

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 607 120**

51 Int. Cl.:

H04W 28/02 (2009.01)

H04W 48/18 (2009.01)

H04W 8/00 (2009.01)

H04W 12/06 (2009.01)

H04W 36/22 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **27.12.2013** **E 13382559 (6)**

97 Fecha y número de publicación de la concesión europea: **14.09.2016** **EP 2890180**

54 Título: **Procedimiento de gestión de una política de usuario para acceder a redes, para descargar tráfico de datos, usando la función de descubrimiento y selección de la red de acceso**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
29.03.2017

73 Titular/es:

TELEFONICA, S.A. (100.0%)
C/ Gran Vía, 28
28013 MADRID, ES

72 Inventor/es:

MATAS SANZ, PRIMITIVO y
FLOREZ RODRIGUEZ, DAVID

74 Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 607 120 T3

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

DESCRIPCIÓN

Procedimiento de gestión de una política de usuario para acceder a redes, para descargar tráfico de datos, usando la función de descubrimiento y selección de la red de acceso

Campo técnico de la invención

- 5 La presente invención se refiere, en general, a la gestión de redes de acceso y, más específicamente, al acceso a redes de Wi-Fi para descargar el tráfico de datos, según políticas pertenecientes a usuarios, en un entorno de la función de descubrimiento y selección de la red de acceso.

Antecedentes de la invención

- 10 Hoy en día, crecientemente complejas y omnipresentes, las redes móviles están dominadas por los flujos de datos. La reciente explosión en el tráfico de datos y de señalización conduce a la impresión de que la clásica arquitectura de red móvil del Proyecto de Colaboración de 3ª Generación (3GPP) no puede afrontar esta sobrecarga de tráfico, fomentando el concepto emergente de “descargar” el tráfico de datos de baja prioridad a otros accesos por radio (es decir, Wi-Fi, Wi-Max) distintos a los del 3GPP puro, de modo que los servicios de primera categoría, tanto de voz como de datos, puedan realizarse óptimamente, evitando la congestión de recursos escasos. Por consiguiente, los Operadores de Red están desplegando pequeñas Células y Puntos de Acceso (AP) de Wi-Fi para facilitar la implementación de este concepto. Este despliegue de equipos es complementado por los Operadores de Red con un buen número de mecanismos y protocolos, ya existentes, usados para realizar la descarga de Wi-Fi. Puede hallarse un ejemplo en el documento US2013/265879.

- 20 La mayoría de los terminales móviles (Equipos de Usuario, UE) están dotados con la capacidad de conectarse con los AP de Wi-Fi estándar, así como de seleccionar cuál usar, entre las opciones disponibles, en base a preferencias, prefijadas o seleccionadas por el usuario, almacenadas en el dispositivo. A fin de ofrecer acceso a Wi-Fi como parte integral de sus soluciones móviles, un Operador de Red necesita poder instalar sus propias políticas de acceso/selección en el UE, y adaptarlas dinámicamente a los cambios ambientales. Para implementar una solución a este problema, el 3GPP desarrolló la serie de estándares de la Función de Descubrimiento y Selección de Red de Acceso (ANDSF) (básicamente, las especificaciones técnicas TS 23.402, TS 24.302 y TS 24.312).

- 30 El procedimiento de ANDSF suministra al UE información acerca de las redes de acceso disponibles, reconocidas como tales por un Operador de Red, que proporcionan conectividad en una cierta área geográfica, así como condiciones de validez y reglas de prioridad a aplicar al seleccionar entre ellas. La ANDSF está básicamente construida en torno a dos entidades básicas mostradas en la figura 1: un servidor (1) de ANDSF, situado en la Red del Operador, que almacena las distintas políticas con respecto al acceso por radio (3GPP, Wi-Fi, Wi-Max); y un cliente de ANDSF instalado en el UE (2) que extrae y aplica las políticas de la ANDSF, decide cuál acceso de red sería el más adecuado en cada circunstancia y envía sucesos al servidor de ANDSF cuando tiene lugar un cambio de entorno.

- 35 La conexión entre el cliente de ANDSF y el servidor será abierta a través de cualquier acceso por radio disponible (3) en el momento, ya sea de 3GPP o no de 3GPP, y, en este último caso, ya sea fiable (conocido y gestionado por el Operador de Red) o no fiable (ni conocido ni gestionado por el Operador de Red).

Al usar información de políticas de ANDSF, el UE puede decidir si, cómo y a qué acceso de red, debería traspasar parte de, o todo, su tráfico entrante/saliente. Este proceso de decisión estará regulado por distintas políticas como, por ejemplo, la disponibilidad y validez del acceso a red, según, por ejemplo, restricciones de ubicación o intervalos de horas/fechas.

- 45 A fin de aplicar el conjunto adecuado de políticas para cada usuario, el servidor de ANDSF debe obtener información acerca de la identidad del UE. Esta identidad no es enviada directamente por el UE, sino que es obtenida desde una tercera entidad. El concepto básico subyacente es que, antes de cualquier diálogo entre el UE y el servidor de ANDSF, ambos deben autenticarse entre sí, a fin de evitar fallos de seguridad por impostura.

- 50 La técnica anterior abarca distintas obras basadas en la ANDSF, por ejemplo, la solicitud de patente US20120122422 A1, “ANDSF, Nodo Distribuidor de Información de Grupos Cerrados de Abonados (CSG)” se refiere a un procedimiento en un nodo de la ANDSF para distribuir información de grupos cerrados de abonados (es decir, disponible solamente para un conjunto restringido de abonados). O bien, la solicitud de patente WO2013029672 “Optimización de la provisión de información de ANDSF

5 *para terminales múltiples de radio*, que también está basada en el estándar ANDSF, y que se refiere a un nuevo dispositivo de red dentro de una red de comunicación, para proveer información de red de acceso a un UE. Otra solución del estado de la técnica (WO2013029672) propone un sistema para generar información de descubrimiento de red de acceso, ANDI, para la transmisión a un Equipo de Usuario, UE, de un abonado de red, por una ANDSF. El documento *“Provisión de ANDSF”* (US 2013/0.165.131) revela un UE proveedor en comunicación con un servidor de ANDSF, a través de una red de acceso que incluye una unidad de interfaz de red del Equipo de Usuario Proveedor (PUE), desde el cual se envía una solicitud de registro al servidor de ANDSF, a través de la red de acceso, y que recibe un resultado de autenticación exitosa y un conjunto de instrucciones de configuración desde el servidor de ANDSF. El documento US2013754648 *“Procedimiento y aparato para seleccionar acceso inalámbrico, usando información de identificación de aplicación, en un sistema de comunicación inalámbrica”* define un procedimiento basado en ANDSF, de modo que un terminal pueda hallar un acceso alternativo por radio en caso de avería / inactividad del acceso primario.

15 Hoy en día, distintos competidores están trabajando en productos relacionados con el estándar ANDSF, con una marcada tendencia en cuanto a cómo hacer que el servidor de ANDSF tome conciencia de las políticas/configuraciones establecidas por otros elementos existentes de red. La característica nueva más extendida es la inclusión de un motor administrador de políticas para permitir una priorización flexible más allá de lo estándar, como la solución *“Descarga Dinámica In-Touch”* de la compañía *“Greenpacket”*, o integraciones con elementos de control estándar en la *“SmartANDSF”* de Interdigital, en el sector del Operador de Red, que, como característica adicional, incluye activadores específicos en el UE para iniciar la función de descubrimiento y selección de manera transparente, seguido por un proceso de autenticación y conexión, sin ninguna interacción, transparente para el usuario.

25 Ha de mencionarse el trabajo en los entornos integrados con otras entidades relacionadas con la gestión y la aplicación de políticas dentro de la red del operador, según lo ofrecido por fabricantes principales de equipos, como Ericsson, Nokia o Tekelec. Incluyen Pasarelas de Wi-Fi para gestionar puntos de acceso a Wi-Fi desde dentro de la Red Central del Operador y el servidor de ANDSF integrado a los elementos de red, para el control de acceso (servidor de AAA o HSS) y la definición de políticas (PCRF).

30 Según lo definido en 3GPP, el estándar ANDSF define un mecanismo para instruir a un UE acerca de cuándo, cómo y en qué orden puede el UE activar un proceso de descarga para un acceso de red disponible. Sin embargo, también exhibe varios inconvenientes importantes. ANDSF es un primer paso firme para abordar la descarga del tráfico móvil del 3GPP a redes de Wi-Fi, por medio de la propagación de políticas de portadora a los UE, pero actualmente frustra las expectativas, debido a que la ANDSF permite solamente *“políticas estáticas”*, y no aborda políticas dinámicas, o en tiempo real, como aquellas que puede proporcionar un servidor de PCRF.

40 El servidor de ANDSF usa el concepto de Fiable y no-Fiable, pero solamente almacena y gestiona políticas de descarga referidas a las redes de Wi-Fi fiables desde el punto de vista del Operador de Red. De ese modo, un usuario no puede definir un conjunto personal de políticas, o incluir, como una opción de acceso a red, los propios AP (Puntos de Acceso) de Wi-Fi fiables del usuario (Wi-Fi doméstica/corporativa, o similar). Adicionalmente, no hay ningún medio para hacer que los AP de la Wi-Fi que un usuario posee o conoce aparezcan en las políticas de ANDSF de otros usuarios, o de invitarlos a conectarse a través de ellos, incluso como invitados.

