

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 931 775**

51 Int. Cl.:

H04W 48/18	(2009.01)
H04W 12/02	(2009.01)
H04W 48/16	(2009.01)
H04W 60/00	(2009.01)
H04W 12/72	(2011.01)
H04W 12/75	(2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **15.01.2019 PCT/EP2019/050931**

87 Fecha y número de publicación internacional: **18.07.2019 WO19138133**

96 Fecha de presentación y número de la solicitud europea: **15.01.2019 E 19701793 (2)**

97 Fecha y número de publicación de la concesión europea: **26.10.2022 EP 3639571**

54 Título: **Selección de instancia de función de red**

30 Prioridad:

15.01.2018 WO PCT/CN2018/072579

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

02.01.2023

73 Titular/es:

**TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)
(100.0%)
164 83 Stockholm, SE**

72 Inventor/es:

**WANG, CHENG;
CASTELLANOS ZAMORA, DAVID;
TORVINEN, VESA y
NAKARMI, PRAJWOL KUMAR**

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 931 775 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

Selección de instancia de función de red

Campo Técnico

5 La presente solicitud se refiere en general a una red de comunicación inalámbrica, y más particularmente se refiere a la selección de una instancia de función de red en una red de comunicación inalámbrica.

Antecedentes

10 La red central (CN) de próxima generación (5G) utilizará una arquitectura basada en servicios que aprovecha las interacciones basadas en servicios entre las funciones de red (NF) de CN. En este sentido, las NF posibilitan que otras NF autorizadas accedan a sus servicios. Alternativamente, o además de las interfaces predefinidas que se definen entre los elementos de red, una instancia de una NF que necesita consumir un servicio de cierto tipo consulta una, así llamada función de repositorio de red (NRF) para descubrir y comunicarse con una instancia de otra NF que proporciona ese determinado tipo de servicio.

15 En particular, las NF pueden asumir un rol de proveedor como un proveedor de un servicio (NFp) y/o un rol de consumidor como un consumidor de un servicio (Nfc). Se inicia una instancia de una NFp y se registra a sí misma en el NRF. Este registro permite que la NRF sepa que la instancia de la NFp existe. En un momento posterior, una instancia de una Nfc que necesita utilizar un servicio específico ejecuta un procedimiento llamado descubrimiento hacia la NRF. En caso de que la NRF tenga una instancia registrada de la NFp que coincida con esta solicitud de descubrimiento, la NRF proporciona a la instancia de la Nfc la información necesaria para establecer la comunicación con una instancia descubierta de la NFp. Esta información puede ser, por ejemplo, la dirección IP y el puerto de la instancia de NFp.

20 La arquitectura basada en servicios habilita ventajosamente una mayor flexibilidad y velocidad en el desarrollo de nuevos servicios CN, ya que es posible conectarse a otros componentes sin introducir nuevas interfaces. La arquitectura basada en servicios también introduce la posibilidad de utilizar interfaces de programación de aplicaciones (API) basándose en tecnología web que facilitan el desarrollo, ya que las bibliotecas y las herramientas de desarrollo para dicha tecnología ya están ampliamente disponibles. No obstante, la arquitectura basada en servicios presenta desafíos para el descubrimiento y la selección de NF, especialmente a medida que aumenta la cantidad de abonados en la red.

25 El documento C4-173259, Pseudo-CR sobre Requisitos para el descubrimiento y selección de servicios NF, da a conocer los requisitos de 3GPP para el descubrimiento y selección de funciones de red. El descubrimiento de servicios de NF posibilita que una NF descubra una instancia o instancias de NF que proporcionan el servicio o servicios de NF esperados. El descubrimiento de servicios de NF se implementa mediante el soporte del descubrimiento de NF utilizando la NRF (Función de repositorio de red). La selección de NF consiste en seleccionar una instancia de NF entre la instancia o instancias de NF descubiertas durante el descubrimiento del servicio de NF. La selección de NF es implementada por el solicitante de NF, por ejemplo, la selección SMF es compatible con AMF.

30 S3-173140, el movimiento del UE que maneja SUCI a la cláusula SUCI, da a conocer que el UE incluirá un identificador oculto de suscripción (SUCI) solamente en los mensajes 5G NAS si el UE está enviando un mensaje de solicitud de registro del tipo "registro inicial" a una PLMN para que el UE aún no tenga un 5G-GUTI, el UE incluirá un SUCI en el mensaje de solicitud de registro. También da a conocer algunas excepciones en las que el UE nunca generará un SUCI utilizando un "esquema nulo".

35 S3-172356, la funcionalidad SIDF, da a conocer una funcionalidad de revelación de identificador de suscripción (SIDF) que es responsable de revelar el SUPI del SUCI.

Compendio

40 La presente invención define un método realizado por un equipo de red según la reivindicación 1 independiente y una entidad de red correspondiente según la reivindicación 14 independiente. La presente invención define otro método realizado por un equipo de red según la reivindicación 6 independiente y una entidad de red correspondiente según la reivindicación 15 independiente. La presente invención también define un método realizado por un equipo de usuario según la reivindicación 11 independiente y un equipo de usuario correspondiente según la reivindicación 16 independiente, así como programas informáticos según las reivindicaciones 17 y 18 independientes y un portador según la reivindicación 19 independiente. Las realizaciones preferidas están definidas por las reivindicaciones dependientes.

45 Las realizaciones de la presente memoria incluyen un método realizado por un equipo de red en una red de comunicación inalámbrica. El método comprende la recepción al menos de una parte de un identificador oculto de suscripción para un abonado, en donde el identificador oculto de suscripción contiene un identificador permanente de suscripción oculta para el abonado. La recepción de al menos una parte del identificador oculto de suscripción indica un código de subdominio. El código de subdominio indica un determinado subdominio, de entre múltiples

- 5 subdominios de una red doméstica del abonado, al que está asignado el abonado. El método también puede incluir la determinación, basándose en el código de subdominio y de entre varias instancias de una función de red de proveedor en la red doméstica asignada respectivamente para proporcionar un servicio a ser consumido por abonados asignados a diferentes subdominios, una instancia de la función de red de proveedor para proporcionar el servicio a ser consumido por el abonado.
- En algunas realizaciones, la determinación de la instancia de la función de red de proveedor para proporcionar el servicio a ser consumido por el abonado también se basa en un identificador de red doméstica.
- 10 En algunas realizaciones, el método también comprende la recepción de una solicitud de descubrimiento para descubrir una o más instancias de la función de red de proveedor en la red doméstica para proporcionar el servicio a ser consumido por el abonado y responder a la solicitud de descubrimiento con la instancia seleccionada de la función de red de proveedor.
- En algunas realizaciones, el equipo de red implementa una función de repositorio de red, NRF.
- 15 En algunas realizaciones, el método también puede comprender la recepción de información que configura el equipo de red para asociar el código de subdominio con una o más instancias de la función de red de proveedor asignadas para proporcionar el servicio a ser consumido por abonados asignados a cierto subdominio. En una o más de tales realizaciones, por ejemplo, la información incluye cierto código de subdominio e información de enrutamiento para una o más instancias de la función de red de proveedor, de tal manera que la información configura el equipo de red para asociar el código de subdominio con la información de enrutamiento. En algunas realizaciones a este respecto,
- 20 la información de enrutamiento es un Protocolo de Internet, una dirección IP, un nombre de servidor, un nombre de dominio o un identificador de recurso uniforme, de la instancia seleccionada.
- En algunas realizaciones, diferentes subdominios de la red doméstica están asociados con diferente información de enrutamiento, y el código de subdominio es un identificador asociado con la información de enrutamiento para cierto subdominio.
- 25 En algunas realizaciones, la determinación del código de subdominio comprende la determinación del código de subdominio a partir de un campo en al menos una parte del identificador oculto de suscripción, en donde el campo es un campo de código de subdominio dedicado a indicar un código de subdominio.
- En algunas realizaciones, la función de red de proveedor es una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.
- 30 Las realizaciones también incluyen un método realizado por un equipo de red en una red de comunicación inalámbrica según otras realizaciones. El método incluye la obtención de un código de subdominio que indica un cierto subdominio, de entre múltiples subdominios de una red doméstica de un abonado, al que está asignado el abonado. El método también puede incluir la transmisión de información que configura otros equipos de red para asociar el código de subdominio con una determinada instancia de una función de red de proveedor entre múltiples instancias de la función de red de proveedor en la red doméstica que se asignan respectivamente para proporcionar un servicio a ser consumido por abonados asignados a diferentes subdominios de la red doméstica.
- 35 En algunas realizaciones, la información incluye el código de subdominio y la información de enrutamiento para la instancia determinada, de tal manera que la información configura el otro equipo de red para asociar el código de subdominio con la información de enrutamiento. En una o más de tales realizaciones, la información de enrutamiento es un Protocolo de Internet, una dirección IP, un nombre de servidor, un nombre de dominio o un identificador de recurso uniforme, de la instancia determinada.
- 40 En algunas realizaciones, el equipo de red implementa una función de operación y mantenimiento, la instancia determinada de la función de red de proveedor, o un proxy para la instancia determinada de la función de red de proveedor.
- 45 En algunas realizaciones, la función de red de proveedor es una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.
- En algunas realizaciones, el otro equipo de red implementa una función de repositorio de red.
- En algunas realizaciones, diferentes subdominios de la red doméstica están asociados con diferente información de enrutamiento, y el código de subdominio es un identificador asociado con la información de enrutamiento para cierto subdominio.
- 50 En algunas realizaciones, el método también comprende la generación de un campo que indica el código del subdominio. En este caso, el campo puede ser un campo de código de subdominio dedicado a indicar un código de subdominio. En tal caso, la información que configura los otros equipos de la red puede incluir el campo.
- Las realizaciones incluyen además un método realizado por un equipo de red en una red de comunicación inalámbrica según otras realizaciones más. El método incluye la obtención de un código de subdominio que indica

un cierto subdominio, de entre múltiples subdominios de una red doméstica de un abonado, al que está asignado el abonado. El método también puede incluir la transmisión de información que configura un equipo de usuario de abonado, o una tarjeta de circuito integrado asociada con el abonado, con el código de subdominio obtenido.

