

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **3 029 837**

51 Int. Cl.:

H04W 4/50	(2008.01) H04L 67/1001	(2012.01)
H04L 67/02	(2012.01) G06F 21/62	(2013.01)
H04L 9/32	(2006.01)	
H04L 9/40	(2012.01)	
G06F 21/33	(2013.01)	
H04W 12/06	(2011.01)	
H04W 48/16	(2009.01)	
H04W 48/06	(2009.01)	
H04L 67/51	(2012.01)	
H04W 12/084	(2011.01)	

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 86 Fecha de presentación y número de la solicitud internacional: **19.06.2019** **PCT/FI2019/050475**
- 87 Fecha y número de publicación internacional: **02.01.2020** **WO20002764**
- 96 Fecha de presentación y número de la solicitud europea: **19.06.2019** **E 19827138 (9)**
- 97 Fecha y número de publicación de la concesión europea: **23.04.2025** **EP 3815401**

54 Título: **Gestión de seguridad para el acceso a servicios en un sistema de comunicación**

30 Prioridad:

29.06.2018 IN 201841024429

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

25.06.2025

73 Titular/es:

NOKIA TECHNOLOGIES OY (100.00%)
Karakaari 7
02610 Espoo, FI

72 Inventor/es:

S BYKAMPADI, NAGENDRA y
NIEMELÄ, TUOMAS

74 Agente/Representante:

DEL VALLE VALIENTE, Sonia

ES 3 029 837 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

Gestión de seguridad para el acceso a servicios en un sistema de comunicación

5 **Campo**

El campo se refiere generalmente a sistemas de comunicación y, más particularmente, pero no exclusivamente, a la gestión de seguridad dentro de tales sistemas.

10 **Antecedentes**

Esta sección introduce aspectos que pueden ser útiles para facilitar una mejor comprensión de los aspectos de esta exposición. Por lo tanto, las declaraciones de esta sección deben interpretarse bajo este punto de vista y no deben entenderse como admisiones sobre lo que constituye o no técnica anterior.

15 La tecnología de telecomunicaciones móviles inalámbricas de cuarta generación (4G), también conocida como tecnología de evolución a largo plazo (LTE), se diseñó para proporcionar multimedia móvil de gran capacidad con elevadas velocidades de transmisión de datos, especialmente para la interacción humana. La tecnología de nueva generación o de quinta generación (5G) está destinada a utilizarse no solo para la interacción humana, sino también para comunicaciones de tipo máquina en las así denominadas redes de Internet de las cosas (IdC).

20 Aunque las redes 5G están previstas para permitir servicios de IdC masivos (p. ej., números muy grandes de dispositivos de capacidad limitada) y servicios IdC críticos para la misión (p. ej., que requieren una gran fiabilidad), mejoras con respecto a servicios de comunicación móvil de legado están soportadas en forma de servicios de banda ancha móvil potenciada (eMBB) que proporcionan un acceso a Internet mejorado para dispositivos móviles.

25 En un ejemplo de sistema de comunicación, el equipo de usuario (UE de 5G en una red 5G o, más ampliamente, un UE) tal como un terminal móvil (abonado) se comunica a través de una interfaz aérea con una estación base o punto de acceso denominado gNB en una red 5G. El punto de acceso (p. ej., gNB) forma parte, de forma ilustrativa, de una red de acceso del sistema de comunicación. Por ejemplo, en una red 5G, la red de acceso se denomina sistema de 5G y se describe en la Especificación Técnica (TS) de 5G 23.501, V15.0.0, titulada "Technical Specification Group Services and System Aspects; System Architecture for the 5G System". Generalmente, el punto de acceso (p. ej., gNB) proporciona acceso para el UE a una red central (CN), que entonces proporciona acceso para el UE a otros UE y/o a una red de datos tal como una red de datos en paquetes (p. ej., Internet).

35 TS 23.501 va a definir una arquitectura basada en servicios (SBA) de 5G que modela servicios como funciones de red (NF) que se comunican entre sí usando interfaces de programación de aplicaciones de transferencia de estado representacional (Restful API).

40 Asimismo, la Especificación Técnica (TS) de 5G 33.501, V15.1.0, titulada "Technical Specification Group Services and System Aspects; Security Architecture and Procedures for the 5G System" describe adicionalmente detalles de gestión de seguridad asociados con una red 5G.

45 La gestión de seguridad es una consideración importante en cualquier sistema de comunicación. Por ejemplo, la autorización de acceso a los servicios es un ejemplo de gestión de seguridad en una red 5G. Sin embargo, la autorización de acceso al servicio presenta varios retos en los planteamientos existentes de la 5G.

La patente US2006/0.041.669A1 describe técnicas para proteger un servicio web.

50 **Resumen**

La invención está definida por las reivindicaciones independientes adjuntas.

55 Se definen otras realizaciones en las reivindicaciones dependientes adjuntas.

Los aspectos ilustrativos proporcionan técnicas mejoradas para la gestión de seguridad en sistemas de comunicación, particularmente con respecto a la autorización de acceso al servicio.

60 Por ejemplo, en un aspecto ilustrativo, un método comprende las siguientes etapas. Una entidad de autorización en un sistema de comunicación que comprende una arquitectura basada en servicios recibe una solicitud de un consumidor de servicios en el sistema de comunicación para acceder a un tipo de servicio determinado. La entidad de autorización obtiene un token de acceso que identifica una pluralidad de productores de servicios para el tipo de servicio dado y envía el token de acceso al consumidor de servicios.

65 En otro aspecto, un método comprende las siguientes etapas. Un consumidor de servicios en un sistema de comunicación que comprende una arquitectura basada en servicios envía a una entidad de autorización en el sistema

de comunicación una solicitud de acceso a un tipo de servicio determinado. El consumidor de servicios recibe un token de acceso de la entidad de autorización, en donde el token de acceso identifica una pluralidad de productores de servicios en el sistema de comunicación para el tipo de servicio dado. Uno de la pluralidad de productores de servicios del token de acceso se selecciona basándose en uno o más criterios de selección.

En otro aspecto adicional, un método comprende las siguientes etapas. Un elemento proxy en un sistema de comunicación que comprende una arquitectura basada en servicios recibe un token de acceso, en donde el token de acceso identifica una pluralidad de productores de servicios en el sistema de comunicación para un tipo de servicio determinado generado por una entidad de autorización en el sistema de comunicación en respuesta a una solicitud de un consumidor de servicios en el sistema de comunicación para acceder al tipo de servicio dado. Uno de la pluralidad de productores de servicios del token de acceso se selecciona en el elemento proxy basándose en uno o más criterios de selección. En un aspecto adicional, el elemento proxy envía la información de identificación del consumidor de servicios para el productor de servicios seleccionado al consumidor de servicios.

En otro aspecto más, un método comprende las siguientes etapas. Un consumidor de servicios recibe un token de acceso en un sistema de comunicación que comprende una arquitectura basada en servicios desde una entidad de autorización, en donde el token de acceso identifica una pluralidad de elementos proxy correspondientes a los productores de servicios en el sistema de comunicación para un tipo de servicio determinado. El consumidor de servicios selecciona uno de la pluralidad de elementos proxy del token de acceso y envía una solicitud para acceder al tipo de servicio dado al elemento proxy seleccionado.

Se proporcionan aspectos ilustrativos adicionales en forma de un soporte de almacenamiento legible por ordenador no transitorio que tiene incorporado en el mismo un código de programa ejecutable que, cuando es ejecutado por un procesador, hace que el procesador realice las etapas anteriores. Otros aspectos ilustrativos adicionales comprenden un aparato con un procesador y una memoria configurados para realizar las etapas anteriores.

Estas y otras características y ventajas de los aspectos descritos en la presente memoria resultarán más evidentes a partir de los dibujos adjuntos y la siguiente descripción detallada.

Breve descripción de los dibujos

La figura 1 ilustra un sistema de comunicación con el que se pueden implementar uno o más aspectos ilustrativos.

La figura 2 ilustra elementos/funciones de red para proporcionar una gestión de seguridad con la que se pueden implementar uno o más aspectos ilustrativos.

La figura 3 ilustra una arquitectura de sistema de comunicación con funciones de red que interactúan entre y dentro de una red visitada y una red doméstica con la que se pueden implementar uno o más aspectos ilustrativos.