45 El servidor de ANDSF está definido como un elemento aislado, sin interfaces con otros Elementos de Red. Esto dificulta que un operador de red aplique políticas específicas para cada usuario, según los perfiles de usuario (sin conexión con AAA/HSS o PCRF), especialmente en respuesta a cambios en las condiciones de red (la mayoría de las soluciones de los vendedores, según lo explicado anteriormente, pretenden abordar este problema). Además, las políticas de ANDSF son efectivamente de consulta, por lo que un usuario puede invalidarlas fácilmente y volver a las opciones por defecto de fábrica, o a las preferencias del usuario.

50 El estándar ANDSF no considera la gestión de las credenciales requeridas para conectarse con el AP de Wi-Fi durante la descarga, apoyándose en cambio en conjuntos de credenciales pre-almacenadas en el UE (p. ej., EAP). Dado que esta información debe ser conocida de antemano, puede convertir el procedimiento de descarga en una tarea engorrosa, si el usuario se aventura fuera de sus circuitos normales, o simplemente no recuerda las credenciales.

55 La implicación del usuario final en la definición y gestión de políticas de ANDSF surge como uno de los problemas más importantes referidos a esta tecnología. Básicamente, ANDSF especifica un

procedimiento para indicar al usuario qué puntos de acceso (AP) fiables de Wi-Fi, desde el punto de vista del Operador de Red, están disponibles sobre una cierta área, y cuándo, cómo y por qué debería descargarse el tráfico a esos AP de Wi-Fi. Sin embargo, no especifica ningún procedimiento para implicar al usuario final, aparte de la decisión final sobre permitir la descarga o no. A los usuarios tampoco se les permite definir sus propias políticas en base a los AP fiables de Wi-Fi desde el punto de vista del usuario, como los puntos de acceso de Wi-Fi en entornos domésticos o corporativos. Normalmente, los usuarios medios pasarán la mayoría de sus horas de vigilia en esos dos tipos de ubicaciones, cuyos accesos a redes pueden ser desconocidos para el Operador de Red, y donde el proceso de descarga sería bastante útil, porque son normalmente áreas de baja cobertura de 3GPP, o propensas a la congestión. Por lo tanto, garantizar la implicación del usuario parece ser crucial para el éxito de la ANDSF, porque si no se percibe una mejora en la experiencia del usuario, el usuario podría simplemente inhabilitar la capacidad de descarga de la ANDSF, arriesgando la resolución de problemas de congestión que son el punto principal de este estándar.

En conclusión, ninguna de las soluciones de la técnica anterior permite definir ninguna clase de políticas de propiedad del usuario final, lo que seguramente aumentaría la experiencia y la satisfacción del usuario de ANDSF. Por lo tanto, se requiere una buena cantidad de mejoras para las entidades y protocolos de ANDSF, para abordar la posibilidad de creación, gestión y control de políticas personales de descarga, lo que comportaría un aumento en la satisfacción del usuario y en la Calidad de Experiencia (QoE) percibida.

20 **Sumario de la invención**

La presente invención resuelve los problemas precitados, fomentando la implicación del usuario al admitir la definición de políticas personales de descarga, basadas en los elementos de red que el usuario considere fiables, por ejemplo, el AP de Wi-Fi en casa, o los de entornos corporativos. Por lo tanto, se presenta un procedimiento para gestionar, por parte de un usuario, una política de usuario de acceso (UOP) a red, asociada a un equipo de usuario (UE1) para descargar tráfico de datos, usando la Función de Descubrimiento y Selección de Acceso a Red (ANDSF), en donde uno o más puntos de acceso de Wi-Fi están disponibles para el UE1, estando el UE1 en comunicación con un servidor, a través de una red de comunicaciones móviles. El procedimiento comprende las etapas de:

30 a) enviar, desde el UE1 al servidor, a través de la red de comunicaciones móviles, un primer mensaje que contiene un identificador de un punto de acceso disponible de Wi-Fi;

b) el servidor recibe el primer mensaje y envía un segundo mensaje al UE1, que requiere una descarga de prueba a través del punto de acceso de Wi-Fi;

c) si la descarga de prueba es exitosa, enviar el UE1, usando el punto de acceso de Wi-Fi, un tercer mensaje, que contiene ciertos parámetros, al servidor para fijar una UOP;

35 d) el servidor fija una UOP para descargar tráfico, según dichos ciertos parámetros;

e) el servidor almacena la UOP en un repositorio de UOP;

f) el servidor envía un cuarto mensaje que contiene la UOP al UE1;

g) el usuario de UE1 gestiona la UOP, emprendiendo al menos una de las siguientes acciones: editar la UOP, aplicar la UOP, distribuir la UOP o eliminar la UOP;

40 Adicionalmente, según una realización específica, la etapa de editar la UOP puede comprender adicionalmente las etapas de:

- enviar un mensaje de solicitud, desde el UE1 al servidor, que contiene una solicitud para editar la UOP;

- el servidor recibe el mensaje de edición, y envía al UE1 otro mensaje que contiene la UOP;

45 - editar uno o más parámetros de la UOP en el UE1;

- enviar un mensaje de edición que contiene la UOP editada, desde el UE1 al servidor;

- el servidor almacena la UOP editada en el repositorio de UOP;

- el servidor envía un mensaje de actualización, que contiene la UOP editada, al UE1.

En una realización de la invención, la aplicación de la UOP, a través de un punto de acceso determinado de Wi-Fi, puede comprender adicionalmente:

- enviar el UE1 un mensaje de solicitud al servidor, que contiene un identificador del punto de acceso de Wi-Fi determinado;

5 - buscar, por parte del servidor, en el repositorio de UOP, una UOP asociada al identificador;

- si se halla la UOP, enviar un mensaje de conexión desde el servidor al UE1, que contiene al menos la UOP;

- el UE1 se conecta con el punto de acceso de Wi-Fi, y descarga el contenido según la UOP.

10 La distribución de la UOP a un segundo equipo de usuario (UE2), según una realización específica de la invención, puede comprender adicionalmente:

- enviar un primer mensaje de invitación, desde el UE1 al servidor, que contiene un identificador del UE2, y que indica la UOP a compartir;

- enviar el servidor un segundo mensaje de invitación al UE2 para la UOP compartida por el UE1;

- el UE2 acepta la invitación para compartir la UOP;

15 - el UE2 añade a la UOP como un usuario autorizado;

- el servidor almacena la UOP en el repositorio de UOP;

- el servidor envía un mensaje de actualización, que contiene la UOP, al UE2.

20 Optativamente, una etapa de autorización puede estar comprendida en la presente invención, en la cual el servidor envía a un elemento de gestión de red un mensaje de autorización que contiene al menos uno entre: {el identificador del punto de acceso a Wi-Fi, un identificador del usuario}, para comprobar si están o no admitidos / registrados / autorizados.

Algunas realizaciones de la invención, en las cuales un punto de acceso a Wi-Fi requiere ciertas credenciales, comprenden adicionalmente que el UE1 proporcione dichas credenciales como un parámetro a incluir en la UOP asociada.

25 Una UOP puede comprender, según una realización de la invención, información entre la siguiente lista: lista de usuarios autorizados para acceder a, y gestionar, la UOP, credenciales a usar para acceder a la UOP, tipo de operación admitida para cada usuario, identificador de un punto de acceso a Wi-Fi, credenciales requeridas para conectarse con el punto de acceso a Wi-Fi, ubicación geográfica e intervalos de hora / fecha que definen la validez para la UOP.

30 Una realización de la invención se refiere a decidir, por parte del UE1, cómo y a qué acceso de red traspasar parte de, o todo, el tráfico entrante / saliente del UE1, según la UOP. Este proceso de decisión puede ser regulado por distintas políticas de la siguiente lista:

• Disponibilidad y validez del acceso de red, según, por ejemplo, restricciones de ubicación o intervalos de hora / fecha.

35 • Prioridad del acceso de red en una lista de reglas.

• Si el traspaso ha de ser llevado a cabo para todo el tráfico o solamente para flujos específicos. En este caso, los flujos implicados tienen que ser caracterizados junto con la lista de accesos de red permitidos para ese flujo, que puede o no coincidir con la lista de accesos a la red para uno distinto.

40 • Si el traspaso ha de ser llevado a cabo para todos los Nombres de Puntos de Acceso (APN) o solamente para algunos específicos entre los usados simultáneamente por el UE1.

• Condiciones / sucesos internos en el UE1.

• Características del acceso a red, p. ej., datos de conexión, tecnología de conexión.

45 El identificador usado para los puntos de acceso a Wi-Fi en la UOP puede ser el SSID, el HESSID o un BSSID.

Un punto de acceso a Wi-Fi puede dar soporte a más de un identificador. Según algunas realizaciones específicas, la invención puede comprender adicionalmente la etapa de fijar una UOP para cada identificador del punto de acceso a Wi-Fi, con uno o más parámetros de la siguiente lista: QoS

deseada, límite superior del ancho de banda, servicios de operador disponibles y visibilidad de la red.

