Si el AT no puede acceder al servidor local, por ejemplo porque la WLAN no tiene acceso a una red pública, el AT avanza hasta el bloque 542. El bloque 534 puede llevarse a cabo, por ejemplo, por al menos el transceptor 252 y el procesador 270.

Sin embargo, si el AT puede acceder al servidor local, en el bloque 536, el AT trata después de establecer una conexión IP segura con el servidor local usando, por ejemplo, el procesador de datos Tx 238 a través del transceptor 252. En este momento puede producirse uno de dos eventos que son importantes para la presente divulgación. En el bloque 538, el servidor local puede rechazar el intento de proteger la conexión IP. Este rechazo puede deberse a varios motivos, incluyendo que se produzca una conexión fallida intermitente o la ausencia de medios de autenticación apropiados en la primera red, u otros motivos. Además o como alternativa, en el bloque 540, el servidor local puede indicar un fallo de autenticación y enviar un mensaje que indica el mismo al AT. El AT puede recibir tales indicaciones en el transceptor 252. Por ejemplo, el servidor local puede ser incapaz de verificar la dirección IP del AT proporcionada por la primera red y, por tanto, la autenticación puede fallar.

Desde cualquiera de los bloques 534, 538 o 540, en el bloque 542, tras no poder acceder en última instancia al servidor local, el AT conmuta desde la primera red hasta una segunda red que soporta un acceso al servidor local y la autenticación del AT por medio del servidor local, por ejemplo usando el transceptor 252. Por ejemplo, mientras está en la segunda red, el AT puede obtener una dirección IP que el servidor local puede reconocer en última instancia como asignada a una identidad global conocida que pertenece al AT. Después, en el bloque 544, el AT obtiene un acceso autenticado al servidor local usando la segunda red. El bloque 544 puede implementarse, por ejemplo, por al menos el procesador 270 y el transceptor 252.

En el bloque 546, usando, por ejemplo, el transceptor 252, el AT solicita y recibe una autorización para el servidor descubierto y también puede recibir información para permitir un acceso autenticado al servidor descubierto. El AT puede tener ahora suficiente información de autorización y, posiblemente, suficiente información de autenticación para el servidor descubierto usando el acceso autenticado obtenido en la segunda red a partir del servidor local. En el bloque 548, el AT conmuta desde la segunda red hasta la primera red, por ejemplo con el transceptor 252 y/o el procesador 270, con el fin de acceder al servidor descubierto, por ejemplo debido a que el servidor descubierto no puede ser accedido desde la segunda red o porque la segunda red genera menos costes de acceso para el usuario del AT. Después, el AT obtiene acceso al servidor descubierto, que está ahora en la red apropiada y que posee suficiente información de autorización y, opcionalmente, de autenticación para acceder al servidor descubierto. En algunas realizaciones, en el bloque 550, el AT y el servidor descubierto pueden usar certificados de dispositivo para llevar a cabo una autenticación mutua con los certificados de dispositivo posiblemente proporcionados al AT por el servidor local como parte del bloque 546. Como alternativa, el servidor descubierto no puede autenticar el AT porque el acceso al servidor descubierto puede estar restringido a la primera red y el servidor descubierto puede proporcionar servicios de localización gratis a cualquier AT que use la primera red.

Teniendo ahora acceso al servidor descubierto, el AT puede obtener servicios de localización a partir del servidor descubierto, por ejemplo puede obtener datos de ayuda a la localización, datos de mapas locales, cálculo de su ubicación.

Haciendo referencia a la FIG. 5C, el diagrama de flujo 560 puede representar un conjunto alternativo de etapas de procedimiento según otras realizaciones. Estas descripciones pueden ser compatibles con cualquiera de las descripciones de las FIG. 1, 2, 3A, 3B, 3C, 4A, 4B y 4C. El diagrama de flujo 560 puede proporcionar una implementación de ejemplo de la FIG. 5B.

En el bloque 562, en algunas realizaciones, un SET puede usar una WLAN y descubrir una plataforma de localización SUPL descubierta (D-SLP) (por ejemplo, descubrir la dirección de una SLP no conocida anteriormente difundida desde la WLAN). El SET usado en este ejemplo puede ser compatible con el AT 116 y/o el sistema 250, por ejemplo. En tales realizaciones, el bloque 562 puede llevarse a cabo, por ejemplo, por al menos el transceptor 252.

En el bloque 564, el SET necesita autorización para la D-SLP a partir de una plataforma de localización SUPL local (H-SLP) y trata de acceder a la H-SLP usando una primera red que puede ser la WLAN usada para descubrir la D-SLP. Si el SET no puede acceder a la H-SLP, por ejemplo porque la primera red no tiene acceso a una red pública, el SET avanza hasta el bloque 572. El bloque 564 puede llevarse a cabo, por ejemplo, por al menos el transceptor 252 y el procesador 270.

Sin embargo, si el SET puede acceder a la H-SLP, en el bloque 566, el SET trata después de establecer una conexión IP segura con la H-SLP usando, por ejemplo, el procesador de datos Tx 238 a través del transceptor 252. En este momento puede producirse uno de dos eventos en el ejemplo ilustrado. En el bloque 568, la H-SLP puede rechazar el intento de proteger la conexión IP. Este rechazo puede deberse a varios motivos, incluyendo que se produzca una conexión fallida intermitente o la ausencia de medios de autenticación apropiados en la primera red, u otros motivos. Además o como alternativa, en el bloque 570, la H-SLP puede indicar un fallo de autenticación y envía un mensaje que indica el mismo al SET. El SET puede recibir tales indicaciones en el transceptor 252. Por ejemplo, la H-SLP puede ser incapaz de verificar la dirección IP proporcionada por la primera red y, por tanto, la autenticación puede fallar. En algunas realizaciones, la H-SLP trata de autenticar el SET usando el procedimiento ACA pero no puede verificar la dirección IP del SET (asignada por la WLAN). La H-SLP rechaza el intento de establecer una conexión IP segura, en el bloque 568, o indica al SET un fallo en la autenticación ACA, por ejemplo enviando un mensaje SUPL END con un código de error apropiado, en el bloque 570.

Desde cualquiera de los bloques 564, 568 o 570, en el bloque 572, tras no haber podido acceder en última instancia a la H-SLP, el SET conmuta desde la primera red hasta una segunda red que soporta la autenticación del SET por medio de la H-SLP, por ejemplo usando el transceptor 252. En algunas realizaciones, la segunda red soporta LTE. En algunas realizaciones, la segunda red puede soportar WCDMA, GSM o HRPD cdma2000. Por ejemplo, cuando está en la segunda red, el SET puede obtener una dirección IP que la H-SLP puede reconocer en última instancia como asignada al SET a través de la asociación de la dirección IP con una identidad global conocida por el SET, tal como una MSDISDN o una IMSI. Después, en el bloque 574, el SET obtiene un acceso autenticado a la H-SLP usando la segunda red. El bloque 574 puede implementarse, por ejemplo, por al menos el procesador 270 y el transceptor 252.

En el bloque 576, el SET solicita y recibe, usando por ejemplo el transceptor 252, autorización para la D-SLP desde la H-SLP y también puede recibir información para permitir la autenticación del SET por medio de la D-SLP o la autenticación de la D-SLP por medio del SET. El SET puede tener ahora suficiente información de autorización y, posiblemente, de autenticación para permitir el acceso a la D-SLP usando la información de autorización y, posiblemente, de autenticación obtenida en la segunda red a partir de la H-SLP. En el bloque 578, el SET conmuta desde la segunda red hasta la primera red, por ejemplo con el transceptor 252 y/o el procesador 270, con el fin de acceder a la D-SLP, por ejemplo debido a que la D-SLP no puede ser accedida desde la segunda red o porque la segunda red genera menos costes de acceso para el usuario del SET. El SET obtiene acceso a la D-SLP, que está ahora en la red apropiada y que posee suficiente información de autorización y, posiblemente, de autenticación para acceder a la D-SLP. En algunas realizaciones, en el bloque 580, el SET y la D-SLP pueden usar certificados de dispositivo para llevar a cabo una autenticación mutua, por ejemplo con los certificados de dispositivo proporcionados al SET por la H-SLP como parte del bloque 576. Por ejemplo, la autenticación mutua puede ser compatible con la SUPL 2.1 o la SUPL 3.0 definidas por la OMA. Como alternativa, la D-SLP no puede autenticar el SET porque el acceso a la D-SLP puede estar restringido a la primera red y la D-SLP puede proporcionar servicios de localización gratis a cualquier SET que use la primera red.