La figura 4 ilustra una metodología para la autorización de acceso al servicio en un sistema de comunicación, según un aspecto ilustrativo.

La figura 5 ilustra una metodología para generar un token de acceso para su uso en la autorización de acceso al servicio en un sistema de comunicación, según un aspecto ilustrativo.

La figura 6 ilustra al menos una porción de un token de acceso para su uso en la autorización de acceso al servicio en un sistema de comunicación, según un aspecto ilustrativo.

La figura 7 ilustra una metodología para el descubrimiento de servicios en un sistema de comunicación, según un aspecto ilustrativo.

Descripción detallada

Se ilustrarán aspectos en la presente memoria junto con ejemplos de sistemas de comunicación y técnicas asociadas para proporcionar gestión de seguridad en sistemas de comunicación. Sin embargo, se debe entender que el alcance de las reivindicaciones no se limitan a tipos particulares de sistemas de comunicación y/o de procesos expuestos. Se pueden implementar aspectos en una amplia variedad de otros tipos de sistemas de comunicación usando procesos y operaciones alternativos. Por ejemplo, aunque se ilustran en el contexto de sistemas celulares inalámbricos que usan elementos del sistema de 3GPP tales como un sistema de 3GPP de nueva generación (5G), los aspectos expuestos se pueden adaptar de una manera directa a una variedad de otros tipos de sistemas de comunicación.

Según los aspectos ilustrativos implementados en un entorno de sistema de comunicación 5G, una o más especificaciones técnicas (TS) e informes técnicos (TR) de 3GPP proporcionan una explicación adicional de los elementos/funciones de red y/o operaciones que interactúan con uno o más aspectos ilustrativos, p. ej., las TS 23.501 de 3GPP y TS 33.501 de 3GPP mencionadas anteriormente. Otros documentos de TS/TR de 3GPP proporcionan otros detalles convencionales que constatará un experto habitual en la técnica. Sin embargo, aunque sean adecuados

para normas de 3GPP referidas a 5G, no se pretende necesariamente que los aspectos estén limitados a ninguna norma particular.

Los aspectos ilustrativos se refieren a la gestión de seguridad asociada con la arquitectura basada en servicios (SBA) para redes 5G. Antes de describir tales aspectos ilustrativos, a continuación se describirá una descripción general de componentes principales de una red 5G en el contexto de las figuras 1 y 2.

La figura 1 muestra un sistema 100 de comunicación dentro del cual se implementan aspectos ilustrativos. Debe entenderse que los elementos mostrados en el sistema 100 de comunicación están destinados a representar funciones principales proporcionadas dentro del sistema, p. ej., funciones de acceso de UE, funciones de gestión de movilidad, funciones de autenticación, funciones de pasarela que da servicio, etc. Como tales, los bloques mostrados en la figura 1 hacen referencia a elementos específicos en redes 5G que proporcionan estas funciones principales. Sin embargo, se utilizan otros elementos de red en otros aspectos para implementar algunas o todas las funciones principales representadas. También debe entenderse que no todas las funciones de una red 5G se representan en la figura 1. Más bien, se representan funciones que facilitan una explicación de aspectos ilustrativos. Las figuras posteriores representan algunos elementos/funciones adicionales.

Por consiguiente, tal como se muestra, el sistema 100 de comunicación comprende un equipo 102 de usuario (UE) que se comunica a través de una interfaz 103 aérea con un punto 104 de acceso (gNB). El UE 102 en algunos aspectos puede ser una estación móvil, y tal estación móvil puede comprender, a manera de ejemplo, un teléfono móvil, un ordenador o cualquier otro tipo de dispositivo de comunicación. Por lo tanto, se pretende que el término “equipo de usuario”, como se utiliza en la presente memoria, se considere de manera amplia para abarcar una variedad de diferentes tipos de estaciones móviles, estaciones de abonado o, más generalmente, dispositivos de comunicación, incluidos ejemplos tales como una combinación de una tarjeta de datos introducida en un ordenador portátil u otro equipo tal como un teléfono inteligente. También se pretende que tales dispositivos de comunicación engloben los dispositivos comúnmente denominados terminales de acceso.

En un aspecto, el UE 102 comprende una parte de tarjeta de circuito integrado universal (UICC) y una parte de equipo móvil (ME). La UICC es la parte dependiente de usuario del UE y contiene al menos un módulo de identidad de abonado universal (USIM) y un software de aplicación apropiado. El USIM almacena de forma segura el identificador de suscripción permanente y su clave relacionada, que se usan para identificar y autenticar abonados a redes de acceso. La ME es la parte independiente de usuario del UE y contiene funciones de equipo terminal (TE) y diversas funciones de terminación móvil (MT).

Obsérvese que, en un ejemplo, el identificador de suscripción permanente es una identidad de abonado móvil internacional (IMSI) de un UE. En un aspecto, la IMSI tiene una longitud fija de 15 dígitos y consiste en un código de país móvil (MCC) de 3 dígitos, un código de red móvil de 3 dígitos (MNC) y un número de identificación de estación móvil (MSIN) de 9 dígitos. En un sistema de comunicación de 5G, una IMSI se denomina identificador permanente de suscripción (SUPI). En el caso de una IMSI como SUPI, el MSIN proporciona la identidad de abonado. Por lo tanto, típicamente solo la porción de MSIN de la IMSI tiene que cifrarse. Las porciones MNC y MCC de la IMSI proporcionan información de enrutamiento, usada por la red que da servicio para enrutar a la red doméstica correcta. Cuando el MSIN de un SUPI está cifrado, se denomina identificador oculto de suscripción (SUCI).

El punto 104 de acceso forma parte, de forma ilustrativa, de una red de acceso del sistema 100 de comunicación. Una red de acceso de este tipo comprende, por ejemplo, un sistema de 5G que tiene una pluralidad de estaciones base y una o más funciones de control de red de radio asociadas. En algunos aspectos, las estaciones base y las funciones de control de red de radio pueden ser entidades lógicamente independientes, pero, en otros aspectos, se implementan en el mismo elemento de red física, tal como, por ejemplo, un enrutador de estación base o un punto de acceso celular femto.

El punto 104 de acceso en este aspecto ilustrativo está acoplado operativamente a funciones de gestión de movilidad 106. En una red 5G, la función de gestión de movilidad se implementa mediante una función de gestión de acceso y movilidad (AMF). Una función de anclaje de seguridad (SEAF) en algunos aspectos también se implementa con la AMF que conecta un UE con la función de gestión de movilidad. Una función de gestión de movilidad, como se utiliza en la presente memoria, es el elemento o función (es decir, entidad) en la parte de red central (CN) del sistema de comunicación que gestiona o participa de cualquier otra manera, entre otras operaciones de red, en operaciones de acceso y movilidad (incluidas de autenticación/autorización) con el UE (a través del punto 104 de acceso). La AMF también se puede denominar en la presente memoria, más generalmente, entidad de gestión de acceso y movilidad.

La AMF 106 en este aspecto ilustrativo está acoplada operativamente a funciones 108 de abonado domésticas, es decir, una o más funciones que residen en la red doméstica del abonado. Como se muestra, algunas de estas funciones incluyen la función de gestión de datos unificada (UDM), así como una función de servidor de autenticación (AUSF). La AUSF y la UDM (por separado o colectivamente) también se denominan en la presente memoria, más generalmente, como una entidad de autenticación. Por añadidura, las funciones de abonado domésticas incluyen, aunque no de forma limitativa, función de selección de segmento de red (NSSF), función de exposición a red (NEF), función de repositorio de red (NRF), función de control de política (PCF) y función de aplicación (AF).

Un punto importante a tener en cuenta es que en un sistema de comunicación SBA, tal como un sistema 5G, el plano de control utiliza un planteamiento de modelo de servicios en el que los componentes (NF) consultan la NRF para descubrir y comunicarse entre sí a través de interfaces de programación de aplicaciones (API). El método de descubrimiento y autorización de servicios NF se describirá con más detalle a continuación.

El punto 104 de acceso también está acoplado operativamente a una función de pasarela que da servicio, es decir, función 110 de gestión de sesión (SMF), que está acoplada operativamente a una función 112 de plano de usuario (UPF). La UPF 112 está operativamente acoplada a una red de datos en paquetes, p. ej., Internet 114. Operaciones y funciones típicas adicionales de tales elementos de red no se describen aquí ya que no son el enfoque de los aspectos ilustrativos y se pueden encontrar en la documentación de 5G de 3GPP apropiada.