5 En algunas realizaciones, el equipo de red implementa una función de operación y mantenimiento, una instancia de una función de red de proveedor en la red doméstica que va a proporcionar o es capaz de proporcionar un servicio a ser consumido por el abonado, o un proxy para uno o más instancias de la función de red de proveedor. Por ejemplo, la función de red de proveedor puede ser una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.

10 En algunas realizaciones, diferentes subdominios de la red doméstica están asociados con diferente información de enrutamiento, y el código de subdominio es un identificador asociado con la información de enrutamiento para cierto subdominio.

15 En algunas realizaciones, el método también puede incluir la generación de un campo que indica el código del subdominio. En una o más realizaciones, el campo es un campo de código de subdominio dedicado a indicar un código de subdominio. En este caso, la transmisión de la información puede comprender la transmisión del campo al equipo de usuario o a la tarjeta de circuito integrado.

20 Las realizaciones también incluyen un método realizado por un equipo de usuario o una tarjeta de circuito integrado asociada con un abonado. El método comprende la recepción, desde un equipo de red en una red de comunicación inalámbrica, de información que configura el equipo de usuario o la tarjeta de circuito integrado con un código de subdominio que indica un determinado subdominio, de entre múltiples subdominios de una red doméstica del abonado, al que está asignado el abonado. En algunas realizaciones, el método también puede comprender la transmisión de un mensaje que incluye un identificador oculto de suscripción. En algunas realizaciones, el identificador oculto de suscripción contiene un identificador permanente de suscripción oculta para el abonado e indica el código de subdominio.

25 En algunas realizaciones, el equipo de red implementa una función de operación y mantenimiento, una instancia de una función de red de proveedor en la red doméstica que va a proporcionar o es capaz de proporcionar un servicio a ser consumido por el abonado, o un proxy para uno o más instancias de la función de red de proveedor.

En algunas realizaciones, la función de red de proveedor es una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.

30 En algunas realizaciones, diferentes subdominios de la red doméstica están asociados con diferente información de enrutamiento, y en donde el código de subdominio es un identificador asociado con la información de enrutamiento para cierto subdominio.

En algunas realizaciones, la recepción del código de subdominio comprende la recepción de un campo que indica el código de subdominio. En una o más realizaciones, el campo es un campo de código de subdominio dedicado a indicar un código de subdominio.

35 En algunas realizaciones, el método también puede comprender la generación del identificador oculto de suscripción para incluir un campo que indique el código de subdominio.

40 Las realizaciones también pueden incluir aparatos, programas informáticos y portadores correspondientes. Por ejemplo, algunas realizaciones de la presente memoria incluyen equipos de red configurados para su uso en una red de comunicación inalámbrica. El equipo de red puede configurarse (por ejemplo, mediante circuitos de comunicación y circuitos de procesamiento) para recibir al menos una parte de un identificador oculto de suscripción para un abonado. La recepción de al menos una parte del identificador oculto de suscripción indica un código de subdominio. El código de subdominio indica un determinado subdominio, de entre múltiples subdominios de una red doméstica del abonado, al que está asignado el abonado. El equipo de red también puede configurarse para determinar, basándose en el código de subdominio y de entre múltiples instancias de una función de red de proveedor en la red doméstica asignada respectivamente para proporcionar un servicio a ser consumido por abonados asignados a diferentes subdominios, una instancia de la función de red de proveedor para proporcionar el servicio a ser consumido por el abonado.

45 Las realizaciones pueden incluir además equipos de red en una red de comunicación inalámbrica según otras realizaciones. El equipo de red puede configurarse (por ejemplo, mediante circuitos de comunicación y circuitos de procesamiento) para obtener un código de subdominio que indique un cierto subdominio, entre varios subdominios de una red doméstica de un abonado, al que está asignado el abonado. El equipo de red también puede configurarse para transmitir información que configura otro equipo de red para asociar el código de subdominio con una determinada instancia de una función de red de proveedor entre múltiples instancias de la función de red de proveedor en la red doméstica que se asignan respectivamente para proporcionar un servicio a ser consumido por abonados asignados a diferentes subdominios de la red doméstica.

55 Las realizaciones también incluyen equipos de red en una red de comunicación inalámbrica según otras

realizaciones más. El equipo de red puede configurarse (por ejemplo, mediante circuitos de comunicación y circuitos de procesamiento) para obtener un código de subdominio que indique un cierto subdominio, entre múltiples subdominios de una red doméstica de un abonado, al que está asignado el abonado. El equipo de red también puede estar configurado para transmitir información que configura un equipo de usuario de abonado, o una tarjeta de circuito integrado asociada al abonado, con el código de subdominio obtenido.

Las realizaciones también incluyen un equipo de usuario o una tarjeta de circuito integrado asociada con un abonado. El equipo de usuario o la tarjeta de circuito integrado está configurado (por ejemplo, mediante circuitos de comunicación y circuitos de procesamiento) para recibir, desde el equipo de red en una red de comunicación inalámbrica, información que configura el equipo de usuario o la tarjeta de circuito integrado con un código de subdominio que indica un determinado subdominio, de entre múltiples subdominios de una red doméstica del abonado, al que está asignado el abonado. En algunas realizaciones, el equipo de usuario o la tarjeta de circuito integrado se configura además para transmitir un mensaje que incluye un identificador oculto de suscripción. En algunas realizaciones, el identificador oculto de suscripción contiene un identificador permanente de suscripción oculta para el abonado e indica el código de subdominio.

Breve descripción de los dibujos

La fig. 1 es un diagrama de bloques de una red de comunicación inalámbrica según algunas realizaciones.

La fig. 2A es un diagrama de bloques de un identificador oculto de suscripción según algunas realizaciones.

La fig. 2B es un diagrama de bloques de un identificador oculto de suscripción según otras realizaciones.

La fig. 2C es un diagrama de bloques de un identificador oculto de suscripción según otras realizaciones más.

La fig. 3 es un diagrama de bloques de una red de comunicación inalámbrica según algunas realizaciones para configurar equipos de red y/o equipos de usuario/ICC.

La fig. 4 es un diagrama de bloques de una red 5G según algunas realizaciones.

La fig. 5 es un diagrama de flujo de llamadas para el procesamiento realizado por un 5G UE y funciones de red para la selección de instancias de función de red de proveedor según algunas realizaciones.

La fig. 6 es un diagrama de flujo de llamadas para el procesamiento realizado por un 5G UE y funciones de red para la selección de instancias de función de red de proveedor según otras realizaciones.

La fig. 7A es un diagrama de flujo lógico de un método realizado por un equipo de red según algunas realizaciones.

La fig. 7B es un diagrama de flujo lógico de un método realizado por un equipo de red según otras realizaciones.

La fig. 8 es un diagrama de flujo lógico de un método realizado por un equipo de red según otras realizaciones.

La fig. 9 es un diagrama de flujo lógico de un método realizado por un equipo de red según aún otras realizaciones.

La fig. 10 es un diagrama de flujo lógico de un método realizado por el equipo del usuario según algunas realizaciones.

La fig. 11A es un diagrama de bloques del equipo de red según algunas realizaciones.

La fig. 11B es un diagrama de bloques del equipo de red según otras realizaciones.

La fig. 12A es un diagrama de bloques del equipo de red según algunas realizaciones.

La fig. 12B es un diagrama de bloques del equipo de red según otras realizaciones.

La fig. 13A es un diagrama de bloques del equipo de red según algunas realizaciones.

La fig. 13B es un diagrama de bloques del equipo de red según otras realizaciones.

La fig. 14A es un diagrama de bloques del equipo de usuario según algunas realizaciones.

La fig. 14B es un diagrama de bloques del equipo de usuario según otras realizaciones.

Descripción detallada

La fig. 1 muestra una red 10 de comunicación inalámbrica según algunas realizaciones. La red 10 incluye una o más redes 14 de acceso por radio (RAN) que conectan de forma inalámbrica el equipo 12 de usuario a una o más redes

centrales (CN) 16, por ejemplo, de una o más redes móviles terrestres públicas (PLMN), incluyendo una PLMN doméstica asociada con el equipo 12 de usuario. Las CN 16, a su vez, conectan el equipo 12 de usuario a una o más redes 18 de datos, por ejemplo, Internet, una red telefónica pública conmutada (PSTN), etc.

5 El equipo 12 de usuario, como se muestra, puede incluir una tarjeta de circuito integrado (ICC) 12A. La ICC 12A puede ser, por ejemplo, una tarjeta de circuito integrado universal (UICC) que ejecuta una aplicación de módulo de identidad de abonado universal (USIM). Independientemente, el equipo 12 de usuario y/o la ICC 12A pueden estar asociados con un determinado abonado 13. El equipo 12 de usuario y/o la ICC 12A pueden, por ejemplo, almacenar, acceder o utilizar de otro modo un determinado identificador de suscripción que identifique una suscripción de determinado abonado 13, por ejemplo, a una red doméstica tal como una PLMN doméstica. El identificador de suscripción o un derivado del mismo se puede utilizar para identificar y autenticar al abonado 13 en la red 10 de comunicación inalámbrica. Cuando el identificador de suscripción se asigna al abonado 13 a largo plazo o de forma permanente, se puede hacer referencia al identificador de suscripción como un identificador permanente de suscripción (SUPI) 20, que se muestra en la fig. 1 almacenado en la ICC 12A. En realizaciones en las que la red 10 es una red 5G, el identificador de suscripción puede ser un identificador 5G globalmente único que toma la forma de una identidad de abonado móvil internacional (IMSI) o un identificador de acceso a la red (NAI).