Teniendo ahora acceso a la D-SLP, el SET puede obtener servicios de localización desde la D-SLP, por ejemplo para obtener datos de asistencia de localización, datos de mapas locales, cálculo de su ubicación.

Las figuras y diagramas de flujo anteriores proporcionan realizaciones en las que un AT no puede obtener información de autorización ni, posiblemente, de autenticación para poder acceder a un servidor de localización descubierto usando una primera red, y conmuta a una segunda red con el fin de obtener acceso autenticado a un servidor de localización local que puede autorizar al servidor de localización descubierto y, si fuera necesario, proporcionar información para permitir un acceso autenticado subsiguiente por medio del AT al servidor de localización descubierto. Después, el AT conmuta a la primera red para acceder al servidor de localización descubierto. En algunas realizaciones, el AT puede no necesitar o puede preferir no conmutar a la primera red y, en

cambio, puede acceder al servidor de localización descubierto usando la segunda red o usando alguna otra tercera red diferente a la primera y la segunda red. En algunos escenarios, tales realizaciones pueden reducir el retardo a la hora de acceder al servidor de localización descubierto y pueden permitir una autenticación mejorada del AT por medio del servidor de localización descubierto o del servidor de localización descubierto por medio del AT que es posible cuando el AT accede al servidor de localización descubierto usando la primera red.

Tras haber descrito anteriormente múltiples aspectos, un ejemplo de un sistema informático en el que tales aspectos pueden implementarse puede describirse ahora con respecto a la FIG. 6. Según uno o más aspectos, un sistema informático como el ilustrado en la FIG. 6 puede incorporarse como parte de un dispositivo informático, que puede implementar, llevar a cabo y/o ejecutar cualquiera y/o todas las características, procedimientos y/o etapas de procedimiento descritos en el presente documento. Por ejemplo, uno o más del procesador 610, la memoria 635 y los subsistemas de comunicaciones 630 pueden usarse para implementar cualquiera o todos los bloques mostrados en las FIG. 5A, 5B y 5C. Por ejemplo, el sistema informático 600 puede representar algunos de los componentes de un dispositivo manual. Un dispositivo manual puede ser cualquier dispositivo informático con una unidad sensorial de entrada, tal como una cámara y/o una unidad de visualización. Ejemplos de un dispositivo manual incluyen, pero no están limitados a, consolas de videojuegos, tabletas, teléfonos inteligentes y dispositivos móviles. En algunas realizaciones, el sistema 600 está configurado para implementar el dispositivo 250 descrito anteriormente. Por ejemplo, el procesador 610 puede usarse para implementar alguno o todos del procesador de datos Rx 260, el procesador 270 y el procesador de datos Tx 238. El / los dispositivo(s) de entrada 615 puede(n) usarse para implementar algunos o todos los transceptores 252(a)-(r). La memoria 635 puede usarse para implementar la memoria 272, y el subsistema de comunicaciones 630 puede usarse para implementar el modulador 280. La FIG. 6 proporciona una ilustración esquemática de una realización de un sistema informático 600 que puede llevar a cabo los procedimientos proporcionados por otras diversas realizaciones, descritas en el presente documento, y/o que puede funcionar como el sistema informático central, un quiosco / terminal remoto, un dispositivo de punto de venta, un dispositivo móvil, un descodificador y/o un sistema informático. La FIG. 6 tiene simplemente como objetivo proporcionar una ilustración generalizada de varios componentes, pudiendo utilizarse cualquiera de ellos y/o todos ellos según sea necesario. Por lo tanto, la FIG. 6 ilustra en términos generales cómo elementos de sistema individuales pueden implementarse de manera relativamente independiente o de una manera relativamente más integrada.

El sistema informático 600 se muestra comprendiendo elementos de hardware que pueden acoplarse eléctricamente a través de un bus 605 (o que pueden comunicarse de otro modo, según sea apropiado). Los elementos de hardware pueden incluir uno o más procesadores 610, incluyendo de manera no limitativa uno o más procesadores de propósito general y/o uno o más procesadores de propósito especial (tales como chips de procesamiento de señales digitales, procesadores de aceleración de gráficos y/o similares); uno o más dispositivos de entrada 615, que pueden incluir de manera no limitativa una cámara, un ratón, un teclado y/o similares; y uno o más dispositivos de salida 620, que pueden incluir de manera no limitativa una unidad de visualización, una impresora y/o similares.

El sistema informático 600 puede incluir además (y/o puede estar en comunicación con) uno o más dispositivos de almacenamiento no transitorios 625 que pueden comprender, de manera no limitativa, medios de almacenamiento locales y/o accesibles por red, y/o puede incluir, de manera no limitativa, una unidad de disco, una serie de unidades, un dispositivo de almacenamiento óptico, un dispositivo de almacenamiento de estado sólido tal como una memoria de acceso aleatorio ("RAM") y/o una memoria de solo lectura ("ROM"), que puede ser programable, actualizarse de manera inmediata y/o similar. Tales dispositivos de almacenamiento pueden estar configurados para implementar cualquier medio de almacenamiento de datos apropiado, incluyendo de manera no limitativa varios sistemas de archivos, estructuras de bases de datos y/o similares.

El sistema informático 600 también puede incluir un subsistema de comunicaciones 630, que puede incluir de manera no limitativa un módem, una tarjeta de red (inalámbrica o cableada), un dispositivo de comunicación por infrarrojos, un dispositivo de comunicaciones inalámbricas y/o un conjunto de chips (tal como un dispositivo Bluetooth®, un dispositivo 802.11, un dispositivo WiFi, un dispositivo WiMax, componentes de comunicación celular, etc.) y/o similares. El subsistema de comunicaciones 630 puede permitir el intercambio de datos con una red (tal como la red descrita posteriormente, por citar un ejemplo), otros sistemas informáticos y/o cualquier otro dispositivo descrito en el presente documento. En muchas realizaciones, el sistema informático 600 puede comprender además una memoria de trabajo no transitoria 635, que puede incluir un dispositivo RAM o ROM, como los descritos anteriormente.

El sistema informático 600 también puede comprender elementos de software, mostrados dentro de la memoria de trabajo 635, que incluyen un sistema operativo 640, controladores de dispositivo, librerías ejecutables y/u otro código, tal como uno o más programas de aplicación 645, que pueden comprender programas de ordenador proporcionados por diversas realizaciones, y/o que pueden estar diseñados para implementar procedimientos y/o configurar sistemas, proporcionados por otras realizaciones, como los descritos en el presente documento. Simplemente a modo de ejemplo, una o más metodologías descritas con respecto al (a los) procedimiento(s) descrito(s) anteriormente, por ejemplo descritos con respecto a las FIG. 5A, 5B o 5C, pueden implementarse como código y/o instrucciones ejecutables por un ordenador (y/o un procesador de un ordenador); en un aspecto, tal código y/o instrucciones pueden usarse para configurar y/o adaptar un ordenador de propósito general (u otro

dispositivo) para llevar a cabo una o más operaciones según los procedimientos descritos.

Un conjunto de estas instrucciones y/o códigos puede almacenarse en un medio de almacenamiento legible por ordenador, tal como el / los dispositivo(s) de almacenamiento 625 descrito(s) anteriormente. En algunos casos, el medio de almacenamiento puede estar incorporado en un sistema informático, tal como el sistema informático 600. En otras realizaciones, el medio de almacenamiento puede ser independiente de un sistema informático (por ejemplo, un medio extraíble, tal como un disco compacto) y/o proporcionarse en un paquete de instalación, de modo que el medio de almacenamiento puede usarse para programar, configurar y/o adaptar un ordenador de propósito general con las instrucciones / código almacenados en el mismo. Estas instrucciones pueden tomar la forma de un código ejecutable, que puede ejecutarse por el sistema informático 600, y/o puede tomar la forma de un código fuente y/o instalable que, tras la compilación y/o instalación en el sistema informático 600 (por ejemplo, usando cualquiera de una variedad de compiladores, programas de instalación, componentes de compresión / descompresión, etc. disponibles generalmente) toma la forma de un código ejecutable.