Debe apreciarse que esta disposición particular de elementos de sistema es solo un ejemplo y que, en otros aspectos, se pueden utilizar otros tipos y disposiciones de elementos adicionales o alternativos para implementar un sistema de comunicación. Por ejemplo, en otros aspectos, el sistema 100 comprende otros elementos/funciones no mostrados expresamente en la presente memoria.

En consecuencia, la disposición de la figura 1 es solo una configuración de ejemplo de un sistema celular inalámbrico, y pueden utilizarse numerosas configuraciones alternativas de elementos de sistema. Por ejemplo, aunque en el aspecto de la figura 1 solo se muestran elementos/funciones individuales, esto es solo por simplicidad y transparencia de la descripción. Naturalmente, un aspecto alternativo dado puede incluir mayores números de tales elementos de sistema, así como elementos adicionales o alternativos de un tipo habitualmente asociado a implementaciones de sistema convencionales.

También cabe señalar que, aunque la figura 1 ilustra elementos de sistema como bloques funcionales singulares, las diversas subredes que forman la red 5G están divididas en los así denominados segmentos de red. Los segmentos de red (particiones de red) comprenden una serie de conjuntos de funciones de red (NF) (es decir, cadenas de funciones) para cada tipo de servicio correspondiente usando una virtualización de funciones de red (NFV) en una infraestructura física común. Los segmentos de red se instancian cuando es necesario para un servicio dado, p. ej., un servicio de eMBB, un servicio IdC masivo y un servicio IdC crítico de misión. Por lo tanto, un segmento o función de red se instancia cuando se crea una instancia de ese segmento o función de red. En algunos aspectos, esto implica instalar o ejecutar de cualquier otra manera el segmento o función de red en uno o varios dispositivos de anfitrión de la infraestructura física subyacente. El UE 102 está configurado para acceder a uno o más de estos servicios a través del gNB 104. Las NF también pueden acceder a servicios de otras NF.

La figura 2 es un diagrama de bloques de elementos/funciones de red para proporcionar una gestión de seguridad en un aspecto ilustrativo. Se muestra el sistema 200 que comprende un primer elemento/función 202 de red y un segundo elemento/función 204 de red. Debe apreciarse que los elementos/funciones 202 y 204 de red representan cualquier elemento/función de red que esté configurado para proporcionar gestión de seguridad y otras técnicas descritas en la presente memoria, por ejemplo, aunque no de forma limitativa, AMF, SEAF, UDM, AUSF, NSSF, NEF, NRF, PCF y AF.

El elemento/función 202 de red comprende un procesador 212 que está acoplado a una memoria 216 y a un conjunto 210 de circuitos de interfaz. El procesador 212 del elemento/función 202 de red incluye un módulo 214 de procesamiento de gestión de seguridad que puede implementarse, al menos en parte, en forma de software ejecutado por el procesador. El módulo 214 de procesamiento realiza la gestión de seguridad descrita junto con las figuras posteriores y de cualquier otra manera en la presente memoria. La memoria 216 del elemento/función 202 de red incluye un módulo 218 de almacenamiento de gestión de seguridad que almacena datos generados o utilizados de cualquier otra manera durante las operaciones de gestión de seguridad.

El elemento/función 204 de red comprende un procesador 222 que está acoplado a una memoria 226 y a un conjunto 220 de circuitos de interfaz. El procesador 222 del elemento/función 204 de red incluye un módulo 224 de procesamiento de gestión de seguridad que puede implementarse, al menos en parte, en forma de software ejecutado por el procesador 222. El módulo 224 de procesamiento realiza la gestión de seguridad descrita junto con las figuras posteriores y de cualquier otra manera en la presente memoria. La memoria 226 del elemento/función 204 de red incluye un módulo 228 de almacenamiento de gestión de seguridad que almacena datos generados o utilizados de cualquier otra manera durante las operaciones de gestión de seguridad.

Los procesadores 212 y 222 de los elementos/funciones 202 y 204 de red respectivos pueden comprender, por ejemplo, microprocesadores, circuitos integrados de aplicación específica (ASIC), matrices de puertas programables en el campo (FPGA), procesadores de señales digitales (DSP) u otros tipos de dispositivos de procesamiento o conjuntos de circuitos integrados, así como porciones o combinaciones de tales elementos. Tales dispositivos de circuitos integrados, así como porciones o combinaciones de los mismos, son ejemplos de “conjuntos de circuitos”, como se utiliza este término en la presente memoria. Se puede utilizar una amplia variedad de otras disposiciones de hardware y software o firmware asociado para implementar los aspectos ilustrativos.

Las memorias 216 y 226 de los elementos/funciones 202 y 204 de red respectivos pueden usarse para almacenar uno o más programas de software que se ejecutan por los procesadores 212 y 222 respectivos para implementar al menos una porción de la funcionalidad descrita en la presente memoria. Por ejemplo, como se describe junto con figuras posteriores y de cualquier otra manera en la presente memoria, pueden implementarse operaciones de gestión de seguridad y otras funcionalidades de forma sencilla usando un código de software ejecutado por los procesadores 212 y 222.

Por lo tanto, se puede considerar que una dada de las memorias 216 o 226 es un ejemplo de lo que se denomina más generalmente en la presente memoria un producto de programa informático o, aún más generalmente, soporte de almacenamiento legible por procesador que tiene un código de programa ejecutable incorporado en el mismo. Otros ejemplos de soportes de almacenamiento legibles por procesador pueden incluir discos u otros tipos de soportes magnéticos u ópticos, en cualquier combinación. Los aspectos ilustrativos pueden incluir artículos de fabricación que comprenden tales productos de programa informático u otros soportes de almacenamiento legibles por procesador.

Más particularmente, la memoria 216 o 226 puede comprender, por ejemplo, una memoria de acceso aleatorio (RAM) electrónica, tal como una RAM estática (SRAM), una RAM dinámica (DRAM) u otros tipos de memoria electrónica volátil o no volátil. Estas últimas pueden incluir, por ejemplo, memorias no volátiles tales como una memoria flash, una RAM magnética (MRAM), una RAM de cambio de fase (PC-RAM) o una RAM ferroeléctrica (FRAM). Como se utiliza en la presente memoria, se pretende que el término “memoria” se considere de forma amplia, que, por ejemplo, puede abarcar, de forma adicional o alternativamente, una memoria de solo lectura (ROM), una memoria basada en disco u otro tipo de dispositivo de almacenamiento, así como porciones o combinaciones de tales dispositivos.

Los sistemas 210 y 220 de circuitos de interfaz de los elementos/funciones 202 y 204 de red respectivos comprenden, de forma ilustrativa, transceptores u otro hardware o firmware de comunicación que permiten que los elementos de sistema asociados se comuniquen entre sí de la forma descrita en la presente memoria.

A partir de la figura 2 resulta evidente que el elemento/función 202 de red está configurado para una comunicación con el elemento/función 204 de red, y viceversa, a través de sus conjuntos 210 y 220 de circuitos de interfaz respectivos. Esta comunicación implica que el elemento/función 202 de red envía datos al elemento/función 204 de red, y el elemento/función 204 de red envía datos al elemento/función 202 de red. Sin embargo, en aspectos alternativos, otros elementos de red pueden estar acoplados operativamente entre los elementos/funciones 202 y 204 de red. Se pretende que el término “datos” como se utiliza en la presente memoria se considere ampliamente, para abarcar cualquier tipo de información que pueda enviarse entre elementos/funciones de red (así como entre equipos de usuario y redes centrales) incluidos, aunque no de forma limitativa, mensajes, identificadores, claves, indicadores, datos de usuario, datos de control, etc.

Por lo tanto, en un ejemplo, el elemento/función de red 202 es una NF, tal como una AMF, y el elemento/función de red 204 es una NRF. En tal caso, la AMF y la NRF participan en una metodología de autorización de acceso al servicio (descubrimiento y selección) e intercambian mensajes/datos según sea necesario. Tal metodología de autorización de acceso al servicio se describirá adicionalmente a continuación.