15 Las CN 16 en algunas realizaciones tienen una arquitectura basada en servicios que aprovecha las interacciones basadas en servicios entre funciones de red (NF) de CN. Un equipo de red puede implementar una NF, bien como un elemento de red en hardware dedicado, bien como una instancia de software que se ejecuta en hardware dedicado o bien como una función virtualizada instanciada en una plataforma apropiada, por ejemplo, en una infraestructura de nube. Cuando el sistema 10 es un sistema 5G, por ejemplo, las NF en el plano de control pueden incluir una función de gestión de acceso y movilidad (AMF), una función de gestión de sesión (SMF), una función de control de políticas (PCF), una función de servidor de autenticación (AUSF), una función de gestión unificada de datos (UDM), una función de revelación de identificador de abonado (SIDF), etc.

20 Una NF puede prestar sus servicios a otras NF autorizadas que consumen esos servicios para un abonado. Por lo tanto, una NF puede asumir un rol de proveedor como proveedor de un servicio (es decir, NF de proveedor) y/o un rol de consumidor como consumidor de un servicio (es decir, NF de consumidor). Por ejemplo, en una red 5G, una AUSF puede asumir un rol de proveedor para proporcionar servicios de autenticación a una AMF (asumiendo un rol de consumidor) para la autenticación de un abonado. En cualquier caso, una NF que necesita consumir un determinado tipo de servicio inicia o realiza el descubrimiento de una instancia de NF que puede proporcionar ese determinado tipo de servicio. Con una NF de proveedor descubierta, la NF de consumidor puede consumir el servicio de la NF de proveedor.

25 Sin embargo, algunos contextos complican este enfoque de arquitectura basada en servicios. Por ejemplo, la CN 16 de la red doméstica de un abonado puede implementar múltiples instancias de una determinada NF, por ejemplo, con el fin de equilibrar el procesamiento, almacenamiento u otras demandas de recursos en las múltiples instancias de la NF y/o para proporcionar servicios de forma más rápida y/o eficiente. Cuando una determinada NF actúa como una NF de proveedor al proporcionar un servicio a una instancia de una NF de consumidor, esto significa que múltiples instancias de NF de proveedor en la red doméstica del abonado pueden ser candidatas para proporcionar el servicio a la instancia de NF de consumidor. Con esta complejidad añadida a la arquitectura basada en servicios, algunas realizaciones en la presente memoria abordan cómo seleccionar cuál de las múltiples instancias de NF de proveedor proporcionará el servicio a la instancia de NF de consumidor que consumirá el servicio para el abonado 13.

30 La fig. 1 a este respecto muestra una instancia 22 de NF de consumidor (por ejemplo, una instancia de una AMF o AUSF). La instancia 22 de NF de consumidor necesita consumir un servicio (por ejemplo, de un cierto tipo) para el abonado 13 asociado con el equipo 12 de usuario y/o la ICC 12A. La red doméstica de abonado implementa múltiples instancias 24-1, 24-2, ..24-M de NF de proveedor (por ejemplo, múltiples instancias de una función UDM, una SIDF, una AUSF, etc.) que son candidatas para proporcionar este servicio (por ejemplo, del tipo determinado) a la instancia 22 de NF de consumidor que va a consumir el servicio para el abonado 13. El equipo 26 de red está configurado para seleccionar, entre estas múltiples instancias 24-1, 24-2, 24-M de NF de proveedor, una instancia de NF de proveedor para proporcionar el servicio al abonado 13; es decir, para proporcionar el servicio a consumir (por la instancia 22 de NF del consumidor) para el abonado 13. Tal selección en la presente memoria generalmente se refiere al hecho de que el equipo 26 de red determina una instancia de NF de proveedor para proporcionar el servicio a ser consumido por el abonado 13, eligiendo esa instancia de NF de proveedor de las múltiples instancias 24-1, 24-2, 24-M de NF de proveedor que son candidatas para hacerlo.

35 En algunas realizaciones, el equipo 26 de red implementa la instancia 22 de NF de consumidor (es decir, de manera que la instancia 22 de NF de consumidor realiza la selección por sí misma) o un proxy para la instancia 22 de NF de consumidor. En este y otros casos, la selección del equipo de red puede ser denominada formalmente selección NF, o puede realizarse como parte de dicha selección NF formal. En otras realizaciones, el equipo 26 de red implementa una función 28 de repositorio de red (NRF) (es decir, de manera que la función 28 de repositorio de red realiza la selección. En este y otros casos, la selección del equipo de red puede denominarse formalmente descubrimiento de NF, o puede realizarse como parte de dicho descubrimiento formal de NF. En aún otras realizaciones, el equipo 26 de red implementa un proxy para una o más de las instancias de NF de proveedor. Independientemente, el equipo 26 de red según algunas realizaciones en la presente memoria realiza ventajosamente la selección basándose en un

denominado código de subdominio. Es decir, el equipo 26 de red basa aquí su determinación en cuál de las instancias 24-1, 24-2,... 24-M de NF de proveedor va a proporcionar el servicio a consumir para el abonado 13 en un código de subdominio.

5 Más particularmente a este respecto, la red doméstica del abonado, como se muestra en la fig. 1, se divide en múltiples subdominios 30-1, 30-2,... 30-N. Cada uno de los abonados de la red doméstica, incluyendo el abonado 13 asociado con el equipo 12 de usuario y/o la ICC 12A, se asigna a uno o más de los subdominios 30-1, 30-2,... 30-N. Las instancias 24-1, 24-2,... 24-M de NF de proveedor en la red doméstica se asignan a su vez respectivamente para proporcionar un servicio (por ejemplo, de un cierto tipo) para abonados asignados a diferentes subdominios. Es decir, diferentes instancias 24-1, 24-2,... 24-M de NF de proveedor pueden proporcionar el servicio para abonados en diferentes subdominios 30-1, 30-2,... 30-N. Donde $M=N$, por ejemplo, cada una de las instancias de NF de proveedor proporciona el servicio para abonados en uno diferente de los subdominios. Por el contrario, donde $M>N$, algunas de las instancias de NF de proveedor pueden proporcionar el servicio para abonados en el mismo subdominio.

15 Con el fin de seleccionar una instancia de NF de proveedor para proporcionar el servicio para el abonado 13 asociado con el equipo 12 de usuario y/o la ICC 12A, el equipo 26 de red está configurado para seleccionar una instancia de NF de proveedor que se asigna para proporcionar el servicio para los abonados asignados al mismo subdominio que el abonado 13. El equipo 26 de red a este respecto identifica o determina de otro modo un código 32 de subdominio que indica un cierto subdominio, de entre los múltiples subdominios 30-1, 30-2,...30-N de la red doméstica del abonado, al que está asignado el abonado 13. Un código de subdominio como se utiliza en la presente memoria es cualquier información que codifica o indica de otro modo uno determinado de los subdominios 30-1, 30-2,... 30-N, a diferencia de otros subdominios. Después de la determinación del código 32 de subdominio que indica el subdominio al que está asignado el abonado 13, el equipo 26 de red basa su selección de las instancias 24-1, 24-2,... 24-M de NF de proveedor en ese código 32 de subdominio. El equipo 26 de red puede, por ejemplo, realizar la selección según una correspondencia definida o asociación entre códigos de subdominio e instancias 24-1, 24-2,... 24-M de NF de proveedor. En algunas realizaciones, por ejemplo, el equipo 26 de red recibe información (por ejemplo, de una función de operación y mantenimiento, OMF u otro equipo de red) que configura el equipo 26 de red con esta correspondencia o asociación definida.

Basando la selección de instancias de NF del equipo 26 de red en un código de subdominio mejora notablemente la solidez, la eficiencia y/o la flexibilidad de la selección de instancias de NF para el abonado 13. De hecho, dicha selección de instancias de NF es posible incluso en circunstancias en las que el equipo 12 de usuario y/o la ICC 12A oculta el identificador de suscripción (por ejemplo, SUPI 20) de forma inalámbrica para ocultar la identidad del abonado 13 del equipo 26 de red y/o incluso cuando diferentes subdominios están asociados con diferentes rangos de identificadores de suscripción. Por ejemplo, el equipo 12 de usuario y/o la ICC 12A pueden generar un identificador oculto de suscripción (SUCI) que oculta el identificador de suscripción asociado con el abonado 13, por ejemplo, cifrando al menos una parte del identificador de suscripción, como la parte que específicamente identifica al abonado 13. El equipo 12 de usuario y/o la ICC 12A pueden, a continuación, transmitir al menos una parte del SUCI 34 en lugar del propio identificador de suscripción (por ejemplo, en lugar del SUPI 20). El equipo 26 de red puede recibir correspondientemente al menos una parte del SUCI 34, por ejemplo, en un mensaje del equipo 12 de usuario, la ICC 12A u otro equipo de red en la red 10. Incluso en este caso, cuando el identificador de suscripción está oculto, el equipo 26 de red puede, no obstante, determinar el código 32 de subdominio (que indica el subdominio al que está asignado el abonado 13) a partir del SUCI o de la parte 34 de SUCI recibida, por ejemplo, sin necesidad de descifrar o revelar el identificador de suscripción.

En algunas realizaciones, por ejemplo, el SUCI o la parte 34 de SUCI recibida incluye un campo 34A que indica el código 32 de subdominio. El campo 34A puede ser un campo de código de subdominio que está dedicado a indicar un código de subdominio, por ejemplo, en el sentido de que el campo 34A indica exclusivamente un código de subdominio. Alternativamente, el campo 34A puede ser un campo que esté configurado o configurable para (por ejemplo, conjuntamente) indicar un código de subdominio y otra información. En algunas realizaciones, por ejemplo, el campo 34A indica tanto un código de subdominio como información de cifrado que identifica un parámetro en base al cual se cifra o se cifrará el SUCI. En algunas realizaciones, por ejemplo, el campo 34A se puede configurar para indicar tanto el código de subdominio como la información de cifrado mediante la concatenación del código de subdominio con la información de cifrado. Como alternativa o adicionalmente, el campo 34A puede configurarse para indicar tanto el código de subdominio como la información de cifrado indicando el código de subdominio y la información de cifrado en un orden definido, con cero o más delimitadores entre el código de subdominio y la información de cifrado. A continuación, en cualquiera de estos ejemplos, el código de subdominio puede determinarse a partir del campo 34A extrayendo el código de subdominio del campo 34A con el objetivo de separar el código de subdominio de la información de cifrado. Dicha extracción puede implicar dividir el código del subdominio de la información de cifrado y/o aplicar una expresión regular al campo 34A que separa el código del subdominio de la información de cifrado (por ejemplo, entre ellos). Las figs. 2A-2C ilustran algunos ejemplos de estas realizaciones.