Variaciones sustanciales pueden realizarse según requisitos específicos. Por ejemplo, también puede usarse hardware personalizado, y/o elementos particulares pueden implementarse en hardware, software (incluyendo software portable, tal como *applets*, etc.) o en ambos. Además, puede utilizarse una conexión con otros dispositivos informáticos, tales como dispositivos de red de entrada / salida.

Algunas realizaciones pueden utilizar un sistema informático (tal como el sistema informático 600) para llevar a cabo procedimientos según la divulgación. Por ejemplo, algunas o todas las metodologías de los procedimientos descritos pueden llevarse a cabo por el sistema informático 600 como respuesta a que el procesador 610 ejecute una o más secuencias de una o más instrucciones (que pueden incorporarse en el sistema operativo 640 y/u otro código, tal como un programa de aplicación 645) incluidas en la memoria de trabajo 635. Tales instrucciones pueden introducirse en la memoria de trabajo 635 desde otro medio legible por ordenador, tal como uno o más de los dispositivos de almacenamiento 625. Simplemente a modo de ejemplo, la ejecución de las secuencias de instrucciones contenidas en la memoria de trabajo 635 puede provocar que el / los procesador(es) 610 lleve(n) a cabo una o más metodologías de los procedimientos descritos en el presente documento, por ejemplo uno o más de los elementos del procedimiento descrito con respecto a cualquiera de las FIG. 5A, 5B o 5C.

Los términos "medio legible por máquina" y "medio legible por ordenador", como se usan en el presente documento, se refieren a cualquier medio que proporciona datos que hacen que una máquina funciona de manera específica. En una realización implementada usando el sistema informático 600, varios medios legibles por ordenador pueden utilizarse para proporcionar instrucciones / código a uno / varios procesador(es) 610 para la ejecución y/o pueden usarse para almacenar y/o transportar tales instrucciones / código (por ejemplo, como señales). En muchas implementaciones, un medio legible por ordenador es un medio de almacenamiento físico y/o tangible. Un medio de este tipo puede adoptar muchas formas, incluyendo pero sin limitarse a, medios no volátiles, medios volátiles y medios de transmisión. Los medios no volátiles incluyen, por ejemplo, discos ópticos y/o magnéticos, tales como el / los dispositivo(s) de almacenamiento 625. Los medios volátiles incluyen, de manera no limitativa, memoria dinámica, tal como la memoria de trabajo 635. Los medios de transmisión incluyen, de manera no limitativa, cables coaxiales, hilo de cobre y fibra óptica, incluyendo los hilos que comprenden el bus 605, así como los diversos componentes del subsistema de comunicaciones 630 (y/o los medios mediante los cuales el subsistema de comunicaciones 630 proporciona comunicación con otros dispositivos). Por tanto, los medios de transmisión también pueden adoptar la forma de ondas (incluyendo, de manera no limitativa, ondas de radio, acústicas y/o de luz, tales como las generadas durante comunicaciones de datos por ondas de radio y por infrarrojos).

En uno o más ejemplos, las funciones descritas pueden implementarse en hardware, software, firmware o cualquier combinación de lo anterior. Si se implementan en software, las funciones pueden almacenarse en o transmitirse como una o más instrucciones o código en un medio legible por ordenador. Los medios legibles por ordenador pueden incluir medios de almacenamiento de datos de ordenador. Los medios de almacenamiento de datos pueden ser cualquier medio disponible que pueda ser accedido por uno o más ordenadores o uno o más procesadores para recuperar instrucciones, código y/o estructuras de datos para la implementación de las técnicas descritas en esta divulgación. El término "medios de almacenamiento de datos", como se usa en el presente documento, se refiere a productos manufacturados y no se refiere a señales de propagación transitorias. A modo de ejemplo, y no de manera limitativa, tales medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, memoria flash o cualquier otro medio que pueda usarse para almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que pueda accederse mediante un ordenador. Los discos, tal y como se usan en el presente documento, incluyen discos compactos (CD), discos de láser, discos ópticos, discos versátiles digitales (DVD), discos flexibles y discos blu-ray, donde los discos normalmente reproducen datos de manera magnética así como de manera óptica con láser. Las combinaciones de lo anterior también deben incluirse dentro del alcance de los medios legibles por ordenador.

El código puede ser ejecutado por uno o más procesadores, tales como uno o más procesadores de señales digitales (DSP), microprocesadores de propósito general, circuitos integrados de aplicación específica (ASIC), matrices lógicas de campo programable (FPGA), u otro circuito lógico integrado o discreto equivalente. Por

consiguiente, el término "procesador", como se usa en el presente documento, puede referirse a cualquier estructura anterior o cualquier otra estructura adecuada para la implementación de las técnicas descritas en el presente documento. Además, en algunos aspectos, la funcionalidad descrita en el presente documento puede proporcionarse en hardware dedicado y/o módulos de software configurados para la codificación y la descodificación, o incorporarse en un códec combinado. Además, las técnicas podrían implementarse completamente en uno o más circuitos o elementos lógicos.

Las técnicas de esta divulgación se pueden implementar en una gran variedad de dispositivos o aparatos, incluyendo un teléfono inalámbrico, un circuito integrado (IC) o un conjunto de IC (por ejemplo, un conjunto de chips). Varios componentes, módulos o unidades se describen en esta divulgación para enfatizar aspectos funcionales de dispositivos configurados para realizar las técnicas descritas, pero no requieren necesariamente la realización mediante diferentes unidades de hardware. Más bien, como se ha descrito anteriormente, diversas unidades pueden combinarse en una unidad de hardware de códec o proporcionarse por un conjunto de unidades de hardware interoperativas, incluyendo uno o más procesadores como se ha descrito anteriormente, junto con software y/o firmware adecuado almacenado en medios legibles por ordenador.

Se han descrito varios ejemplos. Estos y otros ejemplos están dentro del alcance de las siguientes reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para obtener un acceso autorizado desde un terminal a un servidor de localización descubierto, comprendiendo el procedimiento:

conmutar (502, 542, 572) desde una primera red, que no soporta un acceso autenticado a un servidor de localización local el terminal, a una segunda red que soporta el acceso autenticado al servidor de localización local por el terminal; obtener (504, 544, 574) un acceso autenticado al servidor de localización local usando la segunda red;
obtener (506, 546, 576) autorización para el servidor de localización descubierto a partir del servidor de localización local;
conmutar (508, 548, 578) desde la segunda red de vuelta a la primera red, y acceder (510, 550, 578) al servidor de localización descubierto usando la primera red en función de la autorización obtenida del servidor de localización local.

2. El procedimiento de la reivindicación 1, en el que el servidor de localización local comprende una plataforma de localización local, H-SLP, de localización segura en el plano de usuario, SUPL.

3. El procedimiento de la reivindicación 2, en el que obtener un acceso autenticado comprende usar al menos uno de un mecanismo de autenticación de cliente alternativo, ACA, certificados de dispositivo y una arquitectura de inicialización genérica, GBA, para autenticar el terminal por medio de la H-SLP.

4. El procedimiento de la reivindicación 2, en el que obtener un acceso autenticado comprende usar un certificado de clave pública para autenticar la H-SLP por medio del terminal.

5. Un terminal (116, 122, 250) para obtener un acceso autorizado a un servidor de localización descubierto, comprendiendo el terminal:

un transceptor (254) configurado para:

conmutar desde una primera red, que no soporta un acceso autenticado a un servidor de localización local por el terminal, a una segunda red que soporta un acceso autenticado al servidor de localización local por el terminal; y
conmutar desde la segunda red de vuelta a la primera red después de que el terminal obtenga un acceso autenticado al servidor de localización local usando la segunda red; y

un procesador (270) configurado para:

obtener un acceso autenticado al servidor de localización local usando la segunda red; obtener una autorización para el servidor de localización descubierto a partir del servidor de localización local; y
acceder al servidor de localización descubierto usando la primera red en función de la autorización obtenida del servidor de localización local.

6. El terminal según la reivindicación 5, en el que el servidor de localización local comprende una plataforma de localización SUPL local, H-SLP.

7. El terminal según la reivindicación 6, en el que el procesador está configurado para obtener un acceso autenticado usando al menos uno de un mecanismo de autenticación de cliente alternativo, ACA, certificados de dispositivo y una arquitectura de inicialización genérica, GBA, para autenticar el terminal mediante la H-SLP.