Debe apreciarse que la disposición particular de componentes mostrada en la figura 2 es solo un ejemplo y se usan numerosas configuraciones alternativas en otros aspectos. Por ejemplo, cualquier elemento/función de red puede estar configurado para incorporar componentes adicionales o alternativos y soportar otros protocolos de comunicación.

Otros elementos de sistema, tales como el EU 102 y el gNB 104, pueden configurarse también para incluir componentes tales como un procesador, una memoria y una interfaz de red. Estos elementos no necesitan implementarse en plataformas de procesamiento autónomas e independientes, sino que, por ejemplo, representan distintas porciones funcionales de una única plataforma común de procesamiento.

Dados los conceptos generales descritos anteriormente, ahora se describirán realizaciones ilustrativas que abordan determinadas cuestiones de gestión de seguridad. Más particularmente, los aspectos ilustrativos proporcionan técnicas de gestión de seguridad para sistemas 5G. En la actualidad, la arquitectura de los sistemas 5G se está estandarizando en 3GPP. Como se mencionó anteriormente, la TS 23.501 de 3GPP define la arquitectura del sistema 5G como basada en servicios, p. ej., una arquitectura basada en servicios (SBA).

La figura 3 representa una arquitectura 5G en una configuración que comprende una red móvil terrestre pública visitada (VPLMN) 310 acoplada operativamente a través de una red 320 intermedia de intercambio de paquetes entre redes (IPX) a una red móvil terrestre pública doméstica (HPLMN) 330. Obsérvese que puede haber más de una red IPX acoplada operativamente entre la VPLMN 310 y la HPLMN 330. La figura 3 ilustra también la presencia de un proxy de protección perimetral de seguridad (SEPP) en el perímetro de cada PLMN, es decir, vSEPP 312 en VPLMN 310 y hSEPP 332 en HPLMN 330. Debe apreciarse que las diversas funciones de red mostradas en la VPLMN 310 y la HPLMN 330 se conocen y describen en detalle en varias especificaciones de 5G tales como, aunque no de forma limitativa, las TS 23.501 y TS 33.501 mencionadas anteriormente.

Como se mencionó anteriormente, en 5G, la SBA se introduce para modelar los servicios como funciones de red (NF) que se comunican entre sí mediante interfaces de programación de aplicaciones RESTful (API de transferencia de estado representacional). En la situación donde las dos NF que se comunican están en dos PLMN diferentes (p. ej., la VPLMN 310 y la HPLMN 330), la comunicación se produce a través de una interfaz (N32) interred itinerante entre las dos PLMN participantes.

Para proteger el contenido específico de la NF en los mensajes que se envían a través de la interfaz interred itinerante, 5G presenta el SEPP como la entidad que reside en el perímetro de la red PLMN para proteger la PLMN del tráfico externo y, además, para implementar la seguridad de capa de transporte (TLS) y la seguridad de capa de aplicación (ALS) para todos los datos y la señalización intercambiados entre dos funciones de red interred en la capa de servicio. Por ejemplo, el SEPP realiza funciones de gestión de seguridad en los elementos de información (IE) de los mensajes del protocolo de transporte de hipertexto (HTTP) antes de que los mensajes se envíen externamente a través de la interfaz N32 itinerante. Los mensajes HTTP protegidos se denominan mensajes N32. La protección, tal como ALS, implica proteger la información que se envía en diversas partes del mensaje HTTP, incluidas, aunque no de forma limitativa, la línea de solicitud/respuesta HTTP, el encabezado HTTP y la carga útil HTTP. Sin embargo, puede que algunas partes de este mensaje necesiten modificarse mediante intermediarios (p. ej., el proveedor de red de IPX 330, como se muestra en la figura 3) entre los dos SEPP.

Por lo tanto, en la SBA 5G, el operador de PLMN implementa un SEPP en el perímetro de su red para interoperar y obtener servicios a partir de las funciones de red en sus redes asociadas itinerantes. El SEPP interactúa con uno o más SEPP en una o más redes a través de la interfaz N32. Como proxy perimetral, el SEPP implementa ALS como se mencionó anteriormente para proteger los mensajes HTTP intercambiados entre una función de red en su red y otra función de red en la red asociada itinerante.

Si bien dos NF pueden estar en diferentes PLMN, como ilustra la figura 3, algunos NF en la misma PLMN también tienen la necesidad de comunicarse. En cualquier escenario (comunicación entre PLMN o comunicación dentro de una PLMN), el modelo de comunicación de SBA incluye métodos de seguridad que permiten que un “consumidor de servicios de NF” (cliente de servicio) sea autenticado y autorizado para acceder a un servicio proporcionado por un “productor de servicios de NF” (servidor de servicios) o asociado de cualquier otra manera con él. Uno de los métodos de autorización admitidos en la TS 33.501 (versión 15) de 3GPP mencionada anteriormente se basa en la metodología del token de acceso de OAuth 2.0. En un sistema 5G, se adopta el siguiente modelo cuando se usa OAuth 2.0: (i) la NRF es el servidor de autorización de OAuth 2.0; (ii) el consumidor de servicios de NF es el cliente de OAuth 2.0; y (iii) el productor de servicios de NF es el servidor de recursos de OAuth 2.0.

El consumidor de servicios de NF (cliente) descubre el productor de servicios de NF (servidor de recursos) a través de la NRF y, a continuación, obtiene un token de acceso para presentárselo al productor de servicios de NF al invocar la solicitud de la API del servicio. En los planteamientos existentes (como se describe en la TS 33.501 (versión 15) de 3GPP mencionada anteriormente), el token de acceso está vinculado a la instancia específica del productor de NF que selecciona la NRF o el consumidor de servicios de NF al final del proceso de descubrimiento.

Los aspectos ilustrativos ponen de manifiesto que, al vincular el token de acceso a una única instancia del productor de NF en particular, se evita que la lógica de selección seleccione de entre un grupo de instancias del productor de NF. Los aspectos ilustrativos además ponen de manifiesto que seleccionar de entre un grupo de instancias es relevante para los casos en los que la instancia utilizada actualmente falla, o cuando existe el deseo de seleccionar rápidamente una instancia diferente para fines de equilibrio de carga, o en el caso de una entidad proxy intermediaria que haría la selección en nombre del consumidor de servicios de NF. Por añadidura, los aspectos ilustrativos ponen de manifiesto que tener una asociación 1:1 entre el token de acceso y la instancia del productor de NF es subóptimo, ya que obliga al consumidor de NF a obtener un nuevo token cada vez que hay un cambio en el productor de servicios. De hecho, la solución estandarizada actual de 3GPP requiere que el consumidor de servicios de NF obtenga un nuevo token de acceso para cada solicitud de servicio y tal token de acceso es por cada instancia del productor de NF de la que desee obtener servicios. Véase la TS 33.501 de 3GPP, Cláusula 13.4, mencionada anteriormente.

Como se explicará adicionalmente en detalle en la presente memoria, los aspectos ilustrativos proporcionan una autorización de acceso al servicio mejorada que permite que la lógica de selección de servicios seleccione de entre dos o más instancias del productor de NF. Por ejemplo, en un aspecto, la NRF genera un token de acceso basado en un token web de notación de objetos de JavaScript (JSON) y rellena el campo de reclamación de audiencia del token con direcciones de puntos de conexión (es decir, localizadores de recursos o URL uniformes) para el conjunto de instancia(s) del productor de NF o instancia(s) de servicio del productor de NF descubiertas. La NRF devuelve el token generado cuando el consumidor de servicios de NF solicita un token de acceso después de la etapa de descubrimiento. La lógica de selección de NF utiliza el campo de reclamación de audiencia para seleccionar una instancia del productor de NF basándose en diversos factores, tales como, aunque no de forma limitativa, el equilibrio de carga.

La figura 4 ilustra un ejemplo del proceso global como metodología 400.

Como se muestra en la etapa 402, durante el proceso de descubrimiento de servicios de NF, la NRF captura direcciones de puntos de conexión de todas las instancias del productor de servicios de NF descubiertas en el token de acceso.

- 5 En la etapa 404, la NRF devuelve el token de acceso almacenado a la instancia del consumidor de servicios de NF en un mensaje de respuesta del token de acceso.