Como se muestra en la fig. 2A, la parte 34 de SUCI o SUCI incluye un campo 34B de código de país móvil (MCC), un campo 34C de código de red móvil (MNC) y un campo 34D de número de identificación de suscripción móvil (MSIN) oculto. La SUCI o la parte 34 de SUCI también puede incluir un campo 34E de identificador de esquema de cifrado y/o un campo 34F de identificador de clave pública de red doméstica (HN). El campo 34B MCC en combinación con el campo 34C MNC identifican de forma única un operador de red móvil (portador). El campo 34D

MSIN oculto, una vez revelado, identifica de forma única a un abonado del operador de la red móvil. El campo 34E de identificador del esquema de cifrado identifica un esquema de cifrado que se ha de utilizar o se ha utilizado para cifrar el SUCI o la parte 34 de SUCI (por ejemplo, más particularmente, el campo 34D MSIN oculto). El campo 34F de identificador de clave pública de la red doméstica indica una clave pública de la red doméstica que se ha de utilizar o se ha utilizado para cifrar el SUCI o la parte 34 de SUCI (por ejemplo, más particularmente, el campo 34D MSIN oculto). Además de y/o separado de estos campos, el SUCI o la parte 34 de SUCI según algunas realizaciones también incluye un campo de código de subdominio como campo 34A. El campo 34A de código de subdominio está dedicado a indicar un código de subdominio como se describe en la presente memoria.

Obsérvese que, aunque no se muestra, el código de subdominio también puede agregarse al SUPÍ 20, o proporcionarse por separado en el equipo 12 de usuario y/o la ICC 12A. Cuando se agrega el código de subdominio al SUPÍ 20, el SUPÍ 20 puede utilizar el formato NAI. El código del subdominio se puede agregar a la parte del dominio de la NAI, lo que no requeriría cambios en el formato de la NAI descrito en IETF RFC 4282 o en las especificaciones 3GPP. Ejemplos de dicha codificación pueden ser nombreusuario@SDC.homerealm.example.net o SDC.homerealm.example.net/username@visitedrealm.example.net. Aquí, el "nombre de usuario" corresponde al MSIN y el "dominio" corresponde al MCC+MNC. En la sintaxis NAI del SUCI, el nombre de usuario está cifrado y se incorpora el campo del identificador de clave pública HN y/o el campo de esquema de cifrado.

En otras realizaciones que se muestran en la fig. 2B, por el contrario, el SUCI o la parte 34 de SUCI no incluye un campo dedicado a indicar un código de subdominio. En su lugar, el campo de identificador de clave pública de red doméstica sirve como campo 34A que se puede configurar para indicar tanto un código de subdominio 34A-2 como un identificador 34A-1 de clave pública de red doméstica. El identificador de clave pública de la red doméstica identifica una clave pública de la red doméstica basándose en la cual el SUCI o la parte 34 de SUCI (por ejemplo, más particularmente, el campo 34D MSIN oculto) debe ser o ha sido cifrado.

Algunas realizaciones, por ejemplo, emplean dos contadores, uno para identificar la clave pública HN (por ejemplo, 0x01 en hexadecimal) y otro para indicar el código de subdominio (por ejemplo, 0x05 en hexadecimal). El campo 34A de identificador de clave pública HN equivale, a continuación, a la concatenación de los dos contadores, es decir, 0x0105. Otras realizaciones utilizan una expresión regular que separa el identificador de clave pública HN y el código de subdominio entre sí. Por ejemplo, se puede utilizar una expresión regular "(d)\(d)" sin comillas para dividir un número de 2 dígitos de manera que el primer dígito sea el identificador de clave pública HN y el segundo dígito sea el código de subdominio. Con esa expresión regular, un campo de identificador de clave pública HN con el valor "15" sin comillas daría como resultado 1 que indica el identificador de clave pública HN y 5 como segundo grupo que indica el código de subdominio. Otro ejemplo de una expresión regular que permite caracteres alfanuméricos sería "(d+)-([a-z]+)" sin comillas. Esta expresión regular se puede utilizar de manera que un campo de identificador de clave pública HN con el valor "1-cinco" sin comillas daría como resultado 1 como primer grupo que indica el identificador de clave pública HN y cinco como segundo grupo que indica el código de subdominio, el guión separando los dos. Otro ejemplo más es que el campo de identificador de clave pública HN puede descifrarse utilizando un algoritmo simétrico y una clave secreta que da como resultado un identificador de texto claro de la clave pública HN y el SDC.

En aún otras realizaciones que se muestran en la fig. 2C, el SUCI o la parte 34 de SUCI tampoco incluye un campo dedicado a indicar un código de subdominio. En su lugar, el campo del identificador de esquema de cifrado sirve como campo 34A que se puede configurar para indicar tanto un código 34A-2 de subdominio como un identificador 34A-1 de esquema de cifrado. El identificador 34A-1 de esquema de cifrado identifica un esquema de cifrado basándose en el cual el SUCI o la parte 34 de SUCI (por ejemplo, más particularmente, el campo 34D MSIN oculto) ha de ser o ha sido cifrado. Esto puede implementarse utilizando concatenación u otro formateo como se ha descrito anteriormente con respecto al campo de identificador de clave pública de la red doméstica.

Obsérvese que, en algunas realizaciones, el campo 34A es configurable para indicar tanto un código de subdominio como otra información (por ejemplo, información de cifrado) significa que se permite utilizar el campo 34A de forma flexible para indicar tanto un código de subdominio como otra información, por ejemplo, según un formato definido entendido por el equipo 26 de red y/o el equipo 12 de usuario/ICC 12A. El campo 34A en algunas realizaciones también se puede configurar para indicar solamente la otra información, no el código de subdominio, por ejemplo, según un formato diferente entendido por el equipo 26 de red y/o el equipo 12 de usuario/ICC 12A.

En algunas realizaciones, a continuación, el uso del campo 34A puede seguir siendo específico de la implementación, por ejemplo, de manera que el campo 34A se puede utilizar para indicar el código de subdominio junto con la otra información si o cuando dicho código de subdominio necesita ser señalado. Esto libera cualquier dependencia del equipo 12 de usuario y las NF para soportar varios formatos de SUCI. De hecho, para cualquier red que no implemente múltiples instancias de NF, esas redes no necesitan soportar o implementar un formato de SUCI que indique un código de subdominio. Además, este enfoque específico de la implementación proporciona a los operadores de red flexibilidad y control sobre cómo ocultar la topología de la red, por ejemplo, utilizando expresiones regulares personalizadas. Aún más, este enfoque permite que un operador de red elija de manera flexible implementar una NF autónoma (por ejemplo, SIDF) o NF combinadas (por ejemplo, SIDF ubicada junto con UDM). Aún más, el enfoque específico de la implementación salvaguarda ventajosamente la privacidad del abonado

impidiendo o al menos mitigando la posibilidad de vincular un código de subdominio con un determinado abonado o grupo de abonados.

Independientemente de si un código de subdominio se transmite con el SUCI o la parte 34 de SUCI, o cómo se transmite, indicar los subdominios 30-1, 30-2,... 30-N utilizando códigos de subdominio habilita los subdominios en algunas realizaciones que se han de definir y/o indicar basándose en cualquier tipo de criterio (por ejemplo, basándose en características/responsabilidades físicas, lógicas, funcionales o de otro tipo asociadas con los subdominios). Alternativamente, en otras realizaciones, la indicación de los subdominios 30-1, 30-2,... 30-N que utilizan códigos de subdominio posibilita que los subdominios se definan y/o indiquen arbitrariamente (por ejemplo, al azar o según la preferencia del operador de red).

En algunas realizaciones, por ejemplo, se asignan diferentes subconjuntos de abonados a diferentes subdominios 30-1, 30-2,... 30-N, por ejemplo, de manera que se asignen diferentes instancias de NF de proveedor para proporcionar el servicio a diferentes subconjuntos de los abonados de la red doméstica. Cuando la NF de proveedor es una UDM, por ejemplo, la red 10 puede implementar múltiples instancias de UDM, cada una de las cuales almacena datos de un subconjunto diferente de abonados. Tal puede ser el caso, por ejemplo, cuando la red doméstica tiene un gran número de abonados (por ejemplo, varios millones o incluso miles de millones de abonados). A pesar de la asignación de ciertos abonados a ciertos subdominios, el equipo 26 de red puede determinar el código de subdominio que indica a qué subdominio se asigna un abonado independientemente o sin tener en cuenta la determinación del identificador de suscripción (por ejemplo, SUPi) que identifica ese abonado. De hecho, en algunas realizaciones, los diferentes subdominios se indican mediante diferentes códigos de subdominio específicos del operador de red y/o generados aleatoriamente, por ejemplo, los códigos de subdominio son valores numéricos generados aleatoriamente tales como 12382, 88274, 93422145, etc. A continuación, en estas y otras realizaciones, el equipo 26 de red puede determinar un código de subdominio del SUCI o de la parte 34 de SUCI (por ejemplo, leyendo el campo 34A), incluso si el identificador de suscripción está oculto en el SUCI o en la parte de SUCI (por ejemplo, en el campo 34D MSIN oculto).

De manera similar, en otras realizaciones, diferentes subdominios de la red doméstica pueden corresponder a diferentes ubicaciones geográficas o lógicas, por ejemplo, de la red doméstica. En este caso, un código de subdominio puede ser un identificador de una ubicación geográfica o lógica con la que se corresponde un determinado subdominio. Como alternativa o adicionalmente, un código de subdominio puede basarse en una ubicación geográfica o en la ubicación/topología lógica de una red, por ejemplo, una cadena alfanumérica tal como "Estocolmo-kista-2", "Gotemburgo-5", "Lat:59.3293, Longitud: 18,0686", etc.