Un segundo aspecto de la invención se refiere a un sistema para gestionar, por parte de un usuario, una política de usuario de acceso a red (UOP), asociada a un equipo de usuario (UE1) para descargar tráfico de datos, usando la Función de Descubrimiento y Selección de Red de Acceso (ANDSF), en la cual uno o más puntos de acceso a Wi-Fi están disponibles para el UE1, estando el UE1 en comunicación con un servidor a través de una red de comunicaciones móviles. El sistema comprende:

- el UE1 configurado para: enviar, a través de la red de comunicaciones móviles, mensajes que contienen identificadores de puntos disponibles de acceso a Wi-Fi; enviar, usando el punto de acceso a Wi-Fi, mensajes que contienen ciertos parámetros al servidor para gestionar las UOP, emprendiendo al menos una de las siguientes acciones: aplicar la UOP, editar la UOP, eliminar la UOP o distribuir la UOP;

- un servidor configurado para: recibir mensajes desde el UE1 y enviar mensajes al UE1, requiriendo una descarga de prueba a través de puntos de acceso a Wi-Fi; aplicar, editar, eliminar y distribuir las UOP para descargar tráfico, según dichos ciertos parámetros; y enviar mensajes, que contienen las UOP, al UE1;

- un repositorio de las UOP, en comunicación con el servidor, para almacenar las UOP.

Según una realización de la invención, el UE1 puede ser adicionalmente configurado para enviar un mensaje de solicitud al servidor, que contiene una solicitud para editar la UOP; editar uno o más parámetros de la UOP; y enviar un mensaje de edición que contiene la UOP editada al servidor; y el servidor puede estar adicionalmente configurado para recibir mensajes de edición y enviar al UE1 mensajes que contienen las UOP; y enviar mensajes de actualización que contienen las UOP editadas al UE1.

El sistema de la invención, según algunas realizaciones particulares, puede comprender:

- el UE1 adicionalmente configurado para: enviar un mensaje de solicitud al servidor que contiene un identificador del punto de acceso a Wi-Fi determinado; y conectarse al punto de acceso a Wi-Fi para descargar contenido a través del punto de acceso a Wi-Fi, según la UOP;

- el servidor adicionalmente configurado para: buscar en el repositorio de las UOP una UOP asociada al identificador; y enviar mensajes de conexión al UE1 que contienen al menos la UOP.

El sistema de la invención, según algunas realizaciones particulares en las cuales está comprendido un segundo equipo de usuario (UE2), puede ser adicionalmente configurado para aceptar invitaciones para compartir las UOP, y en el cual:

- el UE1 está adicionalmente configurado para: enviar mensajes de invitación al servidor, que contienen un identificador del UE2 y que indican la UOP a compartir;

- el servidor está adicionalmente configurado para: enviar mensajes de invitación al UE2 para las UOP compartidas por el UE1; añadir el UE2 a la UOP como un usuario autorizado; y enviar mensajes de actualización que contienen las UOP al UE2.

El sistema de la invención, según algunas realizaciones particulares, en las cuales el servidor está adicionalmente configurado para enviar a una red central un mensaje de autorización que contiene al menos uno entre: {el identificador del punto de acceso a Wi-Fi, un identificador del equipo de usuario}, puede comprender adicionalmente un servidor de autorizaciones en la red central, en comunicación con el servidor, configurado para comprobar si el punto de acceso a Wi-Fi y el equipo de usuario están o no admitidos / registrados / autorizados.

En una realización de la invención, el servidor es un servidor de ANDSF.

Un último aspecto de la invención se refiere a un producto de programa de ordenador que comprende código de programa de ordenador adaptado para realizar el procedimiento de la invención cuando dicho código de programa es ejecutado en un ordenador, un procesador de señales digitales, una formación de compuertas programables en campo, un circuito integrado específico de la aplicación, un micro-procesador, un micro-controlador o cualquier otra forma de hardware programable.

Añadiendo el sistema y procedimiento propuestos por la presente invención, los usuarios se implican en la definición de políticas de ANDSF y pueden especificar sus propias configuraciones, y hasta incluir un AP válido de Wi-Fi en el que confían, independientemente de ser o no conocidos por el

Operador de Red. El proceso es por tanto más amigable, aumentando la flexibilidad y la confianza del usuario final.

Desde el punto de vista de un usuario, pueden destacarse las siguientes ventajas:

- 5 • Permitir la creación de UOP para un AP de Wi-Fi de la confianza del usuario (es decir, Wi-Fi doméstico, entorno corporativo, ...).
- Las credenciales del AP de Wi-Fi no son almacenadas en el UE, sino en la nube, habilitando el acceso a ese AP de Wi-Fi desde otros dispositivos, sin que el usuario tenga que configurarlos.
- 10 • Control del usuario de las configuraciones de acceso (Identificador de Wi-Fi, credencial, condiciones de validez), con el operador de red a cargo de la validación de acceso y el almacenamiento en la nube.
- Permitir la definición de grupos de usuarios para conceder acceso a entornos de Wi-Fi doméstico.
- Permitir la definición de listas de usuarios para gestionar, de manera global y única, el acceso de invitados a entornos de Wi-Fi de múltiples usuarios (área corporativa o controlada).
- 15 • Si el AP de Wi-Fi está dotado de múltiples capacidades de SSID, el dueño puede abrir una de ellas para compartición externa (club Wi-Fi, Phonera, ...) y distribuir credenciales / configuraciones a amigos (Wi-Fi doméstico) o usuarios invitados (en entornos corporativos).
- La transferencia de parámetros de conexión y credenciales de seguridad es llevada a cabo por medio del Estándar ANDSF (OMA).

20 Desde el punto de vista del Operador de Red:

- Aumentar el número de posibilidades de redes de descarga, habilitando la inclusión de los AP de Wi-Fi no conocidos por el Operador de Red. La descarga será por tanto facilitada en entornos domésticos y corporativos, con cobertura de 3GPP y / o riesgo de conversión reducidos, y usualmente servida por los AP de Wi-Fi no controlados por el operador, mejorando de ese modo la flexibilidad de la red para una óptima experiencia de descarga del usuario.
- 25 • Permitir el control de QoS haciendo que las Pasarelas del Operador de Red sean conscientes de los AP de Wi-Fi previamente desconocidos.
- Facilita el descubrimiento y el acceso de los Servicios del Operador.
- Mejorar la experiencia y lealtad del usuario (las políticas privadas son almacenadas en el Almacenamiento del Operador de la Red).
- 30 • Integrado con el estándar ANDSF.

Descripción de los dibujos

35 Para completar la descripción que se está haciendo, y con el objeto de ayudar para una mejor comprensión de las características de la invención, de acuerdo a un ejemplo preferido de realización práctica de la misma, acompañando a dicha descripción como una parte integral de la misma, hay un conjunto de dibujos en los cuales, a modo de ilustración y no restrictivamente, ha sido representado lo siguiente:

Figura 1.- muestra un esquema básico de la arquitectura de ANDSF.

40 **Figura 2.-** muestra una configuración y distribución de políticas en un entorno de ANDSF, según una realización de la invención.

Figura 3.- muestra un flujo de creación de políticas según una realización de la invención.

Figura 4.- muestra un flujo de aplicación de políticas según una realización de la invención.

Figura 5.- muestra un flujo de edición de políticas según una realización de la invención.

Figura 6.- muestra un flujo de compartición de políticas según una realización de la invención.

45 **Figura 7.-** muestra un diagrama de una realización de la invención que comparte ancho de banda sobrante.

Figura 8.- muestra una realización particular de la invención que usa ANDSF como herramienta de auto-configuración de los AP de Wi-Fi en un entorno de servicio.

Descripción detallada de la invención

La invención describe un proceso, en términos generales, para fijar, verificar y distribuir Políticas de Propiedad del Usuario (UOP) en un entorno de ANDSF.

5 La Figura 2 ilustra una realización de la invención donde está compuesta por un repositorio de UOP (21) desplegado internamente (o remotamente, según otras realizaciones), un servidor de ANDSF (1), para almacenar las entradas de políticas de descarga de un usuario, que dialoga con un UE (2). Esos elementos son realizados añadiendo un Cliente de UOP (22) al UE, un servidor de UOP (23) al servidor de ANDSF y un repositorio externo de UOP (21) para el almacenamiento de las UOP.

10 Cada entrada de UOP puede consistir en: a) Lista de usuarios autorizados para el acceso a la entrada de UOP, más las operaciones permitidas (es decir, control total de consulta) junto con (optativamente) sus credenciales de gestión de UOP; b) el identificador de la Red de Acceso, usualmente un AP de Wi-Fi, que será usado como un ejemplo principal en la siguiente explicación; c) credenciales requeridas para la conexión con el AP de Wi-Fi; d) ubicación geográfica e intervalos de validez de hora / fecha para la entrada de UOP.

15 En una realización de la invención, el servidor de ANDSF también incluye un servidor de UOP (23), capaz de conectarse al repositorio de UOP, añadir nuevas entradas de UOP, extraer las pertenecientes a, o autorizadas para, un usuario específico, o editar / eliminar las existentes. Este Servidor de UOP también es capaz de conectar Elementos de Gestión de Red (p. ej., un AAA / HSS (24), es decir, un servidor de Autenticación, Autorización y Contabilidad (AAA) o un Servidor de Abonado Doméstico (HSS), para gestionar el abono de los usuarios y su derecho de acceso a los recursos y servicios de la red) para autenticar y validar tanto a usuarios como a los AP de Wi-Fi, si es necesario.