10 En la etapa 406, la lógica de selección (en el consumidor de servicios de NF o en un proxy, como se explicará adicionalmente a continuación) aplica un conjunto de criterios para seleccionar una instancia del productor de servicios de NF basándose en las entradas en el token de acceso. Si la lógica de selección se implementa en el proxy, el proxy puede proporcionar la dirección de la instancia del productor seleccionada a la instancia del consumidor de servicios de NF.

15 Cada una de las etapas 402, 404 y 406 se describirá ahora con más detalle.

20 *Capturar todas las instancias del productor de servicios de NF descubiertas en el token de acceso (etapa 402).* Como parte del procedimiento de detección, la NRF determina la(s) instancia(s) de NF o instancia(s) de servicio de NF descubiertas y proporciona la información de un conjunto de instancia(s) de NF o instancia(s) de servicio de NF descubiertas al consumidor de servicios de NF mediante el mensaje de respuesta *Nnrf_NFDiscovery_Request*. La información incluye: FQDN (nombre de dominio completamente cualificado), dirección IP (protocolo de Internet) o direcciones de puntos de conexión (es decir, URL) para el conjunto de instancia(s) de NF o instancia(s) de servicio de NF descubiertas. Los detalles del proceso de descubrimiento se describen en más detalle en la Cláusula 4.17.4 de la Especificación Técnica (TS) 5G 23.502, V15.2.0, titulada “Technical Specification Group Services and System Aspects; Procedures for the 5G System, Stage 2”.

25 La figura 5 ilustra una metodología 500 con etapas adicionales que la NRF realiza como parte del procedimiento de descubrimiento según un aspecto ilustrativo.

30 En la etapa 502, la NRF genera un token de acceso en el formato token web JSON (JWT) como se describe en la solicitud de comentarios (RFC) 7519 del Grupo de Trabajo de Ingeniería de Internet (IETF), “JSON Web Token (JWT)”, mayo de 2015. Como se explicará, este formato se modifica para incluir una pluralidad de productores de servicios descubiertos con arreglo a la siguiente etapa.

35 En la etapa 504, la NRF rellena el campo de reclamación de audiencia en la estructura de token web JSON con las direcciones de puntos de conexión de todas las instancia(s) de productores de servicios de NF o instancia(s) de servicios de NF descubiertas. En otro aspecto, como se explicará adicionalmente a continuación, el token de acceso puede almacenar alternativamente las direcciones de puntos de conexión de los elementos proxy correspondientes a instancias del productor de servicios de NF.

40 En la etapa 506, la NRF almacena el token de acceso para que se pueda proporcionar a la instancia del consumidor de servicios de NF en el mensaje de respuesta del token de acceso (etapa 404).

45 La figura 6 ilustra al menos una porción de un token web JSON (JWT) 600 y específicamente cómo se usa el campo de reclamación de audiencia para capturar las direcciones de las instancias del productor de NF descubiertas con el token de acceso. Como se muestra, el JWT 600 comprende un campo de identidad NRF 602 (identifica la NRF que genera el token de acceso), la identidad 604 del consumidor NF (identifica la NF que solicita el token de acceso) y un campo de reclamación de audiencia 606 con una pluralidad de identidades y direcciones de productores de NF.

50 En el aspecto de ejemplo mostrado en la figura 6, la reclamación de audiencia es una matriz en la que cada elemento de la matriz comprende la Id. (identidad) de instancia de NF y la dirección de punto de conexión de la instancia del productor descubierta. Son posibles aspectos alternativos sobre cómo se formatea la reclamación de audiencia.

55 *La NRF devuelve la solicitud de token de acceso almacenado en el mensaje de respuesta del token de acceso (etapa 404).* La Cláusula 13.4.1.1 de la TS 33.501 de 3GPP mencionada anteriormente describe un procedimiento para obtener un token de acceso de la NRF. Esto se ejecuta en la instancia de NF del consumidor antes de acceder al servicio. Los aspectos ilustrativos proporcionan, *entre otros*, los siguientes cambios en el procedimiento actual:

60 1) Cuando la NRF recibe el mensaje de solicitud de token de acceso de la Id. de instancia de NF (Id. de consumidor de servicios) que ya estaba autorizada en la etapa de descubrimiento para un tipo de NF y un nombre de servicio objetivo en particular, la NRF omite volver a autorizar la instancia del consumidor de servicios de NF (que es la etapa 2 del procedimiento existente).

2) La NRF recupera el token de acceso que se genera durante el proceso de descubrimiento para esta Id. de instancia de NF (etapa 402) y lo proporciona en una respuesta de token de acceso.

65

Como se ha descrito anteriormente en el contexto de la etapa 402, el token de acceso se rellena con toda la información necesaria de las instancias del productor de servicios de NF descubiertas.

La figura 7 ilustra un flujo de mensajes modificado para una metodología de descubrimiento de servicios 700 según un aspecto ilustrativo. Más particularmente, como se muestra en la etapa 1, el consumidor 702 de servicios de NF envía una solicitud de token de acceso a la NRF 704 (servidor de autorización). La solicitud de token de acceso comprende la Id. de instancia de NF, el nombre de servicio de NF esperado y el tipo de servicio de NF esperado. En la etapa 2, la NRF 704 recupera el token de acceso almacenado para esta solicitud. A continuación, en la etapa 3, la NRF 704 envía una respuesta de token de acceso al consumidor 702 de servicios de NF (que comprende el token de acceso, el tiempo de caducidad del token y el alcance del token).

La lógica de selección selecciona una instancia del productor de servicios de NF (etapa 406). La instancia del consumidor de servicios de NF recibe el mensaje de respuesta del token de acceso con el token de acceso incluido. La instancia del consumidor de servicios de NF después aplica un conjunto de factores de evaluación para determinar qué instancia de productor de servicios de NF usar para la solicitud de servicio. El consumidor de servicios de NF ejecuta una API de solicitud de servicio para obtener el servicio de la instancia del productor de servicios de NF seleccionada. El token de acceso está incluido en la solicitud. Tenga en cuenta que la lógica de selección en algunos aspectos es parte de la instancia de consumidor de servicios de NF, mientras que en otros aspectos la lógica de selección es parte de un elemento proxy.

Dadas las descripciones ilustrativas anteriores, algunos aspectos ilustrativos se describen en más detalle a continuación.

1. Arquitectura basada en servicios (versión 15 de TS 33.501) donde la instancia del consumidor de servicios de NF realiza la selección. Este es un modelo Rel-15 en el que el consumidor de servicios de NF obtiene un token de acceso de la NRF que obtiene el servicio de una instancia del productor de NF seleccionada e incluye este token en la solicitud de servicio de API dirigida a la instancia del productor de servicios de NF. La implementación permite al consumidor de servicios de NF usar un token de acceso para obtener el servicio de más de una instancia del productor de servicios de NF elegible.

2. En una arquitectura donde un proxy actúa como centro para todos o algunos de los mensajes de la capa de servicio entre las NF dentro de la PLMN.

a. El proxy es la entidad que selecciona un productor de servicios de NF de la lista de productores de servicios de NF proporcionada por la NRF en la respuesta de descubrimiento de servicios de NF. La funcionalidad de proxy en algunos aspectos también reside en la propia NRF o tiene una interfaz patentada para la NRF. La NRF proporciona esta información al consumidor de servicios de NF en el mensaje de respuesta de descubrimiento de servicios NF.

b. El consumidor de servicios de NF incluye el token de acceso obtenido en la solicitud de servicio de API dirigida a la instancia del productor de servicios de NF.

c. En algunos aspectos, el proxy aplica el equilibrio de carga en la solicitud de servicio de API, lo que podría resultar en que el proxy seleccionara una nueva instancia del productor de NF de la lista de instancias del productor de NF presentes en el token de acceso. En algunos aspectos, el proxy también selecciona la instancia del productor de NF basándose en motivos distintos al equilibrio de carga.

d. El proxy enruta la solicitud de servicio a la instancia del productor de servicios de NF seleccionada.

3. En la arquitectura donde el proxy solo se encuentra entre los consumidores de servicios de NF y los productores de servicios de NF. En este modelo, el proxy no existe entre el consumidor de servicios de NF y la NRF. Es decir, el proxy solo escucha la comunicación entre dos NF.

Por lo tanto, en algunos aspectos, el proxy recibe el token de acceso del consumidor de servicios y no de la NRF.