En aún otras realizaciones, diferentes subdominios de la red doméstica pueden corresponder a diferentes segmentos o subredes de la red doméstica. En este caso, un código de subdominio puede ser un identificador de un determinado segmento o subred con el que se corresponde un determinado subdominio, por ejemplo, una cadena alfanumérica tal como "segmento-1", "red_7", etc. Alternativa o adicionalmente, un código de subdominio puede basarse en cualquier otra información de despliegue de red.

En aún otras realizaciones, diferentes subdominios de la red doméstica pueden estar asociados con diferente información de enrutamiento (para instancias de proveedor de NF asignadas a diferentes subdominios), por ejemplo, diferentes direcciones IP. En este caso, un código de subdominio puede ser un identificador asociado con la información de enrutamiento para un determinado subdominio y/o para una instancia de proveedor de NF asignada a un determinado subdominio, por ejemplo, una cadena alfanumérica tal como "10.10.1.192" mostrando la dirección IP. Como alternativa o adicionalmente, un código de subdominio puede basarse en una referencia a la información de enrutamiento de una instancia de proveedor de NF asignada a un determinado subdominio, por ejemplo, una cadena alfanumérica tal como "AUSF-1" que se refiere a la dirección IP de un cierta instancia AUSF.

En otras realizaciones, cada subdominio de la red doméstica puede estar asociado con uno o más rangos de identificadores de suscripción (por ejemplo, uno o más rangos de SUPi). En este caso, el código de subdominio puede ser un identificador de uno o más rangos de identificadores de suscripción asociados con un determinado subdominio, por ejemplo, un valor de tupla tal como {1000000-5000000}, etc. Alternativa o adicionalmente, un código de subdominio puede basarse en la información del identificador del abonado.

En aún otras realizaciones, un código de subdominio puede basarse en un identificador interno de clave pública/privada de red doméstica, por ejemplo, interno a la red doméstica, por ejemplo, un valor numérico tal como 2, 3, 4, etc. Alternativa o adicionalmente, un código de subdominio puede basarse en uno o varios esquemas de cifrado admitidos por diferentes instancias de SIDF, por ejemplo, una cadena alfanumérica tal como "ECIES-brainpool", "ECIES-secp256r1", etc.

Independientemente de la forma particular de un código de subdominio, el equipo 26 de red en algunas realizaciones está configurado por otro equipo de red para asociar el código 32 de subdominio con una determinada instancia de NF de proveedor, por ejemplo, para realizar la selección de la instancia de NF de proveedor como se ha descrito anteriormente. El mismo o diferente equipo de red puede alternativa o adicionalmente configurar el equipo 12 de usuario y/o la ICC 12A con el código 32 de subdominio, por ejemplo, para incluirlo en el SUCI o en la parte 34 de SUCI. La fig. 3 ilustra un ejemplo según algunas realizaciones.

Como se muestra en la fig. 3, la red 10 incluye la configuración de un equipo 40 de red. La configuración del equipo 40 de red en algunas realizaciones implementa una función de operación y mantenimiento (OMF), mientras que en otras realizaciones el equipo 40 de red implementa una determinada instancia de NF de proveedor, o un proxy para la instancia de NF de proveedor. Independientemente, el equipo 40 de red configura el equipo 26 de red para realizar la selección de instancia de NF y/o configurar el equipo 12 de usuario o la ICC 12A con un código 32 de subdominio.

El equipo 40 de red en este sentido está configurado para obtener el código 32 de subdominio que indica el subdominio determinado, de entre los múltiples subdominios 30-1, 30-2,... 30-N de la red doméstica, al que está asignado el abonado 13. El equipo 40 de red está además configurado para transmitir información 42 que configura el equipo 26 de red para asociar el código 32 de subdominio con una determinada instancia de NF de proveedor entre las instancias 24-1, 24-2,... 24-M de NF de proveedor que se asignan respectivamente para proporcionar un servicio a los abonados asignados a diferentes subdominios 30-1, 30-2,... 30-N. La fig. 3, por ejemplo, muestra que la información 42 incluye una correspondencia o asociación 42A entre el código 32 de subdominio y una determinada instancia de NF de proveedor. Esta correspondencia o asociación 42A en algunas realizaciones también puede indicar la asociación entre uno o más códigos de subdominio (no mostrados) y una o más instancias de NF de otro proveedor. Independientemente, la información 42 de configuración puede incluir (por ejemplo, como parte de la correspondencia o asociación 42A) el código 32 de subdominio e información de enrutamiento para la instancia de NF de proveedor asociado, por ejemplo, de tal manera que la información configura el equipo 26 de red para asociar el código 32 de subdominio con esa información de enrutamiento. La información de enrutamiento puede estar, por ejemplo, en forma de una dirección IP, un nombre de servidor, un nombre de dominio o un identificador de recurso uniforme de la instancia de NF de proveedor. En cualquier caso, la información 42 de configuración en algunas realizaciones incluye el campo 34A descrito anteriormente que indica el código 32 de subdominio. Es decir, el equipo 40 de red genera u obtiene, de otro modo, el campo 34A y transmite el campo 34A para indicar el código 32 de subdominio, por ejemplo, como parte de la correspondencia o asociación 42A. En algunas realizaciones, el equipo 40 de red extrae el código 32 de subdominio del campo 34A para asociar el código 32 de subdominio con una determinada instancia de NF de proveedor, mientras que en otras realizaciones (por ejemplo, donde el campo 34A está dedicado a indicar un código de subdominio), el equipo 40 de red puede simplemente asociar el campo 34A con una determinada instancia de NF de proveedor.

El equipo 40 de red en la fig. 3, alternativa o adicionalmente, obtiene el código 32 de subdominio que indica el subdominio determinado, de entre los múltiples subdominios 30-1, 30-2,... 30-N de la red doméstica, al que está asignado el abonado 13 y transmite la información 44 que configura el equipo 12 de usuario o la ICC 12A con el código 32 de subdominio obtenido. El equipo 40 de red puede, por ejemplo, generar o, de otro modo, obtener el campo 34A y transmitir el campo 34A para indicar el código 32 de subdominio. El equipo 12 de usuario y/o la ICC 12A pueden recibir correspondientemente la información 44 (por ejemplo, el campo 34A) que configura el equipo 12 de usuario y/o la ICC 12A con el código 32 de subdominio.

Configurado con el código 32 de subdominio, el equipo de usuario y/o la ICC 12A pueden generar posteriormente el SUCI o la parte 34 de SUCI para incluir el campo 34A que indica el código 32 de subdominio. El equipo 12 de usuario y/o la ICC 12A pueden, a continuación, transmitir un mensaje que incluya el SUCI o la parte 34 de SUCI, por ejemplo, tal como un mensaje de registro o un mensaje de solicitud de archivo adjunto.

En algunas realizaciones, tal como cuando el uso del campo 34A es específico de la implementación (por ejemplo, según la preferencia del operador de red), el equipo 12 de usuario y/o la ICC 12A no necesitan extraer el código 32 de subdominio del campo recibido 34A antes de generar el SUCI o la parte 34 de SUCI para incluir el campo 34A. De hecho, en algunas realizaciones en las que el campo 34A indica tanto el código 32 de subdominio como otra información (por ejemplo, información de cifrado), el equipo 12 de usuario y/o la ICC 12A no necesitan comprender o saber que el campo 34A en realidad indica tanto el código 32 de subdominio como la otra información. En su lugar, el equipo 12 de usuario y/o la ICC 12A pueden generar "a ciegas" o "ignorantemente" el SUCI o la parte 34 de SUCI con el campo recibido 34A, sin leer o comprender el campo 34A.

Obsérvese que las realizaciones descritas anteriormente pueden aplicarse a cualquier tipo de NF de consumidor y a cualquier tipo de NF de proveedor. También obsérvese que el equipo 26 de red que realiza la selección de instancia de NF de proveedor puede ser cualquier tipo de equipo 26 de red en la red 10.

Obsérvese que aunque algunas realizaciones (por ejemplo, ilustradas en las figuras) se han descrito con respecto a una instancia de NF de consumidor e instancias de NF de proveedor, algunos aspectos de las realizaciones pueden implementarse mediante un proxy de la instancia de NF de consumidor y/o uno o más proxys de una o más de las instancias de NF de proveedor.

Obsérvese también que el SUCI en el sistema 5G aún puede contener SUPÍ sin cifrar en un caso especial cuando se utiliza el llamado esquema nulo. El esquema nulo no realiza ningún cifrado en el SUPÍ.

Algunas realizaciones se describirán ahora en ocasiones con referencia a una red 5G. El 3GPP es el principal organismo de normalización de funciones de red y protocolos de redes celulares. Ha estandarizado la tercera generación (3G) y la cuarta generación (4G) de redes celulares y también es responsable de la estandarización de la quinta generación (5G) de redes celulares. La especificación técnica de 3GPP llamada 3GPP TS 23.501 define la

arquitectura de red 5G, que se muestra en la fig. 4. En un nivel alto, una red 5G consta de tres entidades principales, a saber, un equipo de usuario de próxima generación (NG UE), una red de acceso por radio 5G (5G RAN) y una red central 5G. El NG UE 52 y el 5G RAN 54 se muestran en la fig. 4. Todo el resto puede considerarse vagamente como la red central 5G. Los abonados de 5G utilizan el NG UE 52 para acceder a la red central de 5G mediante la comunicación de radio inalámbrica proporcionada por la 5G RAN 54. A continuación, se incluye una breve descripción de las funciones de la red central (NF) de 5G. La función 56 de gestión de acceso y movilidad (AMF) soporta la movilidad de NG UE; la función 58 de gestión de sesión (SMF) gestiona la configuración y el mantenimiento del direccionamiento de tráfico del UE; la función 60 de servidor de autenticación (AUSF) es responsable de la autenticación de la suscripción utilizada por el NG UE; la gestión 62 unificada de datos (UDM) almacena y gestiona datos de suscripción; la función 64 de control de políticas (PCF) soporta la infraestructura para regular el comportamiento de la red; la función 66 de repositorio de función de red (NRF) soporta el descubrimiento de varios servicios de red centrales; la función 68 de exposición de la red (NEF) proporciona medios para exponer de forma segura los servicios y capacidades de las NF; y la función 70 de plano de usuario (UPF) proporciona interconexión a la red de datos, enrutamiento y reenvío de paquetes.