25 La Figura 2 también incluye un cliente de UOP (31) como una mejora del cliente estándar de ANDSF, para aplicar las credenciales necesarias al Servidor de UOP y extraer las entradas de UOP asociadas a este usuario, así como activar la Descarga si se satisfacen las condiciones de validez. Las entradas de UOP son extraídas usando la interfaz S14 definida en el estándar de ANDSF. Adicionalmente, la interfaz S14 también está extendida a fin de verificar la accesibilidad de los AP de Wi-Fi incluidos en las entradas de UOP, y no conocidos aún por el Servidor de ANDSF. Por último, el procedimiento de comunicación estándar usado por la interfaz S14 es extendido en consecuencia para incorporar los trozos de información requeridos por las entradas de UOP.

La comunicación entre el Cliente de UOP y el servidor de UOP se construye sobre el estándar de ANDSF, de modo que se mantengan los niveles de seguridad y la fiabilidad de comunicación garantizados por este protocolo.

35 Toda información de ubicación puede ser expresada como coordenadas geográficas, Identificador celular de célula o Identificador de área, o ubicación de WLAN (HESSID, SSID o BSSID).

En los casos en que un usuario o un AP de Wi-Fi necesita ser validado, la presente invención proporciona realizaciones con una interfaz entre el servidor de UOP y elementos de Autorización, Autenticación y Contabilidad (AAA) desplegados en la red central del Operador de Red.

40 Sobre esta arquitectura, se requieren cinco flujos distintos de comando principal para el proceso total de una realización de la invención:

- Flujo de Inicialización. Este flujo asocia el UE y el servidor de ANDSF a través de un Acceso de Red del 3GPP, valida las credenciales del usuario, extrae las políticas de ANDSF del usuario y concede acceso al repositorio de UOP.
- 45 • Creación de UOP. En este flujo un nuevo AP de Wi-Fi es incluido en el repositorio de UOP. Requiere que la ANDSF esté habilitada en el UE, un enlace abierto al servidor de ANDSF a través de un Acceso de Red del 3GPP y que el nuevo AP de Wi-Fi esté dentro del alcance del UE.
- Edición de UOP. Permite editar la información almacenada en una entrada de UOP. Requiere que la ANDSF esté habilitada en el UE y un enlace abierto al servidor de ANDSF a través de un Acceso de Red del 3GPP.
- 50 • Aplicación de UOP. La UOP es transferida al UE y aplicada allí, probablemente activando una descarga. Requiere que la ANDSF esté habilitada en el UE, un enlace abierto al servidor de ANDSF a través de un Acceso de Red del 3GPP y que el AP de Wi-Fi esté dentro del alcance del UE.
- Compartición de UOP. La UOP es compartida con otro usuario / UE. Requiere la ANDSF habilitada en ambos UE, enlaces abiertos desde ellos al servidor de ANDSF a través de un Acceso de Red del 3GPP y que el AP de Wi-Fi esté al menos dentro del alcance del UE invitado.

En el flujo de inicialización, el UE tiene que seguir el mismo proceso para identificar y validar el acceso usado por un cliente estándar de ANDSF (sesión de TLS o conexión de HTTPS con acceso por identificador de conexión y contraseña). Desde el punto de vista del servidor, el repositorio debe ser consultado a fin de incluir la UOP del usuario (si existe) en la configuración inicial de políticas de ANDSF a enviar al cliente de UOP.

5

La Figura 3 se refiere, según una realización de la invención, al flujo para crear una nueva entrada de UOP, para un AP de Wi-Fi de la confianza del usuario, en el repositorio de UOP y su proceso principal. Comienza con un UE (2) que ha completado con éxito un proceso de inicialización, por lo que se habilita un enlace de comunicación al servidor de ANDSF (1) mediante el acceso a la red del 3GPP. Para la creación y validación de UOP, también requiere que el AP de Wi-Fi (31) esté dentro del alcance del UE, de modo que pueda ser completada una operación de descarga. Después de que el usuario ha reunido los datos referidos a la UOP, a saber, un identificador para el AP de Wi-Fi (AP ID), la ubicación del UE y las credenciales del AP de Wi-Fi, si es necesario, comienza el proceso de creación de UOP, con el envío (33) por el UE del nuevo AP ID (solamente el AP ID) al servidor de ANDSF. La ANDSF comprueba (34) con el AAS / HSS (24) si el AP de Wi-Fi, o el usuario, propuestos están autorizados y/o si están asociados de alguna manera (según el conocimiento del Operador de Red).

10

15

Este proceso de autenticación es un proceso optativo, pero para un Operador de Red global puede ser útil comprobar primero si el AP de Wi-Fi es un AP de Wi-Fi registrado/autorizado/prohibido, conectado con su red central fija. Por el contrario, la ANDSF puede incorporar un repositorio interno con información acerca de los AP de Wi-Fi de usuario de confianza, o autorizados, o no llevar a cabo ninguna autenticación (AP de Wi-Fi abierto definido).

20

Si la comprobación de autenticación es correcta (35), el servidor de ANDSF construye una nueva política temporal de ANDSF para forzar una descarga a través del AP de Wi-Fi sugerido, con prioridad máxima y un breve tiempo de validez, que básicamente es un periodo de expiración, y lo envía al UE (36), activando la descarga al AP de Wi-Fi.

25

Si el UE realiza la descarga y la conexión con el AP de Wi-Fi tiene éxito (37), el enlace con el servidor de ANDSF es reiniciado, pero ahora a través del AP de Wi-Fi. Después de haber abierto la nueva conexión, el UE envía (38) (39) los trozos restantes de datos requeridos para completar la creación y almacenamiento de la UOP: las credenciales del usuario del AP de Wi-Fi, la ubicación del AP de Wi-Fi, o del UE, y los intervalos de validez de tiempo / hora. Luego, el servidor de ANDSF inserta (40) esta información en el repositorio de UOP como una entrada permanente de UOP, la entrada de UOP es reenviada (41) al servidor de ANDSF, que refresca (42) el UE, a través de la pasarela de Wi-Fi (32), con las políticas actualizadas, incluyendo los datos de validez especificados en la entrada de UOP, pero no las credenciales, eliminando de tal modo el periodo de expiración.

30

35

En el caso de que se agotara (43) el periodo de expiración sin que el UE intente la descarga (enlace UE-ANDSF no cerrado) o que fracasara en el intento (enlace UE-ANDSF no reabierto), se descarta el nuevo AP de Wi-Fi y cualquier UOP asociada. Si el enlace desde la ANDSF al UE, a través del Acceso de Red del 3GPP, está aún abierto, se envía (44) una denegación para forzar que el UE descarte las políticas temporales.

40

Según el estándar ANDSF, toda vez que un UE se conecta con un servidor de ANDSF, el servidor envía todas las políticas asociadas al abono del usuario y a la ubicación del UE. A fin de cubrir, ya sea la transferencia de credenciales que permitirían la conexión "sin fisuras" con el AP de Wi-Fi, o bien la extracción de políticas de UOP, el flujo es mejorado para poder adjudicar espacio a estos trozos de información. La Figura 4 ilustra el proceso de una realización de la invención, donde el flujo comienza cuando un UE (2) tiene un enlace entre el UE y el servidor de ANDSF (1) abierto a través de un acceso de red del 3GPP, un AP de Wi-Fi (31) definido en las UOP del usuario está dentro del alcance del UE y las condiciones de validez (hora/ubicación) para el AP de Wi-Fi en la UOP son satisfechas.

45

El UE solicita (45) al servidor de ANDSF consultar (46) el AP de Wi-Fi en el repositorio de UOP (21) y, si lo halla (47) allí, enviar (48) de vuelta tanto el "activador de conexión" (este acceso está colocado al principio de la lista de prioridades) como las credenciales de acceso requeridas, así como cualquier actualización en la información de UOP desde su creación. El UE aplica luego la política de la UOP, realizando (49) una descarga al AP de Wi-Fi.

50

Cuando las restricciones de validez de la UOP para ese AP de Wi-Fi ya no son válidas, el UE inhabilita (50) el Acceso de Red del 3GPP.

55

La Figura 5 ilustra el proceso para editar una UOP según una realización de la invención. Si una conexión está abierta entre el UE (2) y el servidor de ANDSF (1), el proceso del flujo para realizar ediciones a una UOP almacenada en el Repositorio de UOP (21) comienza con una solicitud (51) al servidor de ANDSF para editar la entrada de UOP que almacena un Identificador de AP (31) de Wi-Fi. También requiere al UE dentro del alcance del AP de Wi-Fi comprobar la validez de los cambios, es decir, las credenciales a usar en la conexión del AP de Wi-Fi.

Después de que el servidor de ANDSF comprueba (52) (53) con el servidor AAA/HSS (24) que tanto el usuario como el AP de Wi-Fi están autorizados, envía (54) un mensaje al UE con el contenido de la entrada de UOP asociada.

El UE reúne (55) los cambios en la entrada de UOP y los envía (56) al repositorio de UOP, a través de la conexión descargada a través del AP de Wi-Fi. El servidor de ANDSF valida y guarda (57) la nueva UOP en el repositorio de UOP y actualiza (58) las políticas en el UE.

Si hubiera algún error durante el proceso, el servidor de ANDSF enviaría un mensaje de error.

La Figura 6 ilustra el caso de una compartición de UOP. Dos UE están ahora implicados, uno con permisos de acceso a una entrada de UOP en el repositorio de UOP, y un segundo, con el cual el primer UE desea compartir la UOP original.