Como en el escenario 2c. anterior, el proxy en algunos aspectos aplica el equilibrio de carga, o alguna otra funcionalidad referida a la selección, en la solicitud de servicio de API al cambiar la selección realizada por el consumidor de servicios de NF basándose en la información del token de acceso.

En un aspecto alternativo, como se mencionó anteriormente en la etapa 504 de la figura 5, en lugar de que el token de acceso almacene direcciones de puntos de conexión de los productores de servicios, la NRF puede generar un token de acceso que almacene direcciones de puntos de conexión de los elementos proxy. Este aspecto resulta útil cuando, por ejemplo, un proxy se encuentra entre las dos NF (consumidor de servicios y productor de servicios) y la dirección del productor de servicios no es visible externamente. El proxy se usa como controlador de acceso de una o más instancias de productores de servicios en el back-end. Por lo tanto, en este modelo alternativo, la NRF rellena el campo de reclamación de audiencia con las direcciones de puntos de conexión de los agentes (elementos) proxy. El

consumidor de servicios de NF selecciona una dirección y envía el mensaje al proxy. A continuación, el proxy selecciona la instancia del productor de servicios.

5 Por lo tanto, de forma ventajosa, en este modelo, el consumidor de servicios se comunica con el elemento proxy asociado al productor de servicios. En otras palabras, no existe una conexión directa entre el consumidor de servicios y el productor de servicios seleccionado. La conexión pasa por un proxy. Además, en este modelo, el proxy tiene la opción de cambiar el productor seleccionado basándose en los criterios de equilibrio de carga u otros criterios. El proxy usa el campo de reclamación de audiencia del token de acceso para seleccionar un productor de servicios diferente.

10 En otros aspectos, un elemento proxy puede residir en la NRF, en el consumidor de servicios de NF y/o en uno o más productores de servicios de NF.

15 Además del criterio de equilibrio de carga que se utiliza para los criterios de selección del productor de servicios, se pueden utilizar otros criterios tales como la disponibilidad (p. ej., el productor de servicios no está disponible o es defectuoso) y/o el mantenimiento planificado (p. ej., para la actualización del software). Además, en algunos aspectos, los criterios de selección comprenden uno o más criterios de política configurados por el operador.

20 Por lo tanto, debe insistirse de nuevo en que los diversos aspectos descritos en la presente memoria se presentan solo a modo de ejemplo ilustrativo y no se deben considerar como una limitación del alcance de las reivindicaciones. Por ejemplo, aspectos alternativos pueden usar diferentes configuraciones de sistema de comunicación, configuraciones de equipo de usuario, configuraciones de estación base, procesos para proporcionar y utilizar pares de claves, protocolos de mensajería y formatos de mensaje de los descritos anteriormente en el contexto de los aspectos ilustrativos. Estos y otros muchos aspectos alternativos dentro del alcance de las reivindicaciones adjuntas serán fácilmente apreciables para los expertos en la técnica.

25

REIVINDICACIONES

1. Aparato que comprende medios para realizar:
5 recepción en una entidad (704) de autorización en un sistema de comunicación que comprende una arquitectura basada en servicios una solicitud de un consumidor (702) de servicios de funciones de red en el sistema de comunicación para acceder a un tipo de servicio de funciones de red determinado;
10 obtención en la entidad (704) de autorización un token de acceso que identifique (i) la entidad de autorización y (ii) una pluralidad de productores de servicios de funciones de red para el tipo de servicio de funciones de red dado y direcciones para la pluralidad de productores de servicios de funciones de red; y
15 envío del token de acceso desde la entidad (704) de autorización al consumidor (702) de servicios de funciones de red.
2. El aparato de la reivindicación 1, que comprende además la entidad (704) de autorización que autentica al consumidor (702) de servicios de funciones de red en una etapa de descubrimiento antes de recibir la solicitud del consumidor (702) de servicios de funciones de red.
- 20 3. El aparato de la reivindicación 1, en donde la obtención comprende además recuperar del almacenamiento el token de acceso generado durante una etapa de descubrimiento.
- 25 4. El aparato de cualquiera de las reivindicaciones anteriores, en donde la entidad (704) de autorización es una función de repositorio de funciones de red, el consumidor (702) de servicios de funciones de red es una primera función de red y la pluralidad de productores de servicios son otras dos o más funciones de red.
5. El aparato de cualquiera de las reivindicaciones anteriores, en donde el token de acceso comprende un formato de token web de notación de objetos de JavaScript.
- 30 6. El aparato de la reivindicación 5, en donde la pluralidad de productores de servicios de funciones de red para el tipo de servicio dado se identifican en un campo de reclamación de audiencia del formato de token web de notación de objetos de JavaScript.
- 35 7. El aparato de cualquiera de las reivindicaciones anteriores, en donde el medio comprende:
al menos un procesador; y
al menos una memoria que incluye un código de programa informático, estando la al menos una memoria y el código de programa informático configurados para provocar, con el al menos un procesador, el funcionamiento del aparato.
- 40 8. Aparato que comprende medios para realizar:
45 envío desde un consumidor (702) de servicios de funciones de red en un sistema de comunicación que comprende una arquitectura basada en servicios a una entidad (704) de autorización en el sistema de comunicación una solicitud de acceso a un tipo de servicio de función de red dado;
recepción en el consumidor (702) de servicios un token de acceso de la entidad (704) de autorización, en donde el token de acceso identifica (i) la entidad de autorización y (ii) una pluralidad de productores de servicios de funciones de red en el sistema de comunicación para el tipo de servicio de función de red dado y direcciones para la pluralidad de productores de servicios de
50 funciones de red; y
selección de uno de la pluralidad de productores de servicios de funciones de red a partir del token de acceso basándose en uno o más criterios de selección.
- 55 9. Aparato que comprende medios para realizar:
60 recepción de un token de acceso en un elemento proxy en un sistema de comunicación que comprende una arquitectura basada en servicios, en donde el token de acceso identifica (i) una entidad de autorización en el sistema de comunicación y (ii) una pluralidad de productores de servicios de funciones de red en el sistema de comunicación para un tipo y direcciones de servicio de funciones de red dados, en donde la entidad (704) de autorización obtiene el token de acceso en respuesta a una solicitud de un consumidor (702) de servicios de funciones de red en el sistema de comunicación para acceder al tipo de servicio de funciones de red dado; y
selección en el elemento proxy de uno de la pluralidad de productores de servicios de funciones de red a partir del token de acceso basándose en uno o más criterios de selección.
- 65

- 5
10. El aparato de la reivindicación 9, que comprende además, cuando el elemento proxy reside entre la entidad de autorización y el consumidor (702) de servicios de funciones de red, que el elemento de proxy envía al consumidor (702) de servicios de funciones de red información de identificación para el productor de servicios de funciones de red seleccionado.
- 10
11. El aparato de la reivindicación 9, que comprende además, cuando el elemento proxy reside entre la entidad (704) de autorización y el consumidor (702) de servicios de funciones de red, que el elemento proxy selecciona posteriormente otro productor de servicios de funciones de red a partir del token de acceso basándose en un cambio en al menos uno de los uno o más criterios de selección.
- 15
12. El aparato de la reivindicación 11, en donde el criterio de selección en el que se produce el cambio comprende uno o más de: un criterio de equilibrio de carga; un criterio de disponibilidad; y un criterio de mantenimiento.
13. El aparato de cualquiera de las reivindicaciones 8 a 12, en donde el medio comprende:
- al menos un procesador; y
 - al menos una memoria que incluye un código de programa informático, estando la al menos una memoria y el código de programa informático configurados para provocar, con el al menos un procesador, el funcionamiento del aparato.