Las líneas discontinuas en la fig. 4 indican interfaces que transportan tráfico del plano de control y las líneas continuas en la fig. 4 indican interfaces que transportan tráfico del plano de usuario. Las etiquetas de N1 a N15 cerca de las líneas son el nombre de las interfaces correspondientes. Las líneas cortas con terminales de círculos rellenos y etiquetas cerca de ellos indican que forman parte de la SBA, que se explica a continuación.

El 3GPP ha diseñado la arquitectura de red central 5G para una mejor adopción de técnicas de nube y virtualización mediante la introducción de la llamada arquitectura basada en servicios (SBA) donde las funciones de red (NF), por ejemplo, AMF 56, AUSF 60, etc., pueden dinámicamente exponer, descubrir e invocar a las demás y a los servicios de las demás, es decir, NF/servicio. El descubrimiento de NF/servicio se implementa mediante una función lógica llamada función 66 de repositorio de función de red (NRF) que soporta las siguientes funcionalidades según 3GPP TS 23.501: Soporta la función de descubrimiento de servicios, recibe la solicitud de descubrimiento de NF de la instancia de NF y proporciona la información de las instancias de NF descubiertas (ser descubiertas) a la instancia de NF, y mantiene el perfil de NF (descrito más adelante) de las instancias de NF disponibles y sus servicios soportados.

Cuando una NF de consumidor (es decir, una NF de solicitante, digamos una AMF) se pone en contacto con la NRF 66 para descubrir una NF de productor (es decir, una NF solicitada) de algún tipo (digamos del tipo SMF), la NRF 66 puede descubrir y proporcionar múltiples NF de productor (digamos múltiples SMF) a la NF de consumidor (es decir, la AMF). En tal caso, la NF de consumidor realiza la llamada selección de NF. La selección de NF consiste en seleccionar una instancia de NF de productor entre la instancia o instancias de NF de productor descubiertas durante el descubrimiento del servicio de NF. La selección de NF puede ser implementada por la NF de consumidor, por ejemplo, la selección de SMF está soportada por la AMF 56. Alternativamente, la selección de NF puede ser implementada por la NRF 66 o un proxy para la NF de consumidor.

En el contexto de itinerancia, se pueden desplegar múltiples NRF en las diferentes redes, incluyendo las NRF en la PLMN visitada (vNRF) configuradas con información para la PLMN visitada y las NRF en la PLMN doméstica (hNRF) configuradas con información para la PLMN doméstica, referenciada por la vNRF mediante la interfaz N27.

El descubrimiento de servicios NF/NF a través de PLMN funciona de la siguiente manera (basándose en 3GPP TS 23.502, cláusula 4.17.5). La NF de consumidor (digamos una AMF 56) está ubicada en la VPLMN, y la NF de productor (digamos una AUSF 60 o UDM 62) está ubicada en la HPLMN. La NF de consumidor primero contacta a la vNRF. La vNRF, a continuación, desencadena el descubrimiento de NF en nombre del consumidor de NR hacia la hNRF. Básicamente, esto significa que cada PLMN aloja y mantiene sus propios datos NRF localmente. Solamente es necesario estandarizar la interfaz (por ejemplo, los valores de entrada y salida) para el descubrimiento del servicio NF, mientras que el método exacto de descubrimiento puede permanecer local para HPLMN.

Para que la NRF mantenga adecuadamente la información de las instancias de NF disponibles y sus servicios soportados, cada instancia de NF informa a la NRF 66 de la información que comprende la lista de servicios de NF que la instancia de NF soporta, entre otra información de la instancia de NF, siendo la información llamada perfil de NF. La información típica incluida en el perfil de NF podría ser, según 3GPP TS 23.501, lo siguiente: ID de instancia de NF, tipo de NF, identificador de red móvil terrestre pública (ID de PLMN), identificador o identificadores relacionados de segmento de red, por ejemplo, información de asistencia de selección de segmento de red única (S-NSSAI) o identificador de instancia de segmento de red (NSI ID), nombre de dominio completo (FQDN) o dirección IP de NF, información de capacidad de NF, información de autorización de servicios específicos de NF, nombres de servicios soportados, Información de terminal de instancia o instancias de cada servicio soportado y/u otro parámetro de servicio, por ejemplo, nombre de red de datos (DNN), terminal de notificación para cada tipo de notificación que el servicio NF está interesado en recibir.

La red central 5G es capaz de hacer el mejor uso de las técnicas de nube y virtualización porque está diseñada en base al concepto denominado arquitectura basada en servicios (SBA). La ventaja de la SBA es que algunas NF pueden exponerse, descubrirse e invocarse dinámicamente entre sí. Según las realizaciones de la presente memoria, un despliegue de red central 5G puede tener múltiples instancias de NF de productor (también denominadas de manera equivalente en la presente memoria como NF de proveedor). Cada instancia de NF de

productor puede, por ejemplo, configurarse para servir, o ser capaz de servir, solamente a un subconjunto de abonados, no a un conjunto completo de abonados. En tales despliegues, cuando un abonado realiza algún tipo de solicitud a una NF de consumidor, se vuelve un desafío para la NF de consumidor descubrir, seleccionar o invocar una instancia de NF de productor correcta que esté configurada para servir o ser capaz de servir a ese abonado en particular. El mismo desafío es cierto para la NRF 66, si la NRF 66 es responsable de hacer una selección entre múltiples instancias de NF.

Las realizaciones de la presente memoria proporcionan un mecanismo para el descubrimiento y la selección de funciones de red que son adecuadas para dar servicio a ciertos abonados. El mecanismo puede ser efectivo en el sentido de que el mecanismo selecciona una instancia de función de red correcta o adecuada, entre múltiples instancias de función de red (por ejemplo, del mismo tipo), que es capaz de servir a cierto o ciertos abonados. Adicional o alternativamente, el mecanismo puede ser eficiente en el sentido de que impone una carga operativa mínima y/o proporciona armonización con los mensajes existentes.

Más particularmente, es un desafío para una NF de consumidor o una NRF descubrir, seleccionar o invocar una instancia de NF de productor correcta (por ejemplo, de cierto tipo) entre múltiples instancias de NF de productor (por ejemplo, del mismo tipo). A continuación se muestra un ejemplo de este desafío. Un gran operador que ejecuta una red celular puede tener varios millones o incluso miles de millones de abonados, digamos 650 millones. El operador puede optar por tener múltiples instancias de UDM 62, cada una de las cuales almacena datos de sus abonados regionales. Digamos que hay 10 instancias de UDM, es decir, UDM-1 a UDM-10, y las regiones correspondientes son REGION-1 a REGION-10. Ahora, cuando un abonado aleatorio de REGION-5 se desplaza a la REGION-10 y utiliza su NG UE 52 para acceder a la red del operador, se envía una solicitud de registro a una AMF 56. A continuación, la AMF 56 contacta a una NRF 66 para descubrir una instancia de NF de tipo UDM. La NRF 66 descubre y devuelve 10 instancias de UDM a la AMF 56. Ahora, es un desafío para la AMF 56 seleccionar entre las 10 instancias de UDM la correcta que es capaz de servir al abonado, que sería la UDM-5.

En el ejemplo anterior y el siguiente texto, la AMF 56, que es una NF de consumidor, utiliza la NRF 66 para descubrir la instancia de UDM, que es una instancia de NF de productor. En la práctica, un consumidor de NF en las realizaciones de la presente memoria no está limitado sólo a la AMF 56 o a la UDM 62; podrían ser otras funciones, tal como AUSF 60. Los ejemplos se dan como ilustración y no son de ninguna manera limitativos. De hecho, en la mayoría de los casos de uso que se describen actualmente en las especificaciones 3GPP, la AMF 56 descubre AUSF 60. De manera similar, SUPI e IMSI se utilizan indistintamente para indicar un identificador a largo plazo o permanente asignado a un abonado por su operador de red doméstica. Pero el IMSI (como se especifica en 3GPP TS 23.003) es solamente un tipo de SUPI, y también existen otros tipos, tal como NAI (IETF RFC 4282) para SUPI no basados en IMSI. El NG UE 52 y los abonados también se utilizan indistintamente por simplicidad, aunque un abonado puede ser un usuario humano que utiliza el NG UE 52 para conectarse a la red. El término NG UE 52 también se puede utilizar para abarcar el Módulo de Identidad de Abonado Universal (USIM), la Tarjeta de Circuito Integrado Universal (UICC) y el Equipo Móvil (ME).

Con estas calificaciones, una solución potencial para el desafío sería que la AMF 56 haga uso del SUPI del abonado. En el ejemplo anterior, 650 millones de abonados significan 650 millones de SUPI que se separarían en 10 rangos de SUPI, cada rango perteneciente a una región, y se asignarían a las 10 UDM. Significa que cada UDM 62 almacenará datos de 65 millones de SUPI. Los rangos de SUPI y las UDM 72 correspondientes estarían preconfigurados en la AMF 56. Por lo tanto, cuando el abonado de REGION-5 envía una solicitud de registro utilizando su NG UE 52, la AMF 56 inspeccionaría el SUPI contenido en la solicitud de registro, determinaría el rango del SUPI, y sería capaz de seleccionar UDM-5.