El proceso se divide en dos flujos principales: uno para el propietario (UE1 (2)) de la UOP y un segundo para el UE (UE2 (60)) invitado a compartir la política.

El UE1 debe estar inicialmente enlazado con el servidor de ANDSF (1) e iniciar (61) el proceso para conceder derechos de consulta de UOP, sobre la entrada, al UE2. El servidor de ANDSF debería validar (62) (63) en el repositorio de UOP (21) que el UE1 posee esa entrada, y comprobar (64) (65) que tanto el UE2 como el AP de Wi-Fi (31) están registrados / autorizados en el AAA / HSS central. Si todo es correcto, el servidor de ANDSF envía (66) al UE1 un mensaje de "invitación válida a política", informando de que el proceso de invitación está por ser lanzado. Si cualquier parte de este proceso falla, se envía un mensaje de usuario rechazado al UE1. Después de una validación exitosa del UE2 en el AAA/HSS Central, el servidor de ANDSF envía (67) al UE2 un mensaje de "invitación a política" para la entrada de UOP compartida por el UE1. Si el UE2 acepta (68) la invitación, el nuevo usuario es añadido (69) (70) a la lista de usuarios de UOP del UE1, como un usuario con derechos de consulta para este UOP, y se envía (70) una actualización de políticas al UE2. Cuando las condiciones de validez establecidas en la UOP son satisfechas (política de ubicación o de hora), el UE puede solicitar al servidor de ANDSF las credenciales de acceso del AP de Wi-Fi, a fin de realizar la descarga (71).

Una realización particular de la invención cubre el caso de añadir un AP de Wi-Fi doméstico del usuario al repositorio de políticas de ANDSF. Según esta realización, el usuario añade una entrada de UOP para el AP de Wi-Fi doméstico del usuario y define qué otros usuarios (p. ej., miembros de la familia, amigos) pueden consultar y extraer el UOP y descargar su tráfico al AP de Wi-Fi doméstico. Además, un Operador de Red puede comprobar si este AP de Wi-Fi está gestionado por su sistema central, de modo que puedan estar disponibles sobre él características mejoradas, como el acceso a servicios de abonado ofrecidos por este Operador de Red.

A fin de validar tanto el usuario como el AP de Wi-Fi, el nodo de ANDSF necesita verificar que existe una conexión válida entre el AP de Wi-Fi y la red Central, por medio de un enlace con el servidor de ANDSF, abierto mediante el AP de Wi-Fi, y también comprobar la autenticación y autorización de usuarios con los sistemas del operador, si es necesario.

La información de UOP puede ser refinada añadiendo información de ubicación (de modo que la descarga sea llevada a cabo solamente cuando los UE de confianza estén realmente en la vecindad del AP de Wi-Fi) y restricciones temporales (de modo que sea válida solamente cuando se espera que el usuario esté en casa). La asignación de la máxima prioridad a este AP de Wi-Fi forzaría una descarga automática una vez que el usuario llegue a casa, mejorando su QoE (mayor Ancho de Banda) y ayudando a reducir la carga para las células del 3GPP afectadas en el área.

Al ser consciente de la conexión del AP de Wi-Fi con la Red Central, el operador podría aplicar políticas específicas del usuario sobre el AP de Wi-Fi (es decir, servicios de abonado) y estrategias específicas de tarifa / cargo.

Otra ventaja de esta realización es la posibilidad de añadir nuevos usuarios como invitados, sin necesidad de decirles explícitamente cuál es el Identificador del AP de Wi-Fi, o qué credenciales son necesarias, dado que estos fragmentos de información ya están almacenados en la nube (en el

repositorio de UOP del servidor de ANDSF).

La Figura 7 representa una realización particular del uso de capacidades de Múltiples SSID para compartir el ancho de banda sobrante.

5 Según esta realización, un AP de Wi-Fi privado puede ser integrado en un grupo de Wi-Fi públicos compartidos, en el caso de que el AP de Wi-Fi preste soporte a múltiples definiciones de SSID. Esta realización también hace uso de una conexión desde el AP de Wi-Fi a una Pasarela (Gateway) de Wi-Fi del Operador de Red, que es capaz de definir y planificar características específicas para cada nodo de Wi-Fi.

10 El dueño del AP de Wi-Fi tiene que configurarlo con 2 identificadores distintos (por ejemplo, PSSID1 y PSSID2) y almacenar ambos Identificadores de Wi-Fi en un servidor de ANDSF, como UOP distintas. En este caso, recurriendo a la Pasarela de Wi-Fi en la Red Central, pueden aplicarse distintas políticas de red para cada Identificador de Wi-Fi, como la QoS deseada, el límite superior de Ancho de Banda, los servicios de operador disponibles o la visibilidad de la red. En la Figura 8, el PSSID2 es el principal acceso con un mayor ancho de banda y privilegios de acceso, mientras que PSSID1 es la parte sobrante, con ancho de banda mínimo con fines de compartición, y sin acceso a servicios de abonado ni visibilidad avanzada de la red.

15 Para incluir el AP de Wi-Fi en un entorno compartido, el dueño solamente necesita definir una entrada de UOP con el SSID y el usuario/contraseña genéricos a usar por parte del grupo de usuarios pretendido. Por lo que, cuando un miembro del grupo, con la ANDSF habilitada en el UE, está en la vecindad del AP de Wi-Fi, recibirá toda la información de conexión requerida (por ejemplo, el SSID y las credenciales), y procederá automáticamente a descargar al AP de Wi-Fi.

20 En entornos corporativos, esta realización tiene claras ventajas, dado que el administrador del AP de Wi-Fi puede definir fácilmente invitaciones a huéspedes para un SSID con menor prioridad y menos privilegios que el tronco principal para el acceso corporativo, de modo que los visitantes puedan usar automáticamente el procedimiento de descarga dentro del área de cobertura corporativa para conectarse con el Wi-Fi de invitados. El administrador de Wi-Fi del sistema, como dueño de la entrada de UOP de esas políticas, puede invitar fácilmente a los visitantes al Wi-Fi de invitados, siguiendo los procedimientos definidos en esta invención.

25 La Figura 8 representa una realización particular de la invención, usando ANDSF como herramienta de auto-configuración de AP de Wi-Fi en un entorno de servicio.

30 Según esta realización, allí donde el procedimiento normal para definir una entrada de UOP implica la validación del usuario (2) y del AP de Wi-Fi (31) ante el Operador de Red, la ANDSF (1) alerta a los elementos de red (24) (p. ej., HSS / PCRF) sobre la existencia de un AP de Wi-Fi recién instalado (31), y activa un proceso de auto-configuración de ese AP de Wi-Fi, prevaleciendo sobre las configuraciones de fábrica, con configuraciones de operador según los servicios abonados/habilitados para la ubicación del AP de Wi-Fi.

35 Hay una ventaja básica que se deriva de este procedimiento: no requiere la intervención del equipo de soporte de la red, ya sea remotamente o en el hogar del usuario. Sencillamente, las validaciones llevadas a cabo por la ANDSF son suficientes para hallar los detalles del abono del usuario y aplicarlos según se requiera.

40 Este documento usa a menudo los términos “usuario” y “equipo de usuario” sin ninguna distinción, dado que se entiende el equipo de usuario (UE) como cualquier dispositivo usado directamente por el usuario para comunicarse. Puede ser un teléfono móvil, un teléfono inteligente, un ordenador portátil equipado con un adaptador de banda ancha móvil, o cualquier otro dispositivo similar.

45

REIVINDICACIONES

- 5 1.- Procedimiento de gestión, por parte de un usuario, de una política de usuario de acceso a red (UOP) asociada a un equipo de usuario (UE1), para descargar tráfico de datos, usando la Función de Descubrimiento y Selección de Red de Acceso (ANDSF), en el cual uno o más puntos de acceso de Wi-Fi están disponibles para el UE1, estando el UE1 en comunicación con un servidor a través de una red de comunicaciones móviles; el procedimiento está **caracterizado por** comprender las siguientes etapas:
- a) enviar desde el UE1 (2) al servidor (1, 23), a través de la red de comunicaciones móviles, un primer mensaje (33) que contiene un identificador de un punto de acceso de Wi-Fi (31) disponible;
- 10 b) el servidor recibe el primer mensaje y envía un segundo mensaje (36) al UE1, solicitando una descarga de prueba a través del punto de acceso de Wi-Fi:
- c) si la descarga de prueba es exitosa, el UE1 envía, usando el punto de acceso de Wi-Fi, un tercer mensaje (38, 39) que contiene ciertos parámetros al servidor, para configurar una UOP;
- d) el servidor configura una UOP para descargar tráfico según dichos ciertos parámetros;
- 15 e) el servidor (40) almacena la UOP en un repositorio de UOP;
- f) el servidor envía un cuarto mensaje (42) que contiene la UOP al UE1.
- g) el usuario del UE1 gestiona la UOP, emprendiendo al menos una de las siguientes acciones: aplicar la UOP, editar la UOP, eliminar la UOP o distribuir la UOP.
- 20 2.- Procedimiento según la reivindicación 1, en el cual la edición de la UOP comprende adicionalmente:
- enviar un mensaje de solicitud, desde el UE1 al servidor, que contiene una solicitud para editar la UOP;
- el servidor recibe el mensaje de edición y envía al UE1 otro mensaje que contiene la UOP;
- editar uno o más parámetros de la UOP en el UE1;
- 25 - enviar un mensaje de edición que contiene la UOP editada, desde el UE1 al servidor;
- el servidor almacena la UOP editada en el repositorio de UOP;
- el servidor envía un mensaje de actualización que contiene la UOP editada al UE1.
- 3.- Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual la aplicación de la UOP a través de un punto de acceso determinado de Wi-Fi comprende adicionalmente:
- 30 - el UE1 envía un mensaje de solicitud al servidor, que contiene un identificador del punto de acceso determinado de Wi-Fi;
- buscar, por parte del servidor, en el repositorio de UOP, una UOP asociada al identificador;
- si se halla la UOP, enviar un mensaje de conexión desde el servidor al UE1, que contiene al menos la UOP;
- 35 - el UE1 se conecta con el punto de acceso de Wi-Fi y descarga el contenido según la UOP.
- 4.- Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual la distribución de la UOP a un segundo equipo de usuario (UE2) comprende adicionalmente:
- enviar un primer mensaje de invitación, desde el UE1 al servidor, que contiene un identificador del UE2 y que indica la UOP a compartir;
- 40 - el servidor envía un segundo mensaje de invitación al UE2 para la UOP compartida por el UE1;
- el UE2 acepta la invitación para compartir la UOP;
- añadir el UE2 a la UOP como un usuario autorizado