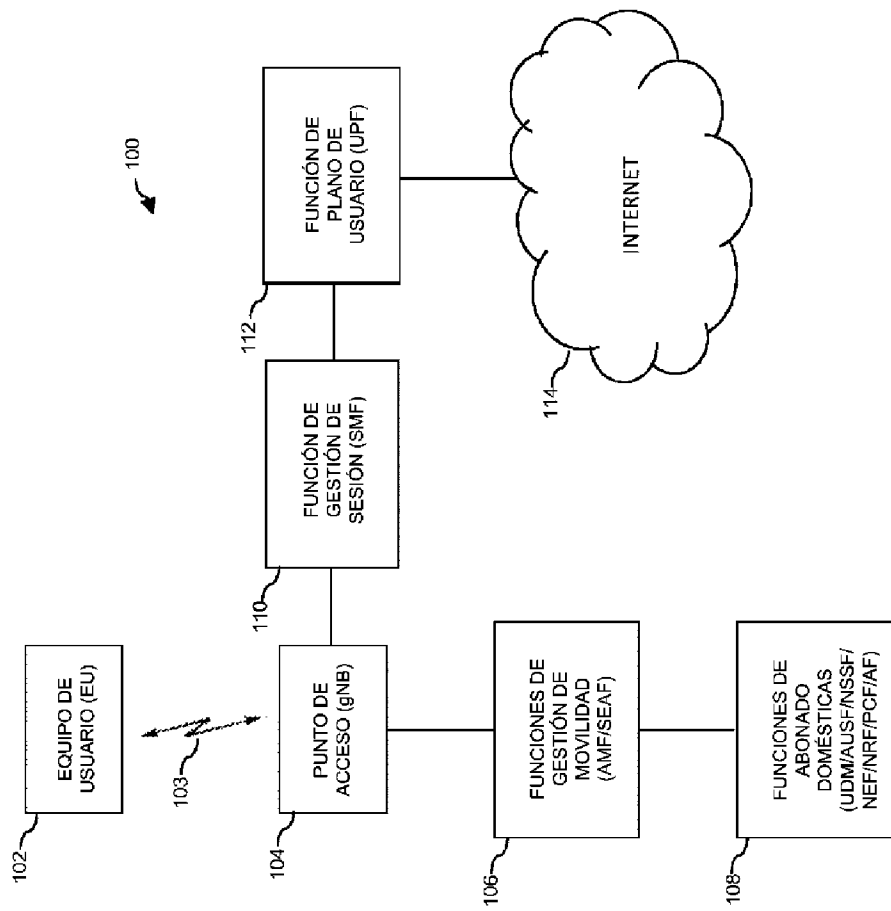


Figura 1

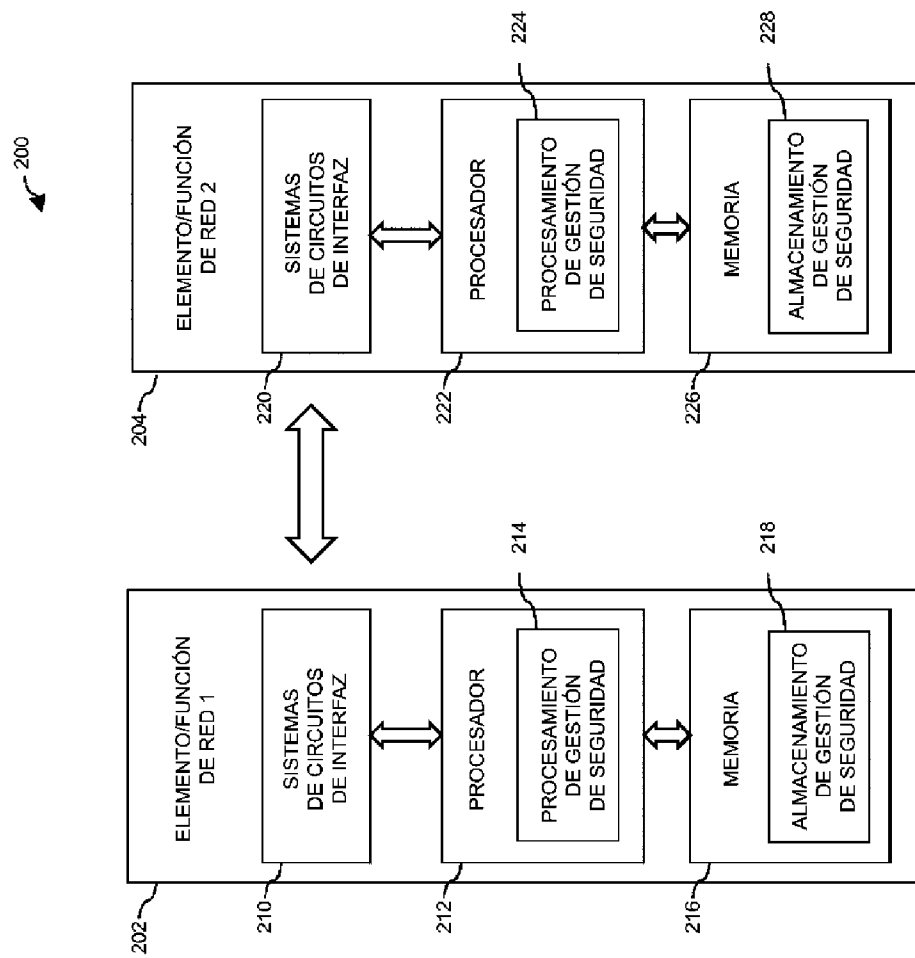


Figura 2

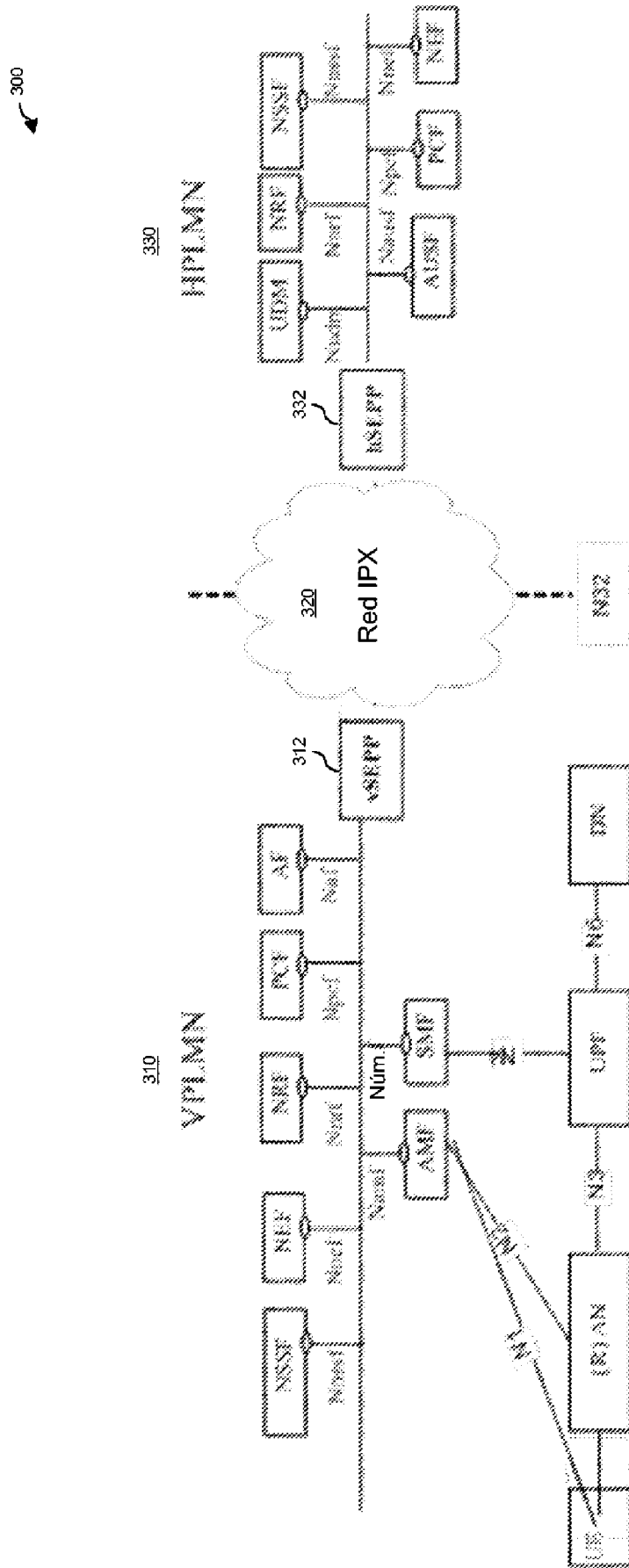


Figure 3

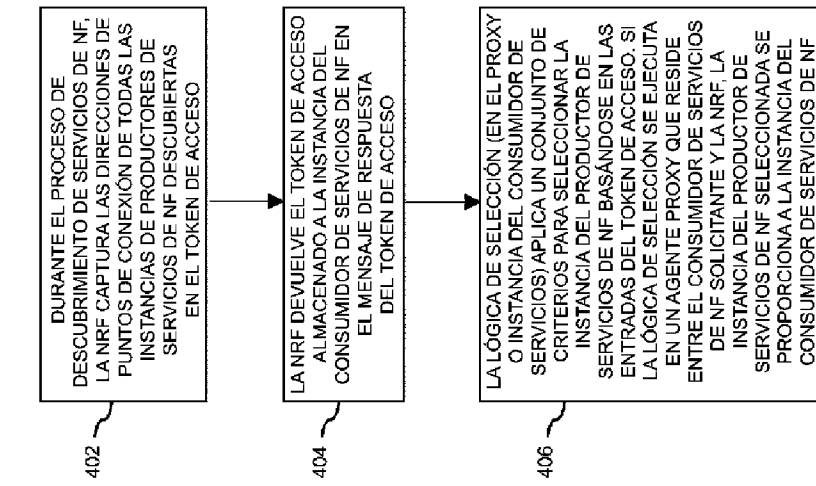