8. El terminal según la reivindicación 6, en el que el procesador está configurado para obtener un acceso autenticado usando un certificado de clave pública para autenticar la H-SLP por medio del terminal.

9. Un aparato para obtener un acceso autorizado a un servidor de localización descubierto, comprendiendo el aparato:

medios para conmutar desde una primera red, que no soporta un acceso autenticado a un servidor de localización local por un terminal, a una segunda red que soporta un acceso autenticado al servidor de localización local por el terminal; medios para obtener un acceso autenticado al servidor de localización local usando la segunda red; medios para obtener una autorización para el servidor de localización descubierto a partir del servidor de localización local;
medios para conmutar desde la segunda red de vuelta a la primera red; y
medios para acceder al servidor de localización descubierto usando la primera red en función de la autorización obtenida del servidor de localización local.

10. El aparato según la reivindicación 9, el terminal según la reivindicación 5 o el procedimiento según la

reivindicación 1, en los que el servidor de localización descubierto comprende una plataforma de localización SUPL descubierta, D-SLP.

11. El aparato según la reivindicación 9, en el que el servidor de localización local comprende una plataforma de localización SUPL local, H-SLP.

12. El aparato según la reivindicación 11, en el que los medios para obtener un acceso autenticado comprenden medios para usar al menos uno de un mecanismo de autenticación de cliente alternativo, ACA, certificados de dispositivo y una arquitectura de inicialización genérica, GBA, para autenticar el terminal mediante la H-SLP.

13. El aparato según la reivindicación 11, en el que los medios para obtener un acceso autenticado comprenden medios para usar un certificado de clave pública para autenticar la H-SLP por medio del terminal.

14. El aparato según la reivindicación 9, el terminal según la reivindicación 5 o el procedimiento según la reivindicación 1, en los que la primera red es una red de área local inalámbrica, WLAN; y/o en los que la segunda red es una red que soporta Evolución a Largo Plazo, LTE, WCDMA, GSM o HRPD cdma2000.

15. Un medio legible por procesador no transitorio que comprende instrucciones legibles por procesador configuradas para hacer que un procesador lleve a cabo el procedimiento según cualquiera de las reivindicaciones 1 a 4, 10 o 14.

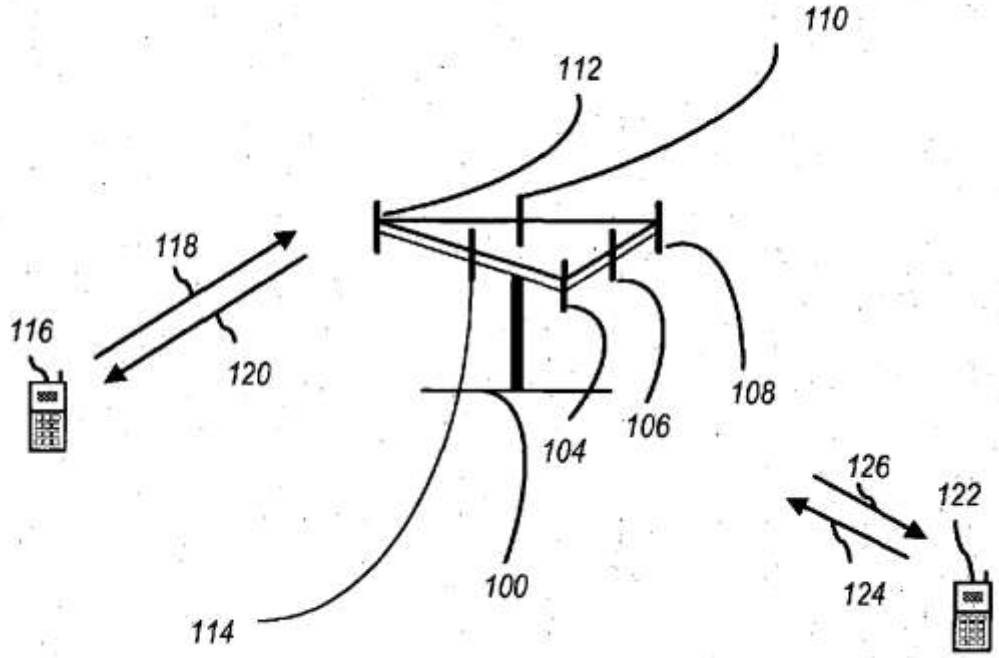

FIG. 1

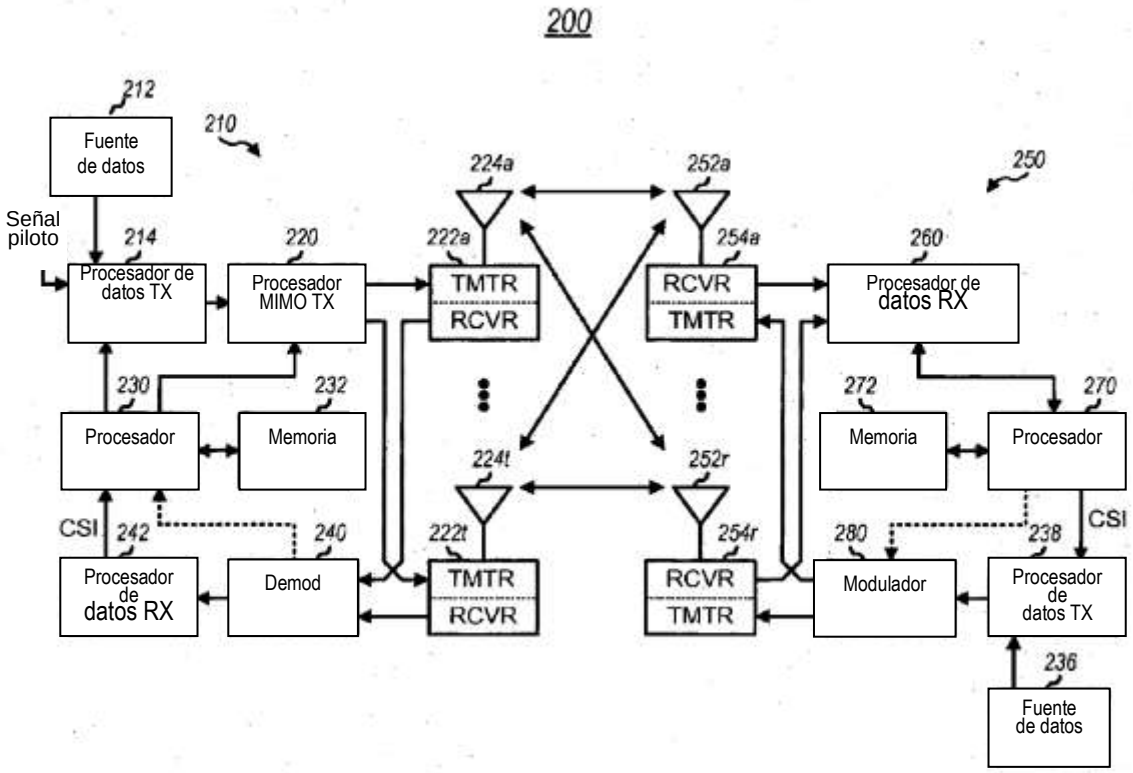
200
212
Fuente de datos
210
224a
252a
250
Señal piloto
214
220
222a
254a
260
Procesador de datos TX
Procesador MIMO TX
TMTR
RCVR
RCVR
TMTR
Procesador de datos RX
230
232
272
270
Procesador
Memoria
Memoria
Procesador
224t
252r
CSI
242
240
222t
254r
280
238
CSI
Procesador de datos RX
Demod
TMTR
RCVR
RCVR
TMTR
Modulador
Procesador de datos TX
236
Fuente de datos