- el servidor almacena la UOP en el repositorio de UOP;

- el servidor envía un mensaje de actualización, que contiene la UOP, al UE2.

5 **5.-** Procedimiento según cualquiera de las reivindicaciones anteriores, que comprende adicionalmente una etapa de autorización, en el cual el servidor envía a un elemento de gestión de red un mensaje de autorización que contiene al menos uno entre: {el identificador del punto de acceso de Wi-Fi, un identificador del usuario}, para comprobar si están admitidos / registrados / autorizados.

6.- Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual un punto de acceso de Wi-Fi requiere ciertas credenciales, comprendiendo adicionalmente que el UE1 proporcione dichas credenciales como un parámetro a incluir en la UOP asociada.

10 **7.-** Procedimiento según cualquiera de las reivindicaciones anteriores, en el cual una UOP comprende información de la siguiente lista: lista de usuarios autorizados para acceder y gestionar la UOP, credenciales a usar para acceder a la UOP, tipo de operación autorizada para cada usuario, identificador de un punto de acceso de Wi-Fi, credenciales requeridas para conectarse al punto de acceso de Wi-Fi, ubicación geográfica e intervalos de hora / fecha que definen una validez para la UOP.

8.- Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual el identificador del punto de acceso de Wi-Fi en la UOP es un SSID, un HESSID o un BSSID.

20 **9.-** Procedimiento según cualquiera de las reivindicaciones precedentes, en el cual un punto de acceso de Wi-Fi da soporte a más de un identificador, que comprende adicionalmente fijar una UOP para cada identificador del punto de acceso de Wi-Fi con uno o más parámetros de la siguiente lista: QoS deseada, límite superior del ancho de banda, servicios de operador disponibles y visibilidad de red.

25 **10.-** Sistema de gestión, por parte de un usuario, de una política de usuario de acceso a red (UOP) asociada a un equipo de usuario (UE1) para descargar tráfico de datos, usando la Función de Descubrimiento y Selección de Red de Acceso (ANDSF), en el cual uno o más puntos de acceso de Wi-Fi están disponibles para el UE1, estando el UE1 en comunicación con un servidor a través de una red de comunicaciones móviles; el sistema está **caracterizado por** comprender:

30 - el UE1 configurado para: enviar, a través de la red de comunicaciones móviles, mensajes que contienen identificadores de los puntos de acceso de Wi-Fi disponibles; enviar, usando el punto de acceso de Wi-Fi, mensajes que contienen ciertos parámetros al servidor, para gestionar las UOP emprendiendo al menos una de las siguientes acciones: aplicar la UOP, editar la UOP, eliminar la UOP o distribuir la UOP;

35 - un servidor configurado para: recibir mensajes desde el UE1 y enviar mensajes al UE1, requiriendo una descarga de prueba a través de puntos de acceso de Wi-Fi; aplicar, editar, eliminar y distribuir las UOP para descargar tráfico, según dichos ciertos parámetros; y enviar mensajes que contienen las UOP al UE1;

- un repositorio de UOP en comunicación con el servidor para almacenar las UOP.

11.- Sistema según la reivindicación 10, en el cual:

40 - el UE1 está adicionalmente configurado para: enviar un mensaje de solicitud al servidor, que contiene una solicitud para editar la UOP; editar uno o más parámetros de la UOP; y enviar un mensaje de edición que contiene la UOP editada al servidor;

- y el servidor está adicionalmente configurado para: recibir mensajes de edición y enviar al UE1 mensajes que contienen las UOP; y enviar mensajes de actualización que contienen las UOP editadas al UE1.

45 **12.-** Sistema según una cualquiera de las reivindicaciones precedentes 10, 11, en el cual:

- el UE1 está adicionalmente configurado para: enviar un mensaje de solicitud al servidor, que contiene un identificador del punto de acceso de Wi-Fi determinado; y conectarse con el punto de acceso de Wi-Fi para descargar contenido a través del punto de acceso de Wi-Fi, según la UOP;

50 - el servidor está adicionalmente configurado para: buscar en el repositorio de UOP una UOP asociada al identificador; y enviar mensajes de conexión al UE1 que contienen al menos la UOP.

13.- Sistema según una cualquiera de las reivindicaciones precedentes 10, 12, que comprende adicionalmente un segundo equipo de usuario (UE2) configurado para aceptar invitaciones para compartir las UOP, y en el cual:

5 - el UE1 está adicionalmente configurado para: enviar mensajes de invitación al servidor, que contienen un identificador del UE2 y que indican la UOP a compartir

- el servidor está adicionalmente configurado para: enviar mensajes de invitación al UE2 para las UOP compartidas por el UE1; añadir el UE2 a la UOP como un usuario autorizado; y enviar mensajes de actualización que contienen las UOP al UE2.

10 **14.-** Sistema según una cualquiera de las reivindicaciones precedentes 10, 13, en el cual el servidor está adicionalmente configurado para enviar a una red central un mensaje de autorización que contiene al menos uno entre: {el identificador del punto de acceso de Wi-Fi, un identificador del equipo de usuario}, que comprende adicionalmente un servidor de autorización en la red central, en comunicación con el servidor, configurado para comprobar si el punto de acceso de Wi-Fi y el equipo de usuario están admitidos / registrados / autorizados.

15 **15.-** Un producto de programa de ordenador que comprende código de programa de ordenador adaptado para realizar el procedimiento según cualquiera de las reivindicaciones 1 a 9 cuando dicho código de programa es ejecutado en un ordenador, un procesador de señales digitales, una formación de compuertas programables en campo, un circuito integrado específico de la aplicación, un micro-procesador, un micro-controlador o cualquier otra forma de hardware programable.