Sin embargo, la solución mencionada anteriormente puede no ser suficiente en algunas circunstancias. Esto se debe a que el SUPI podría estar oculto, lo que significa que la AMF 56 no siempre puede inspeccionar el SUPI. A diferencia de los sistemas 4G, el sistema 5G posibilita que el NG UE 52 oculte el SUPI mediante el uso de técnicas de cifrado basadas en la clave pública del operador de la red doméstica, siendo el SUPI oculto denominado identificador oculto de suscripción (SUCI). Por lo tanto, la AMF 56 podría obtener el SUCI en lugar del SUPI y, debido al cifrado, la AMF 56 no sería capaz de determinar el rango del SUPI. Es así porque la AMF 56 necesitaría revelar el SUCI en SUPI mediante el uso de técnicas de descifrado, y la AMF 56 no puede hacerlo. En 5G, la revelación del SUCI en SUPI solamente lo realiza una NF llamada función de revelación de identificador de suscripción (SIDF). La SIDF podría desplegarse como una NF independiente o coubicarse con otras NF, por ejemplo AUSF 60 o UDM 62. Actualmente, se asume, por 3GPP y también aquí, que la SIDF se ubicaría junto con la UDM 62, y por lo tanto, en el resto del texto, se asume que la UDM 62 puede revelar el SUCI en SUPI.

Otra posible solución sería que la AMF 56 realice algunas heurísticas en el SUCI y adivine el rango del SUPI, por ejemplo, inspeccionando el patrón de bits de los bits cifrados en el SUCI. Sin embargo, tal solución es inviable, si no imposible, porque la técnica de cifrado utilizada para ocultar SUPI en SUCI es probabilística, lo que significa que cada cifrado produce una salida diferente.

Otra posible solución que resuelve el problema mencionado anteriormente con SUCI sería utilizar tantas claves públicas del operador de la red doméstica (claves públicas HN) como instancias de UDM. Como se ha dicho anteriormente, en los sistemas 5G, el NG UE 52 podría ocultar el SUPI en SUCI mediante el uso de técnicas de

cifrado basadas en la clave pública HN. Si bien es posible y está permitido que el operador de la red doméstica utilice una única clave pública HN para todos los abonados, no es obligatorio hacerlo. En la práctica, el operador de red doméstica podría tener 10 claves públicas HN diferentes, en el ejemplo anterior, cada una para el SUPI almacenado en una de las 10 regiones o instancias de UDM. En otras palabras, la clave pública HN utilizada por el NG UE 52, en el ejemplo anterior, sería específica para la UDM-5. Cuando el NG UE 52 envía la solicitud de registro, el NG UE 52 indicaría un identificador para la clave pública HN que se ha utilizado para ocultar el SUPI en SUCI. Por lo tanto, aunque la AMF 56 no sería capaz de determinar el rango del SUPI, la AMF 56 podría identificar la UDM-5 basándose en el identificador de clave pública HN enviado por el NG UE 52.

Si bien la solución mencionada anteriormente de utilizar múltiples claves públicas HN funciona para algunos casos de uso, podría tener limitaciones para otros. Una razón es que tener múltiples claves públicas HN significaría requerir múltiples claves privadas HN correspondientes. Con múltiples pares de claves públicas/privadas HN, habría una carga operativa y de seguridad adicional, por ejemplo, para la generación de claves, distribución de claves y revocaciones de claves.

En relación con el ejemplo mencionado anteriormente, algunas realizaciones de la presente memoria posibilitan ventajosamente que la AMF 56 seleccione la instancia correcta de UDM 62, es decir, la UDM-5. En general, algunas realizaciones en la presente memoria agrupan lógicamente las instancias de NF en diferentes subdominios, por ejemplo, de manera que el NG UE 52 sea capaz de enviar a la red una indicación del subdominio al que pertenece el abonado del NG UE. A continuación, la red puede seleccionar la instancia de UDM correcta basándose en la indicación de subdominio enviada por el NG UE 52. Podría ser, bien la AMF 56 o bien la NRF 66, en el ejemplo anterior, quien selecciona la UDM-5.

A las 10 instancias de UDM, posiblemente junto con 10 AUSF u otras NF que se consideren necesarias, se les asignarían 10 códigos de subdominio. Las 10 instancias de UDM pueden utilizar el mismo par de claves pública/privada HN. Por lo tanto, debería apreciarse que con algunas realizaciones que explotan códigos de subdominio, no hay necesidad de un par de claves pública/privada de HN específicas de UDM.

Según algunas realizaciones, el SUPI, cuando se utiliza el formato IMSI, se compone de un código de país móvil (MCC), un código de red móvil (MNC) y un número de identificación de suscripción móvil (MSIN). Y el SUCI se compone de al menos el MCC, el MNC, un MSIN cifrado y un campo identificador de clave pública HN que se ha utilizado para cifrar el MSIN. La sintaxis NAI de SUPI es muy similar a IMSI: el "nombre de usuario" corresponde al MSIN y el "dominio" corresponde al MCC+MNC (por ejemplo, nombredusuario@dominiolocal.ejemplo.net o dominiolocal.ejemplo.net!nombredusuario@dominiovisitado.ejemplo.net). En la sintaxis NAI de SUCI, el nombre de usuario está cifrado y se incorpora el campo de identificador de clave pública HN.

Algunas realizaciones explotan el SUCI para indicar un código de subdominio (SDC). En algunas realizaciones, por ejemplo, un código de subdominio se indica mediante el campo de identificador de clave pública HN, además de identificar la clave pública HN. En otras realizaciones, se utiliza un campo separado para indicar el SDC, lo que significa que, bien el SUPI se amplía para estar compuesto por el SDC además del MCC, el MNC y el MSIN, o bien el SDC se aprovisionará por separado en el NG UE 52. En consecuencia, el SUCI se amplía para estar compuesto por el SDC además de al menos el MCC, MNC, MSIN cifrado y el campo de identificador de clave pública HN.

La fig. 5 ilustra una implementación ejemplar de la realización anterior en la que el campo de identificador de clave pública HN indica un SDC además de la clave pública HN. En la etapa 1 a/b de la fig. 5, alguna función o nodo en la red del operador aprovisiona la NRF 66 y el NG UE 52 respectivamente con la información que se muestra (por ejemplo, el campo de identificador de clave pública HN), como se ha explicado anteriormente. El campo de identificador de clave pública HN se construye de manera que contenga tanto la identificación de la clave pública HN que se ha de utilizar para cifrar el SUPI como el SDC. Cualquier función o nodo puede realizar el aprovisionamiento, no solo el que se muestra en la fig. 5. Generalmente, aquellas NF que podrían descubrirse más tarde pueden registrar su soporte para el descubrimiento basándose en el SDC y cualquier otra información de enrutamiento necesaria. En nuestro ejemplo, es la UDM 62 donde se ubica la SIDF.

En la etapa 2, el NG UE 52 envía una solicitud de registro a la AMF 56. La solicitud comprende al menos el SUCI. El SUCI, a su vez, está compuesto al menos del MCC, MNC, MSIN cifrado y el campo de identificador de clave pública HN. El campo identificador de clave pública HN comprende a su vez el SDC.

En la etapa 3, la AMF 56 descubre la instancia de NF correcta con la que es necesario contactar a continuación (por ejemplo, AUSF 60, UDM/SIDF) utilizando la NRF 66 y toda o parte de la información recibida del NG UE 52. (Obsérvese que en un caso de uso más común, la AMF 56 descubre la AUSF 60.) Como se muestra en la fig. 5, NRF 66 descubre la instancia 62-1 de UDM entre múltiples instancias 62-1...62-N de UDM posibles, determinando la instancia 62-1 de UDM basada en el SDC. La NRF 66 en algunas realizaciones basa este descubrimiento en el MCC, MNC y el campo de identificador de clave pública HN (incluyendo el SDC) como se muestra. En la etapa 4, la AMF 56 invoca los servicios requeridos en la instancia de NF descubierta.

Para mayor aclaración, en la fig. 6 se muestra un diagrama de secuencia de algunas realizaciones.

Recuerde que la ubicación de SIDF es determinada por el operador, por lo que podría ser independiente, combinado

con AUSF 60, combinado con UDM 62, etc. en diferentes soluciones de despliegue de operadores propietarios. Aquí, la ubicación conjunta de UDM/SIDF 62 se toma como ejemplo.

5 En la etapa 0, la UDM/SIDF 62 u otra entidad de red (por ejemplo, la función de operaciones y mantenimiento (O&M) del operador) construye un campo de identificador de clave pública HN (que incluye el SDC para diferentes casos de despliegue de SIDF) y lo hace corresponder con claves públicas HN.

10 El SDC en sí mismo puede basarse en varios parámetros como: (i) Un identificador específico de operador generado aleatoriamente, por ejemplo, un valor numérico, digamos 12382, 88274, 93422145, etc.; (ii) Un identificador interno de claves públicas/privadas HN, por ejemplo, un valor numérico, digamos 2, 3, 4, etc.; (iii) Una información de despliegue de red, por ejemplo, información de segmento, identificador de red o identificador de subred, por ejemplo, cadena alfanumérica "segmento-1", "red_7", etc.; (iv) Una ubicación geográfica o ubicación/topología lógica de red, por ejemplo, cadena alfanumérica, digamos "estocolmo-kista-2", "gotemburgo-5", "lat:59.3293, lon:18.0686", etc.; (v) Un esquema o esquemas de cifrado soportados por diferentes instancias SIDF, por ejemplo, cadena alfanumérica, diga "ECIES-brainpool", "ECIES-secp256r1", etc. (vi) Referencias a la información de enrutamiento de la información NF relacionada, por ejemplo, SIDF, UDM, AUSF, digamos cadena alfanumérica como "AUSF-1" que se refiere a la dirección IP, etc.; (vii) Una información de enrutamiento de la información NF relacionada, por ejemplo, cadena alfanumérica como "10.10.1.192" que muestra la dirección IP, etc.; y/o (viii) Una información de identificación de abonado, por ejemplo, rango del SUPI, un valor de tupla digamos {1000000-500000}, etc.

20 En la etapa 1, la UDM/SIDF aprovisiona la NRF 66 invocando un procedimiento de registro de servicio/NF hacia la NRF 66. El mensaje al NRF 66 comprende el perfil NF de la UDM/SIDF. La NRF 66 recibe y almacena el perfil NF en consecuencia. Obsérvese que la NRF 66 es la hNRF en un contexto de itinerancia.