Figura 4

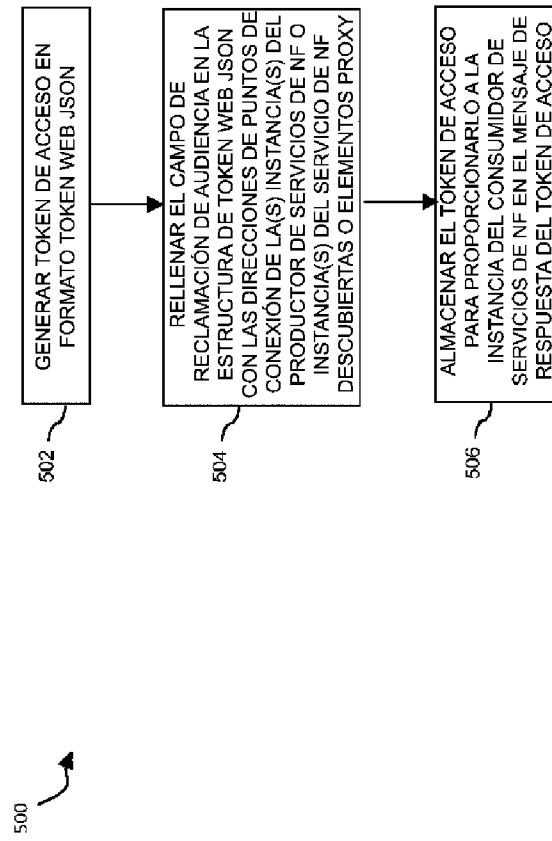


Figura 5

600

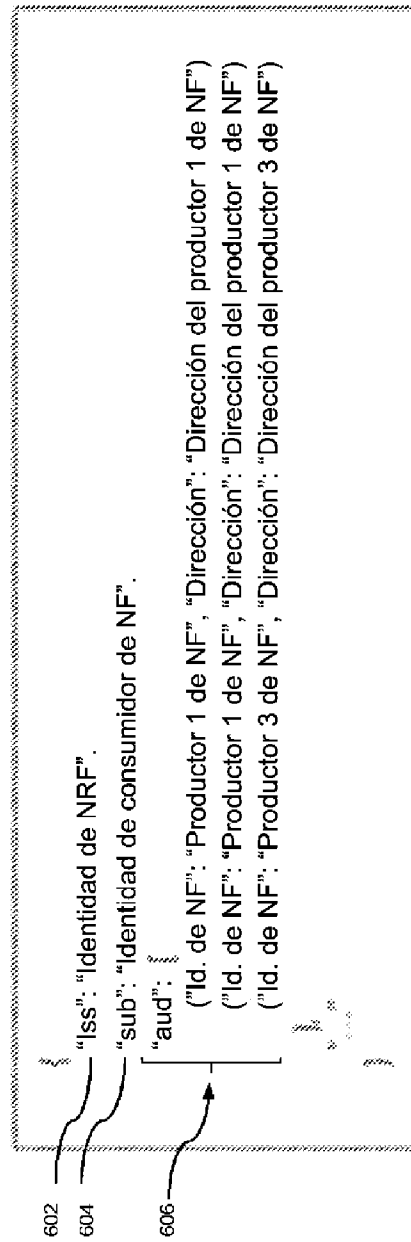


Figura 6

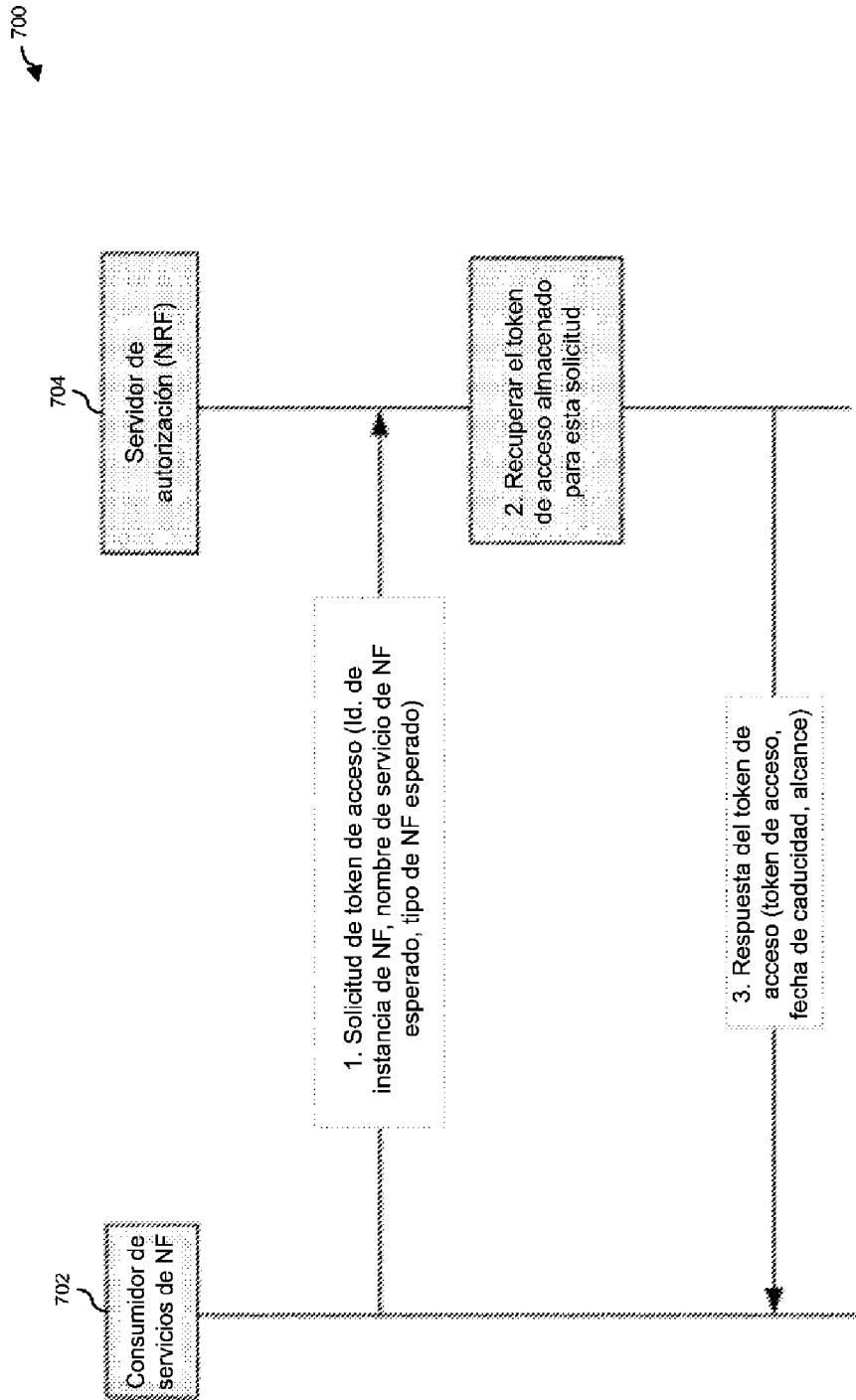


Figura 7