20



FIG. 1

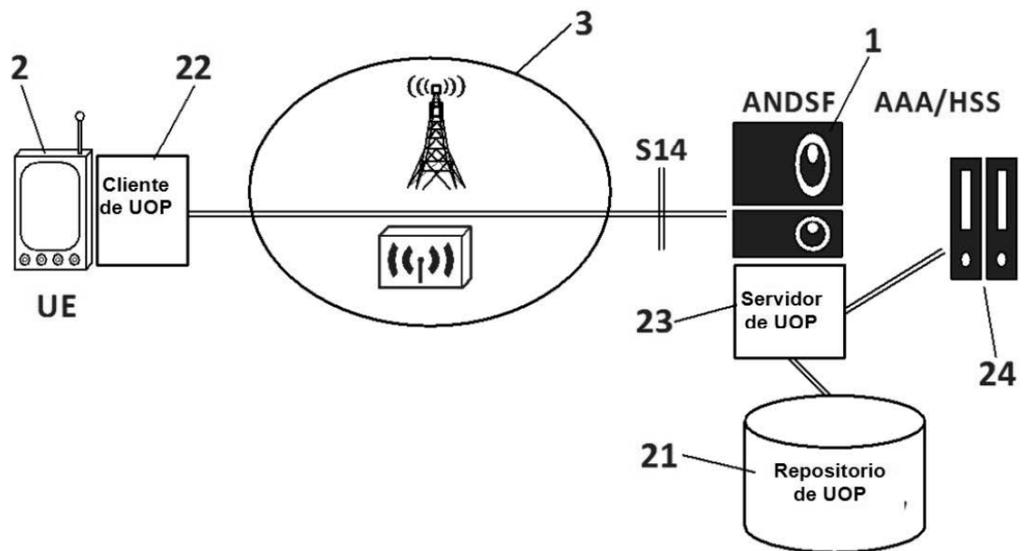


FIG. 2

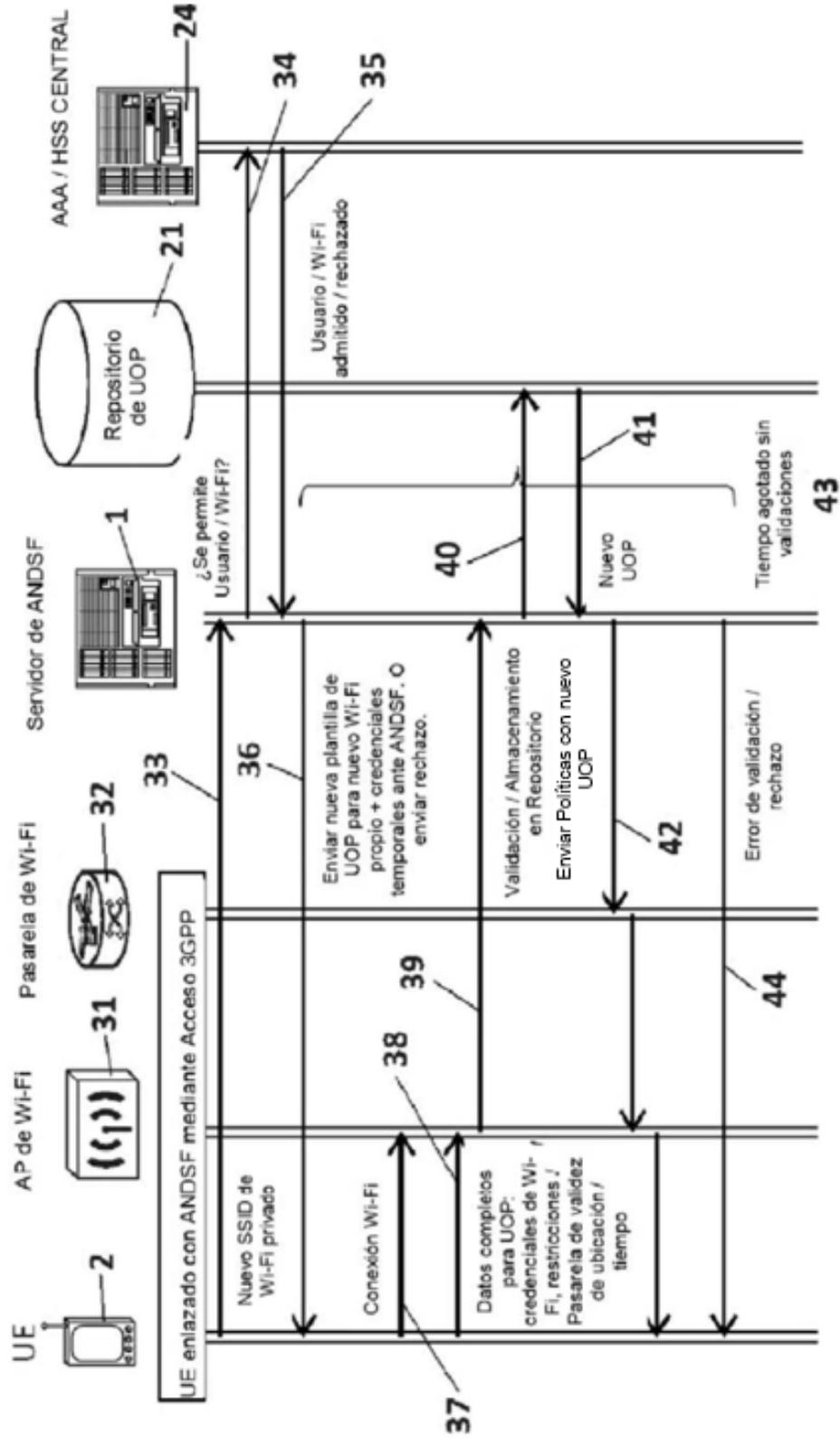


FIG. 3

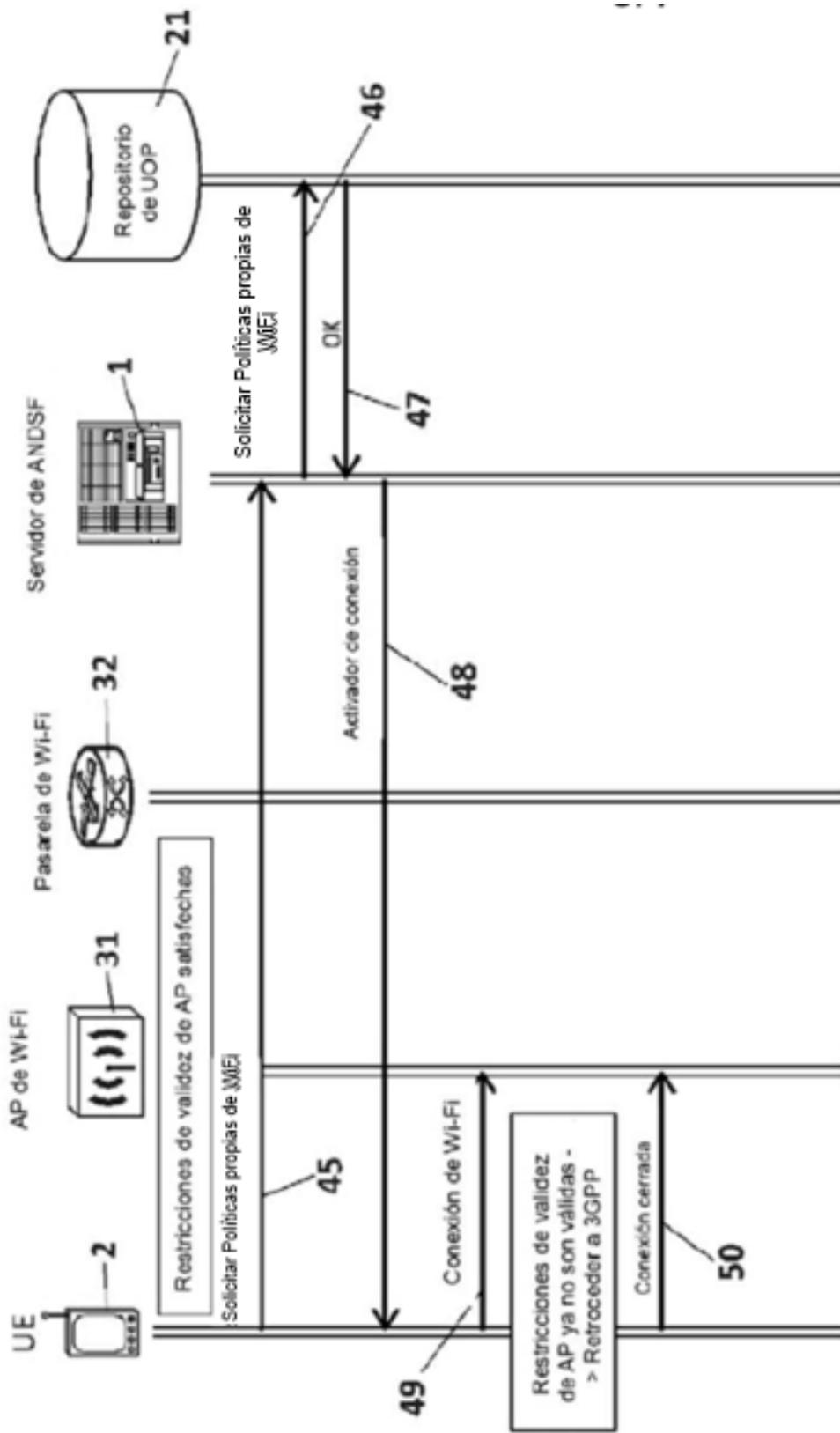