FIG. 2

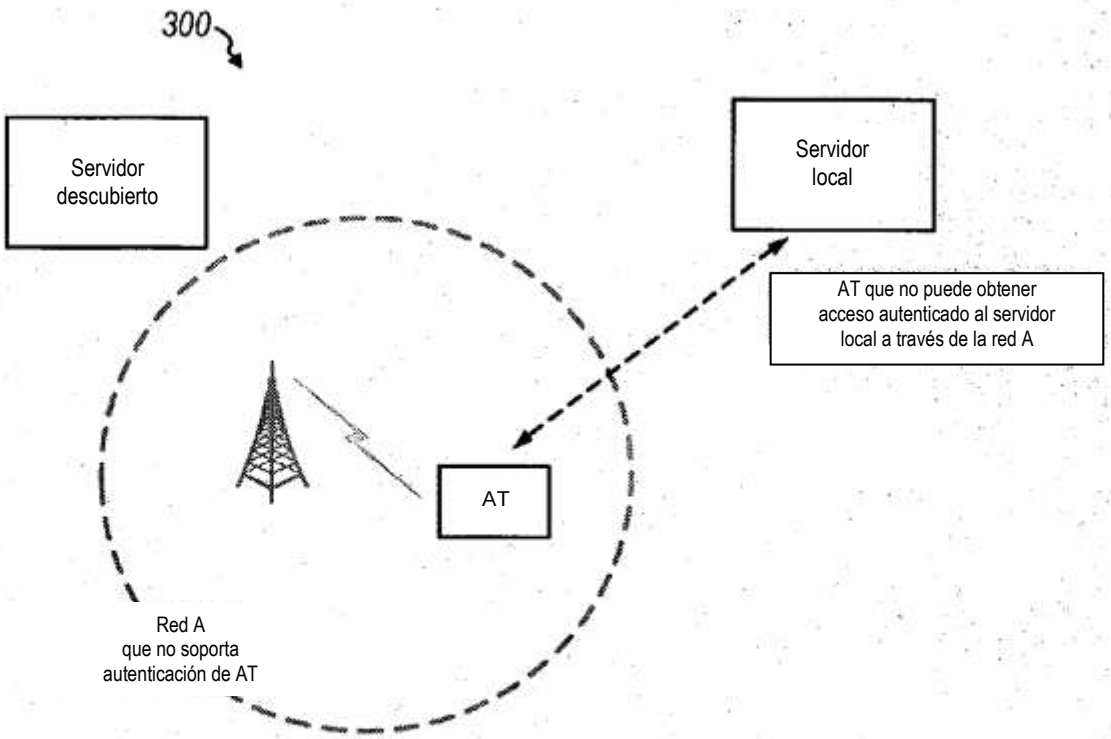
300
Servidor descubierto
Servidor local
AT que no puede obtener acceso autenticado al servidor local a través de la red A
AT
Red A que no soporta autenticación de AT

FIG. 3A

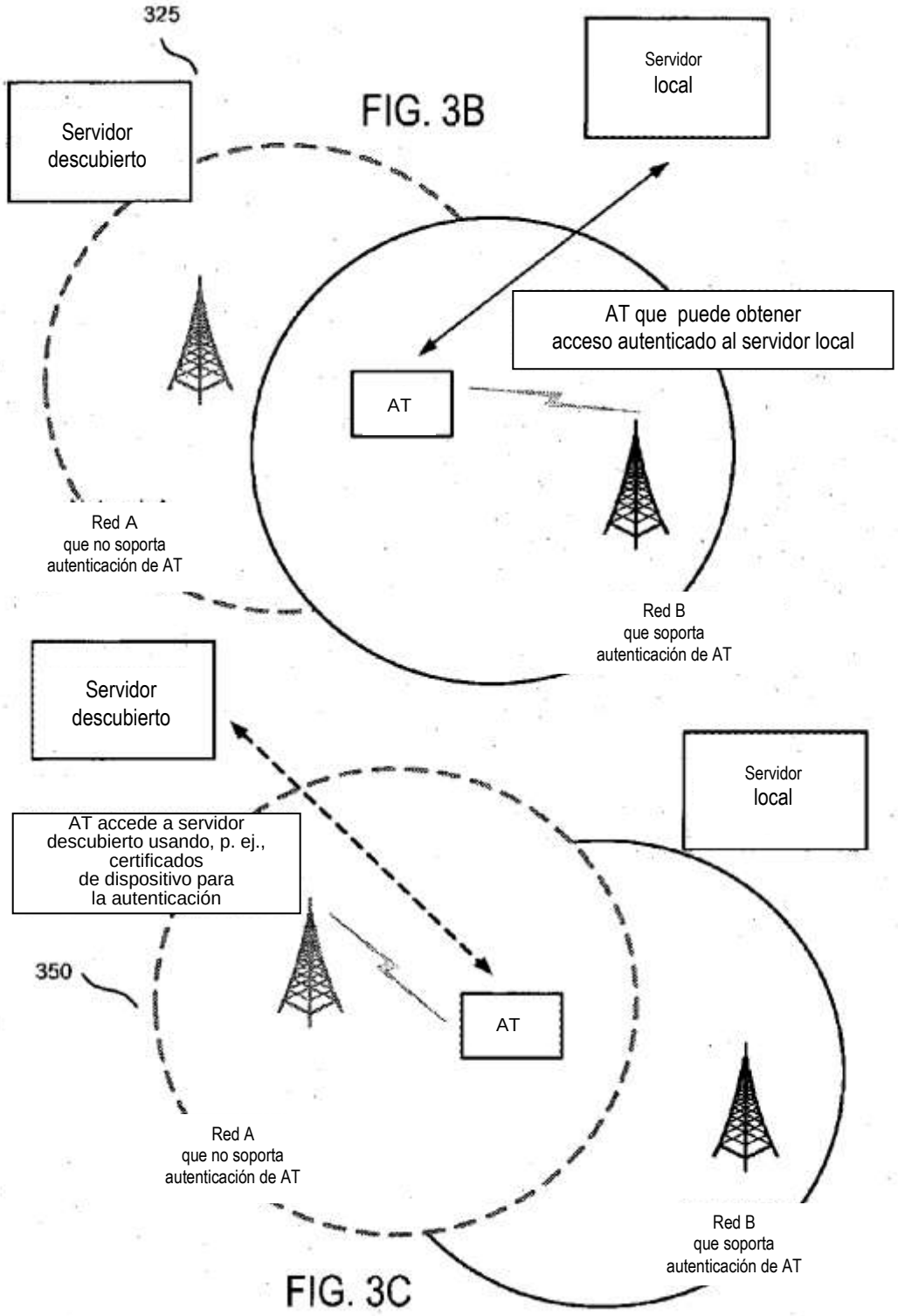
325
Servidor descubierto
Servidor local
AT que puede obtener acceso autenticado al servidor local
AT
Red A que no soporta autenticación de AT
Red B que soporta autenticación de AT

FIG. 3B

Servidor descubierto
Servidor local
AT accede a servidor descubierto usando, p. ej., certificados de dispositivo para la autenticación
350
AT
Red A que no soporta autenticación de AT
Red B que soporta autenticación de AT

FIG. 3C

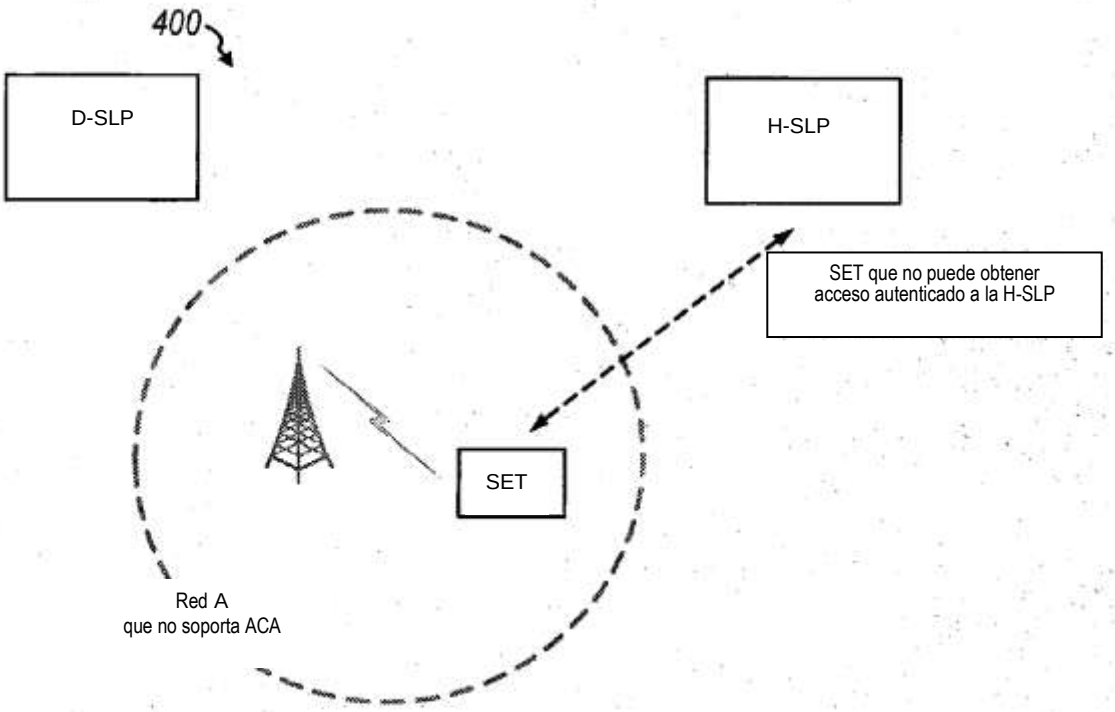
400
D-SLP
H-SLP
SET que no puede obtener
acceso autenticado a la H-SLP
SET
Red A
que no soporta ACA

FIG. 4A

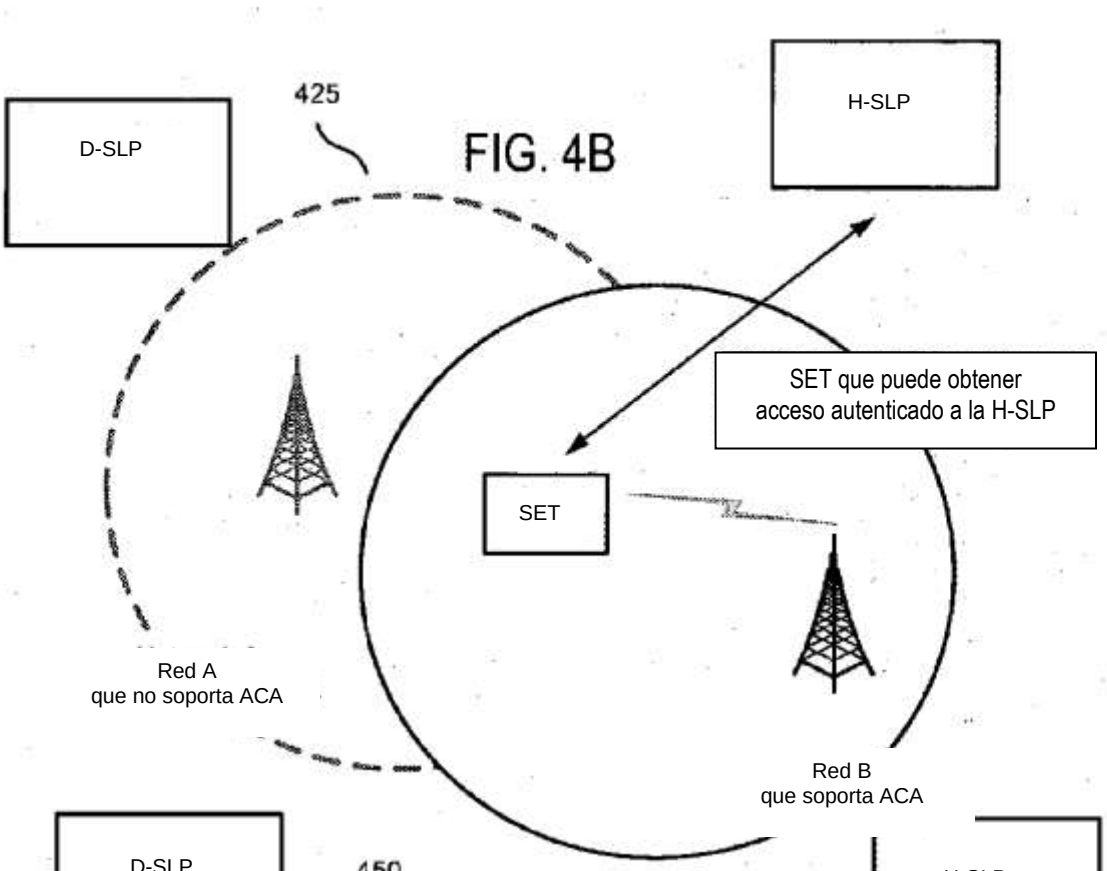
425
D-SLP
H-SLP
SET que puede obtener
acceso autenticado a la H-SLP
SET
Red A
que no soporta ACA
Red B
que soporta ACA

FIG. 4B

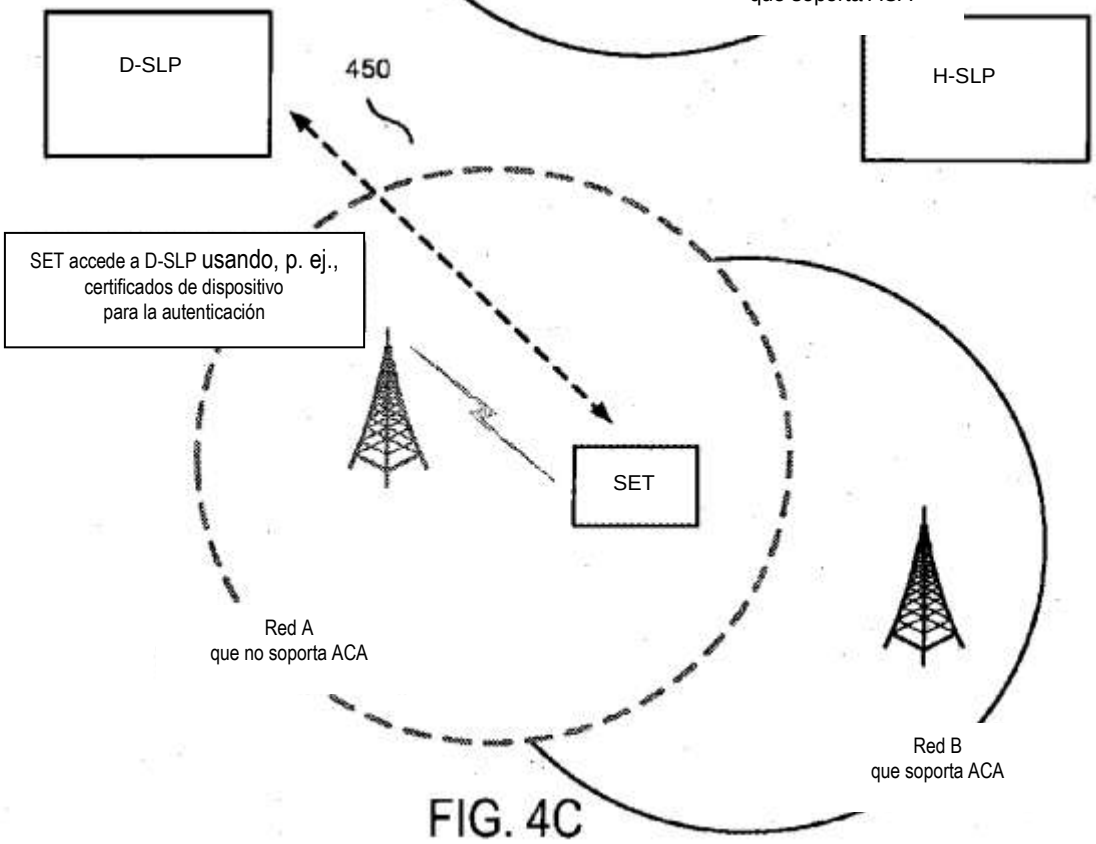
D-SLP
450
H-SLP
SET accede a D-SLP usando, p. ej.,
certificados de dispositivo
para la autenticación
SET
Red A
que no soporta ACA
Red B
que soporta ACA