FIG. 4

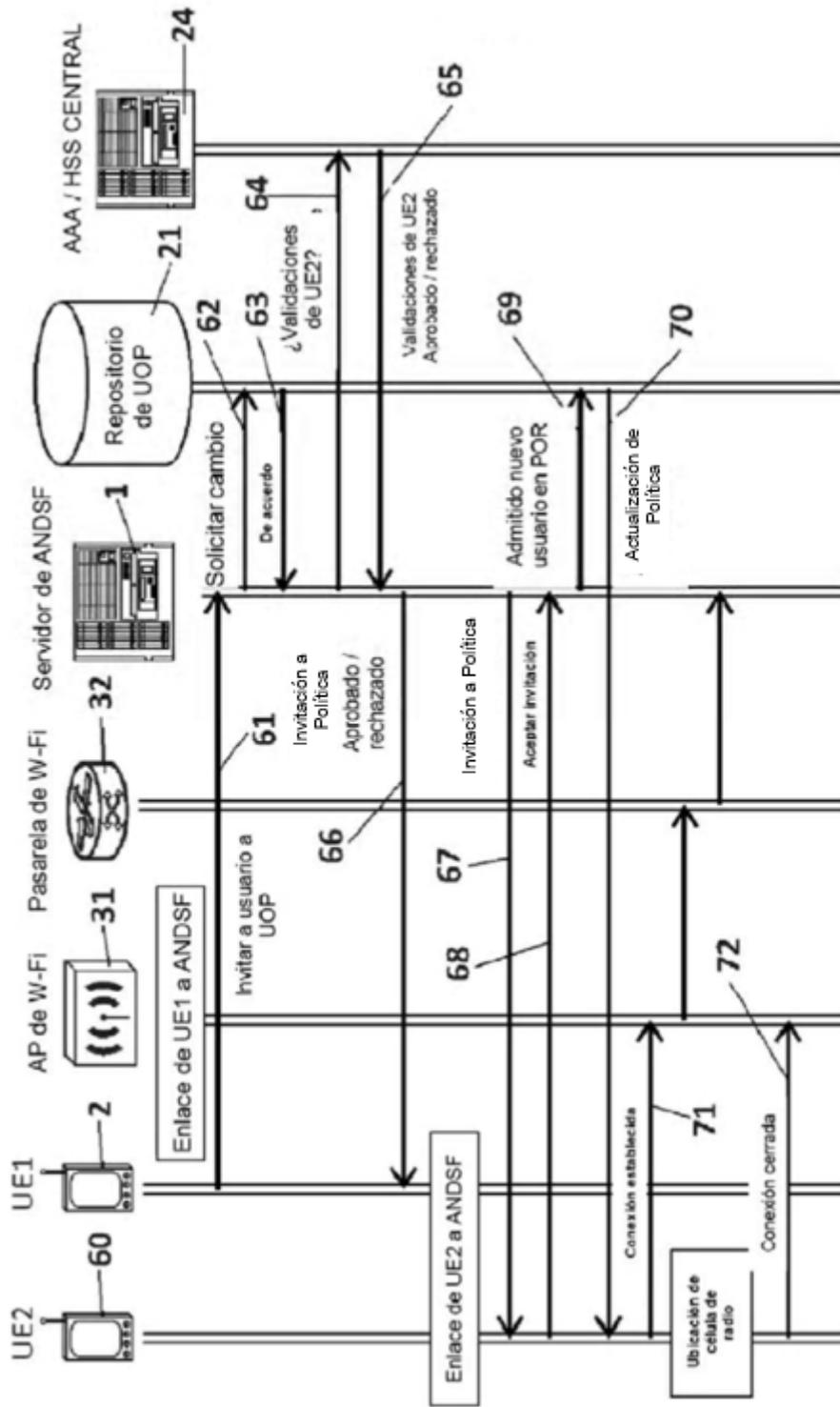


FIG. 6

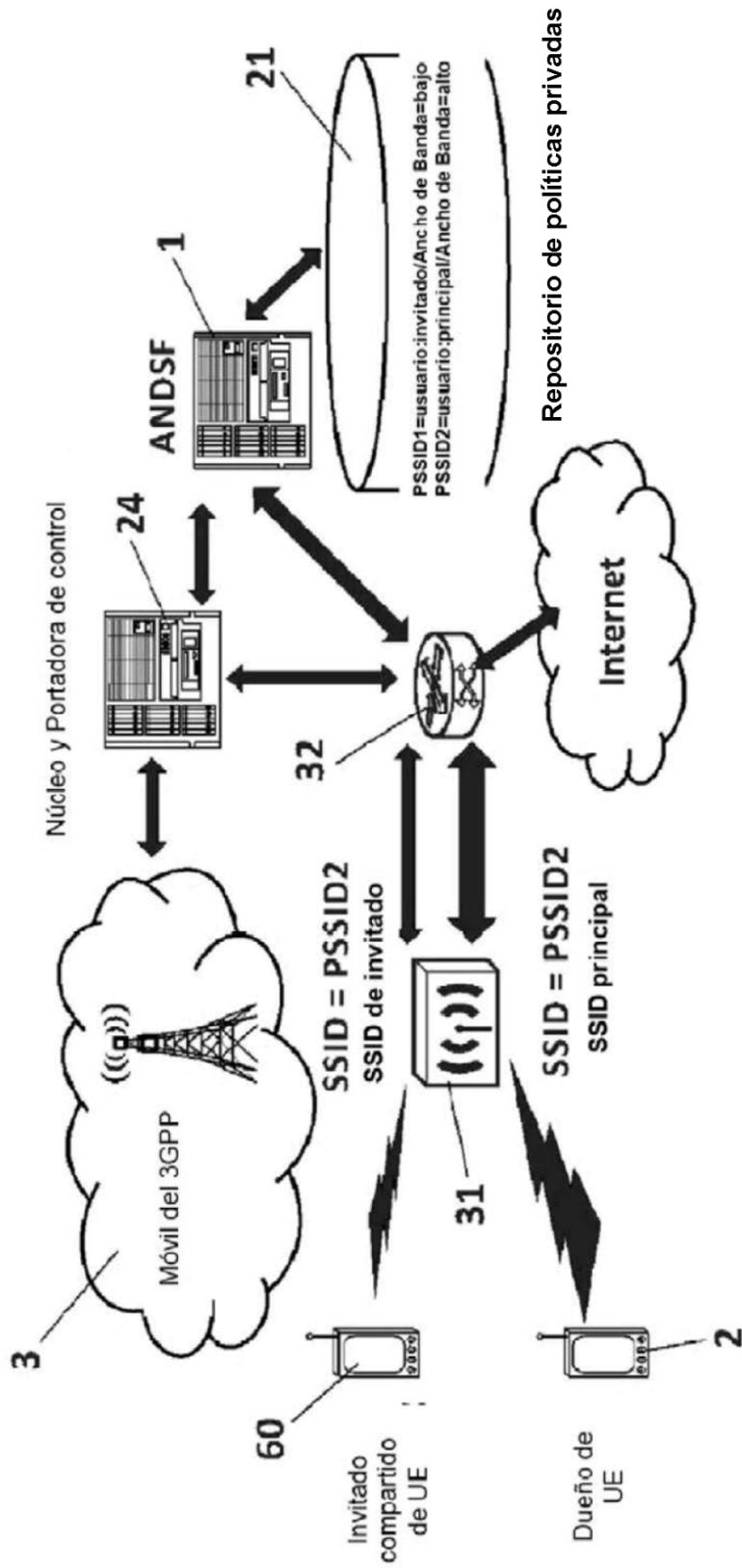


FIG. 7

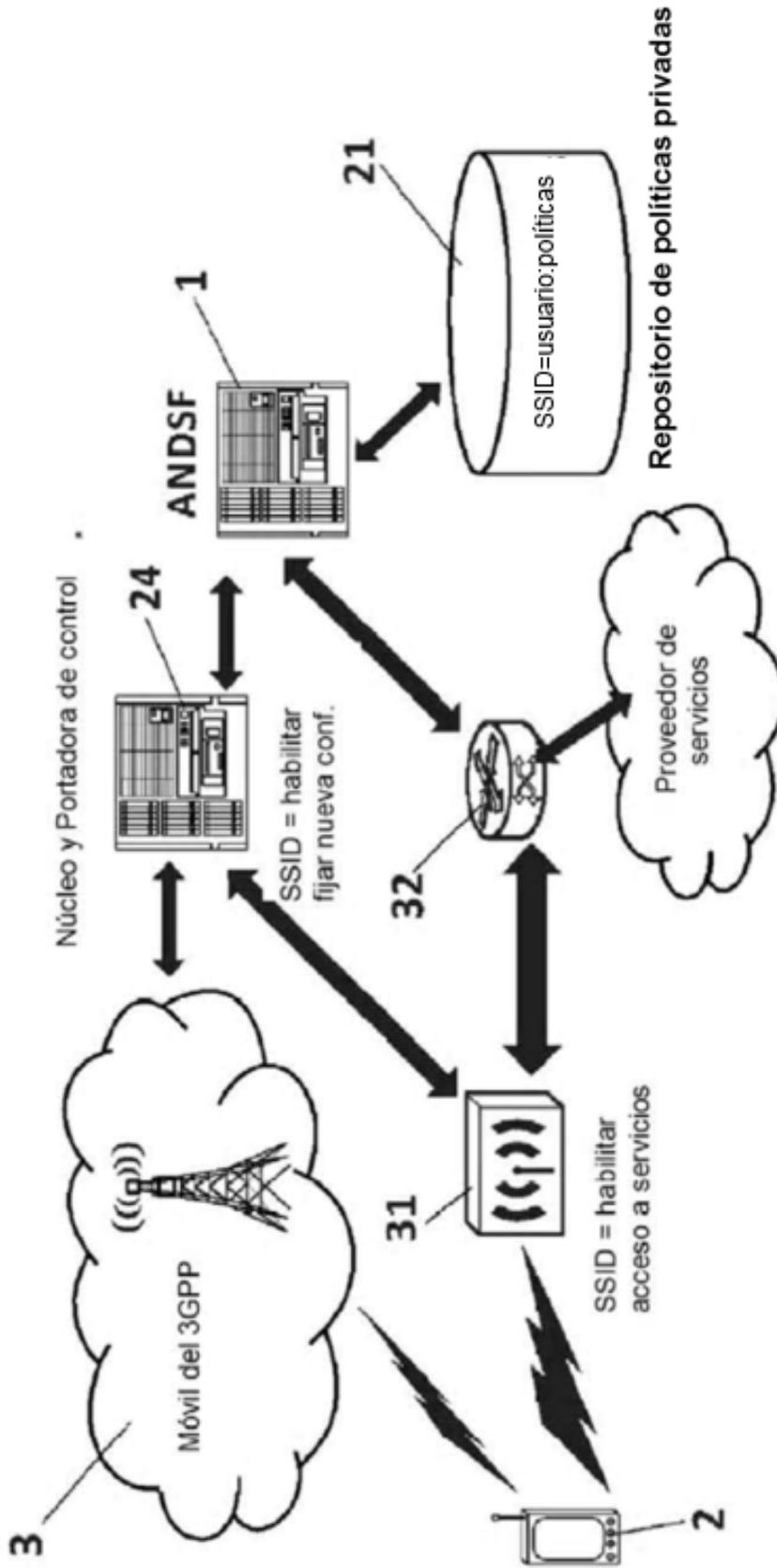


FIG. 8