FIG. 4C

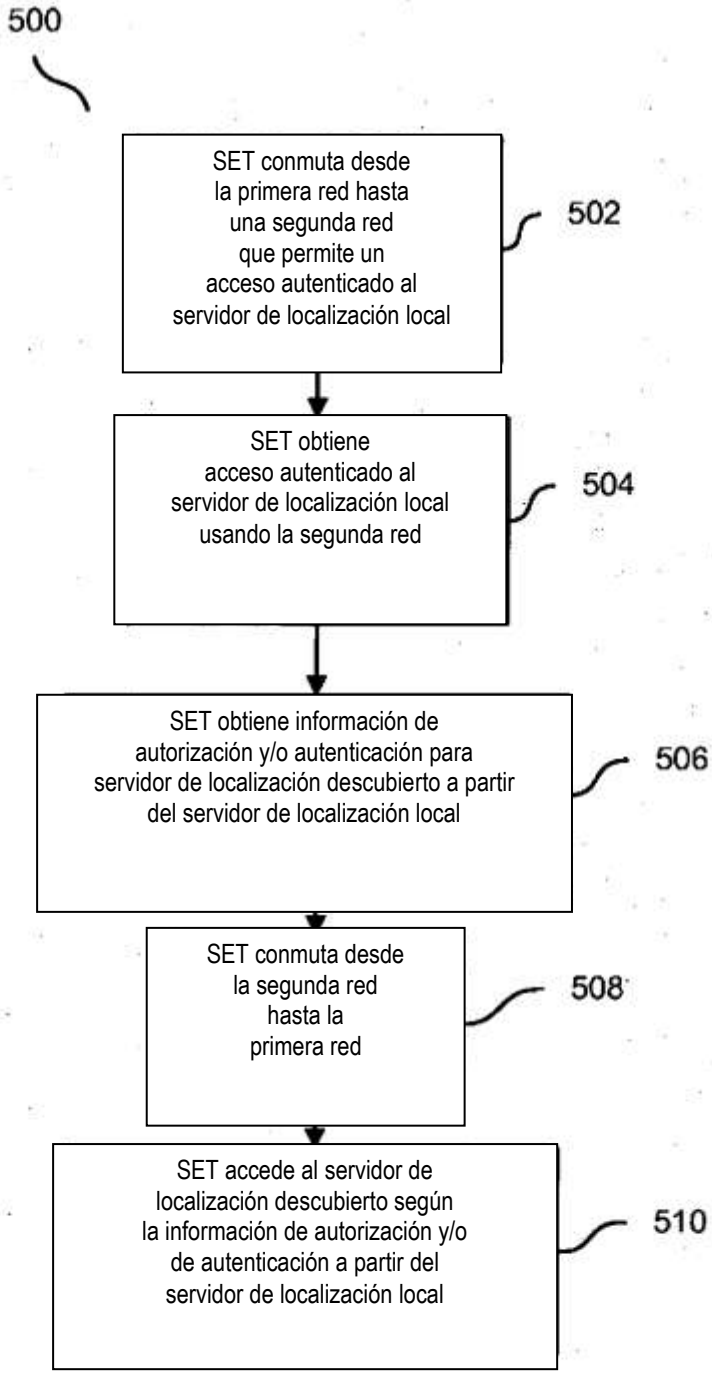
500
SET conmuta desde la primera red hasta una segunda red que permite un acceso autenticado al servidor de localización local
502
SET obtiene acceso autenticado al servidor de localización local usando la segunda red
504
SET obtiene información de autorización y/o autenticación para servidor de localización descubierto a partir del servidor de localización local
506
SET conmuta desde la segunda red hasta la primera red
508
SET accede al servidor de localización descubierto según la información de autorización y/o de autenticación a partir del servidor de localización local
510

FIG. 5A

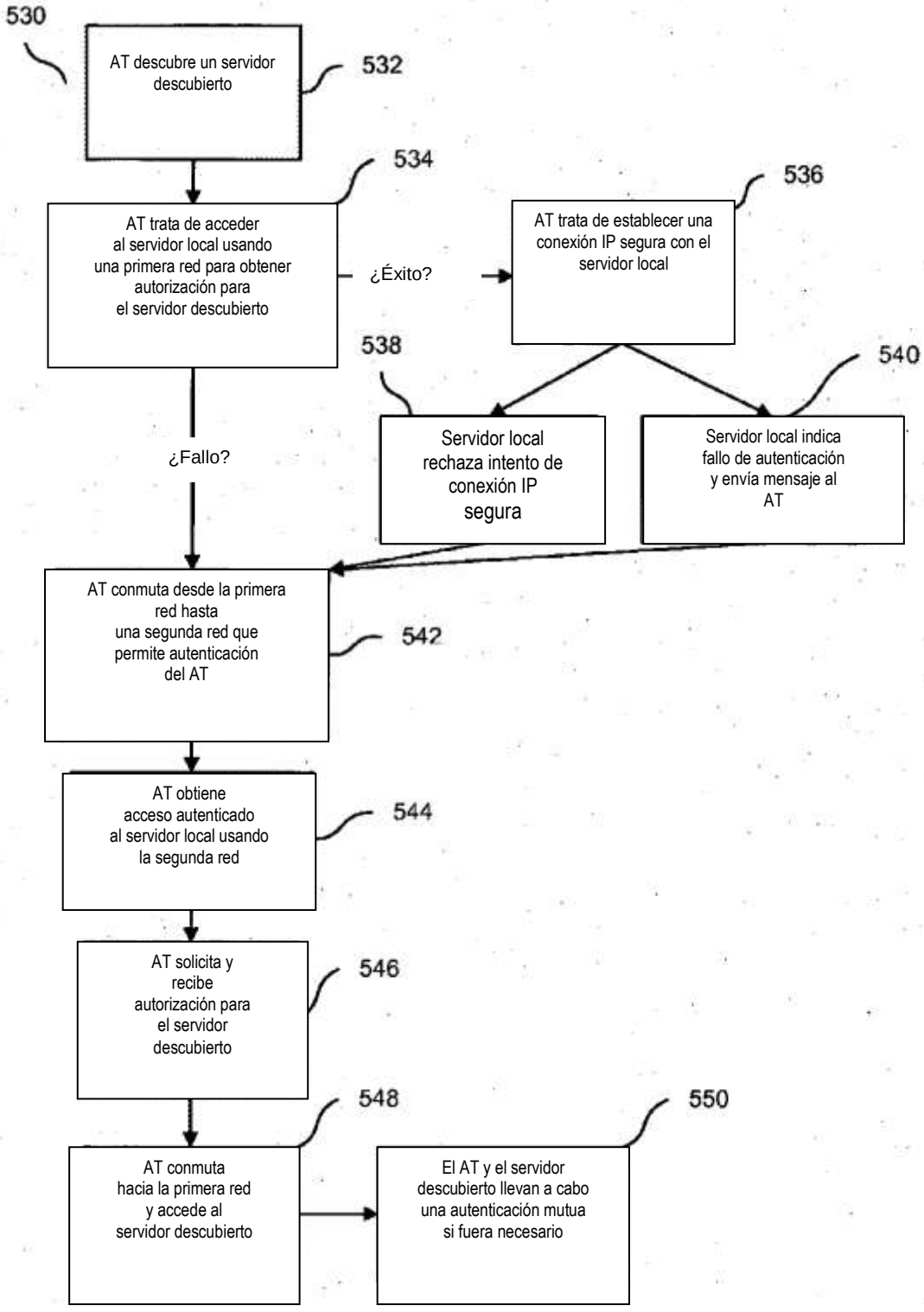
530
AT descubre un servidor descubierto
532
534
AT trata de acceder al servidor local usando una primera red para obtener autorización para el servidor descubierto
¿Éxito?
536
AT trata de establecer una conexión IP segura con el servidor local
538
Servidor local rechaza intento de conexión IP segura
540
Servidor local indica fallo de autenticación y envía mensaje al AT
¿Fallo?
AT conmuta desde la primera red hasta una segunda red que permite autenticación del AT
542
AT obtiene acceso autenticado al servidor local usando la segunda red
544
AT solicita y recibe autorización para el servidor descubierto
546
548
AT conmuta hacia la primera red y accede al servidor descubierto
550
El AT y el servidor descubierto llevan a cabo una autenticación mutua si fuera necesario

FIG. 5B

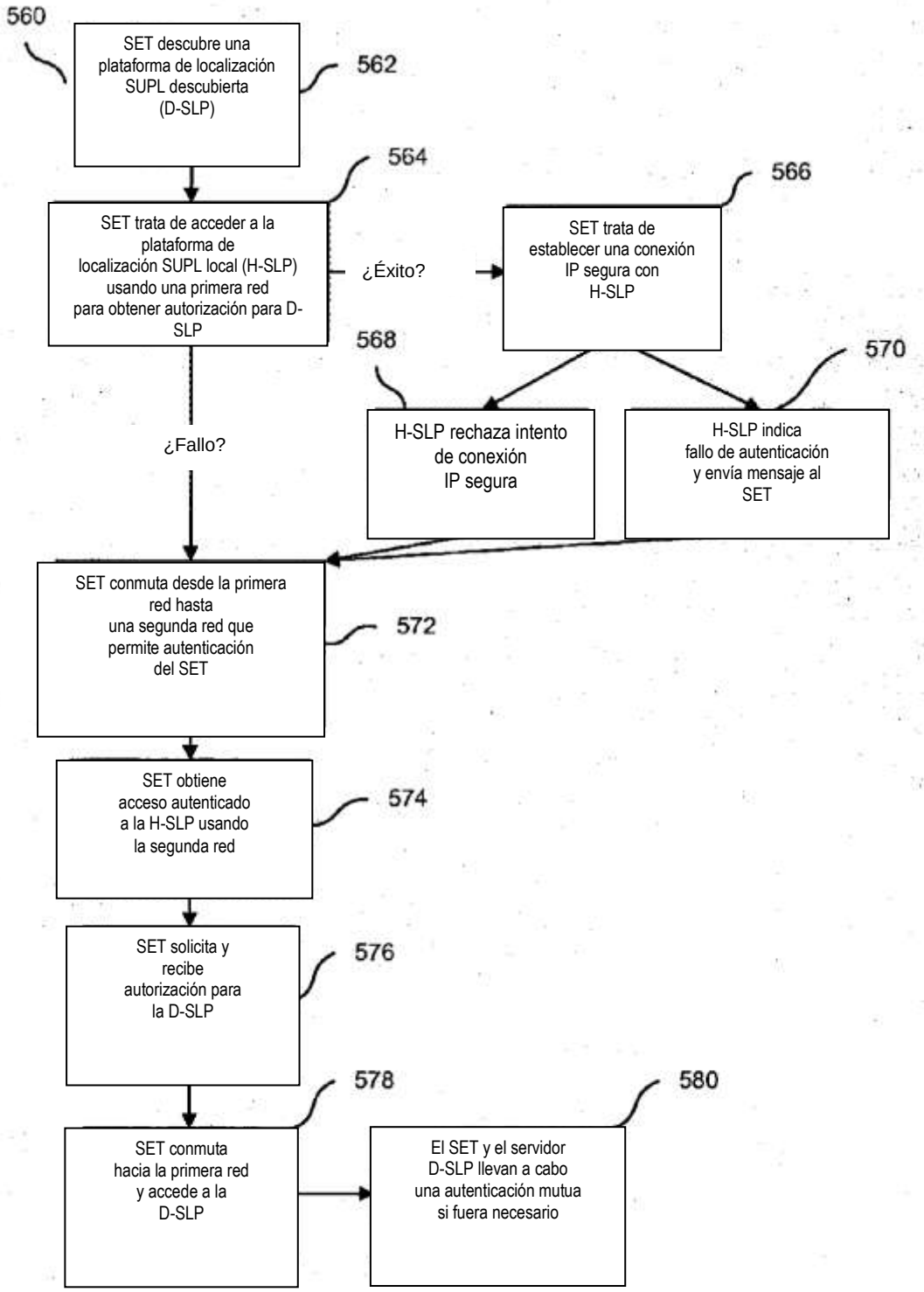
560
SET descubre una plataforma de localización SUPL descubierta (D-SLP)
562
564
SET trata de acceder a la plataforma de localización SUPL local (H-SLP) usando una primera red para obtener autorización para D-SLP
¿Éxito?
566
SET trata de establecer una conexión IP segura con H-SLP
568
H-SLP rechaza intento de conexión IP segura
570
H-SLP indica fallo de autenticación y envía mensaje al SET
¿Fallo?
SET conmuta desde la primera red hasta una segunda red que permite autenticación del SET
572
SET obtiene acceso autenticado a la H-SLP usando la segunda red
574
SET solicita y recibe autorización para la D-SLP
576
578
SET conmuta hacia la primera red y accede a la D-SLP
580
El SET y el servidor D-SLP llevan a cabo una autenticación mutua si fuera necesario

FIG. 5C

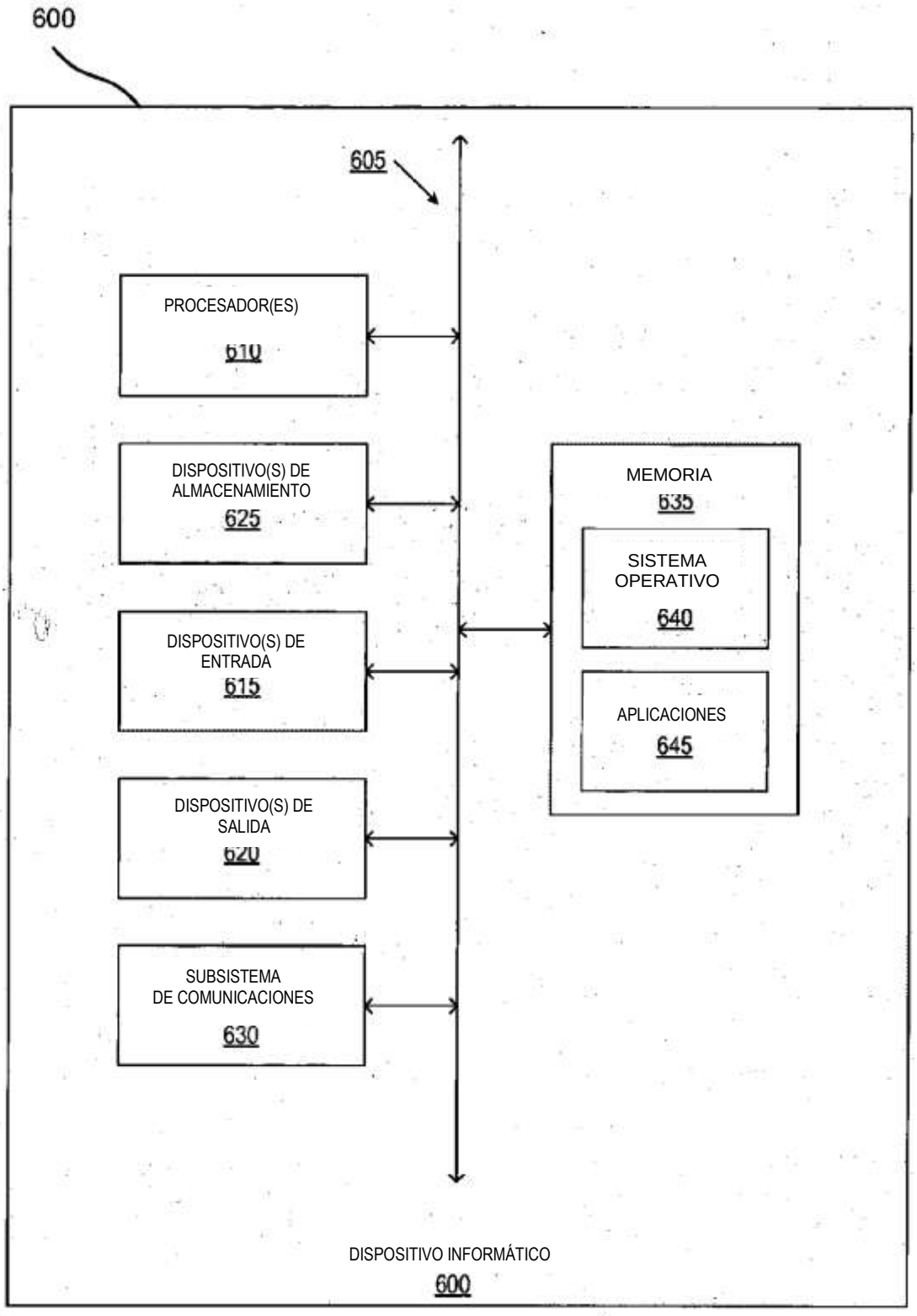
600
605
PROCESADOR(ES)
610
DISPOSITIVO(S) DE ALMACENAMIENTO
625
DISPOSITIVO(S) DE ENTRADA
615
DISPOSITIVO(S) DE SALIDA
620
SUBSISTEMA DE COMUNICACIONES
630
MEMORIA
635
SISTEMA OPERATIVO
640
APLICACIONES
645
DISPOSITIVO INFORMÁTICO
600

FIG 6