Obsérvese que además de la información habitual en el perfil NF, la UDM/SIDF 62 también almacena su campo de identificador de clave pública HN soportado (incluyendo SDC) y otra información de enrutamiento (por ejemplo, direcciones IP) como se ha mencionado anteriormente en el perfil NF.

25 En la etapa 2, la UDM/SIDF 62 u otra entidad de red (por ejemplo, la función de operaciones y mantenimiento (O&M) del operador), a continuación, aprovisiona al NG UE 52 con el campo de identificador de clave pública HN junto con otra información, por ejemplo, clave pública HN.

30 En la etapa 3, el NG UE 62 activa un procedimiento de registro hacia la red mediante el envío de un mensaje de solicitud de registro que incluye su SUCI. Recuérdese que el SUCI a su vez comprende al menos lo siguiente cuando se utiliza IMSI como SUPI (y que existen otros formatos SUPI, tal como NAI): (i) MSIN oculto o cifrado por la clave pública HN provisionada; (ii) MCC y MNC; y (iii) campo de identificador de clave pública HN que identifica la clave pública HN utilizada para el cifrado. En nuestro ejemplo, el mismo campo también identifica el SDC.

35 En la etapa 4, la AMF 56, basándose en la configuración local o la política del operador, puede invocar el servicio de descubrimiento de NF hacia la NRF 66 para descubrir y seleccionar una instancia de AUSF correcta para manejar la autenticación del NG UE. (Obsérvese que, en algunos casos de uso, si la AMF 56 tiene que descubrir UDM 62 primero, la AMF 56 puede descubrir una instancia de UDM directamente en esta etapa). Obsérvese que con el contexto de itinerancia, AMF 56 contacta con vNRF y vNRF contacta con hNRF (no se muestra en la figura). La AMF 56 también puede ser capaz de descubrir la propia AUSF 60 si tiene la capacidad local para realizar el descubrimiento como lo tiene la NRF 56 (como se explica en la etapa 5). La AMF 56 utiliza el SUCI recibido o algunas partes del SUCI recibido, por ejemplo, solamente el campo de identificador de clave pública HN, como entrada para la selección de instancia de NF.

40 En la etapa 5, la NRF 66 utiliza la entrada de AMF 56 para descubrir la instancia correcta de AUSF. La NRF 66 informa a la AMF 56 sobre la AUSF 60 descubierta. Obsérvese que en un contexto de itinerancia, tanto vNRF como hNRF están involucradas.

45 Por ejemplo, la NRF 66 puede utilizar el SUCI recibido completo o partes del SUCI, por ejemplo, el campo de identificador de clave pública HN recibido o solamente el SDC incluido en el campo de identificador de clave pública HN, para hacer coincidir los atributos almacenados en los perfiles NF e identificar además la instancia adecuada de AUSF. La Identificación del SDC incluido en el campo de identificador de clave pública HN es similar a la construcción del campo de identificador de clave pública HN como se ha explicado anteriormente, por ejemplo, dividir si se ha utilizado concatenación, realizar una coincidencia de expresión regular si se ha utilizado expresión regular y descifrar si se ha utilizado cifrado.

50 A continuación, la AMF 56 selecciona la instancia de AUSF a partir de la salida del resultado del descubrimiento de NRF y, en la etapa 6, envía la solicitud de autenticación junto con la información de SUCI a esa instancia de AUSF seleccionada.

55 En la etapa 7, la AUSF 60, basándose en la configuración local o la política del operador, puede invocar el servicio de descubrimiento de NF hacia NRF 66 para encontrar y seleccionar una instancia de UDM/SIDF correcta para manejar la solicitud de autenticación del UE y revelar o descifrar el SUCI. La AUSF/NRF puede repetir los procedimientos similares en las etapas 4 y 5 para descubrir una instancia correcta de UDM/SIDF.

En la etapa 8, la AUSF 60 selecciona, a continuación, instancias 62 de UDM/SIDF adecuadas a partir de la salida del resultado del descubrimiento de NRF y envía la solicitud de información de autenticación junto con la información de SUCI a esa instancia de NF seleccionada.

5 Como demuestra este ejemplo, a continuación, el SUCI completo puede estar disponible para el descubrimiento y/o selección de instancias de NF de proveedor. Esto puede incluir el identificador de red doméstica (por ejemplo, MNC y/o MCC) de SUCI y también otros parámetros, como el esquema de protección y el identificador de clave pública de la red doméstica. Estos parámetros pueden aprovisionarse previamente al UE 52 y siempre incluirse en el SUCI. Obsérvese que hacerlo no impide el descubrimiento o la selección de NF; más bien, el uso de esos parámetros o campos en SUCI habilita un mecanismo extremadamente flexible que podría ser diferente entre diferentes proveedores.

10 En algunas realizaciones, la SIDF es responsable de revelar el SUPI del SUCI. La SIDF utiliza la parte de la clave privada del par de claves pública/privada de la red doméstica relacionada con la privacidad que se almacena de forma segura en la red del operador doméstico. La revelación tendrá lugar en la UDM 62. Se definirán los derechos de acceso a la SIDF, de tal manera que solamente se le permite a un elemento de red de la red doméstica solicitar la SIDF.

15 En algunas realizaciones, el descubrimiento y la selección de funciones de red (NF como AUSF, SIDF/UDM) con o sin utilizar NRF 66 deben usar SUCI como parámetro de entrada, cuando el UE 52 proporciona el SUCI. La red puede utilizar el SUCI en una implementación de forma específica

20 Los despliegues de red pueden comprender varias instancias de AUSF y/o UDM que atienden diferentes rangos de SUPI. Sin embargo, dado que el identificador de suscripción está oculto en SUCI, el rango del identificador de suscripción no está disponible para la selección de AUSF o UDM. Para ayudar a la selección de AUSF y UDM en el subdominio de red doméstica correcto, el SUCI según algunas realizaciones incluye un parámetro relacionado con el subdominio al que pertenece el usuario. El descubrimiento de NF con SUCI puede configurarse localmente en los consumidores de NF o implementarse en la hNRF. La selección de AUSF y/o UDM basada en parámetros codificados en SUCI depende del despliegue de la red. En algunas realizaciones, el SUCI completo debe estar disponible para el descubrimiento. Esto incluye el identificador de la red doméstica (por ejemplo, MNC y/o MCC) de SUCI y también otros parámetros, como el esquema de protección y el identificador de clave pública de la red doméstica. Estos parámetros pueden aprovisionarse previamente al UE 52 y siempre incluirse en el SUCI.

25 Cuando la SEAF y la AUSF 60 reciben el SUCI y se utiliza la NRF 66, el SUCI completo se utiliza como parámetro de entrada para el descubrimiento del servicio AUSF y UDM. Si no se utiliza NRF 66, SEAF y/o AUSF 60 pueden utilizar parámetros codificados en SUCI para seleccionar AUSF y/o UDM respectivamente.

30 Una opción para implementar la selección de AUSF y/o el descubrimiento de UDM se ha de utilizar el identificador de clave pública de la red doméstica como criterio de selección de NF. Por ejemplo, cada UDM 62 puede tener su propia clave pública de red doméstica, y la UDM 62 puede seleccionarse basándose en el identificador relacionado. Sin embargo, cuando se utiliza una nueva clave pública de red doméstica en la UDM 62, el nuevo identificador también se ha de actualizar en el descubrimiento de NF.

35 Alternativamente, el identificador de clave pública de la red doméstica puede tener una estructura interna para identificar el subdominio y la clave pública de la red doméstica. Por ejemplo, el identificador que tiene una longitud de N bits podría construirse utilizando un prefijo de M bits de longitud que identifica la clave pública de la red doméstica y un sufijo de N-M bits de longitud que identifica el subdominio, y la hNRF puede utilizar el sufijo para descubrir la NF correcta. La estructura interna del identificador solamente la conoce HPLMN y es compatible con la privacidad.

40 Por lo tanto, las realizaciones de la presente memoria pueden incluir un método, implementado en una función en la red doméstica (por ejemplo, función de operación y mantenimiento, UDM 62 o SIDF) para habilitar el descubrimiento de una instancia de NF adecuada para manejar la solicitud de un abonado. El método comprende la construcción de un código de subdominio. El código de subdominio puede identificar un subdominio, por ejemplo, con el objetivo de identificar efectivamente una instancia de NF (por ejemplo, AUSF/SIDF/UDM) adecuada para el manejo de un abonado. El método también comprende la provisión del código de subdominio al UE. El método también puede comprender la provisión del código de subdominio y la información de enrutamiento correspondiente a otra función de red.

45 En algunas realizaciones, el código de subdominio es o está indicado por un campo de identificador de clave pública HN que identifica la clave pública HN utilizada para el cifrado SUPI. Como alternativa o adicionalmente, el campo de identificador de clave pública HN está compuesto de la identificación de la clave pública HN utilizada para el cifrado SUPI y una concatenación o máscara (por ejemplo, expresión regular) del código de subdominio. En algunas realizaciones, la información de enrutamiento es una dirección IP. En algunas realizaciones, la otra función de red es una NRF 66. En otras realizaciones, la otra función de red es AMF 56 o AUSF 60.

55 Las realizaciones de la presente memoria también incluyen un método implementado en una función de red (por ejemplo, AMF 56) en una red (por ejemplo, red doméstica o visitada), para seleccionar una instancia de función de red para proporcionar un servicio (por ejemplo, autenticación, recuperación de NSSAI permitidos) para un UE. El método puede comprender la determinación, basándose en un código de subdominio (SDC) recibido del UE, cuál de una pluralidad de instancias de NF (por ejemplo, AUSF/SIDF/UDM) se ha de utilizar para proporcionar el servicio. En

algunas realizaciones, el método también puede comprender comunicarse con una instancia de NF identificada.

5 En algunas realizaciones, la determinación comprende el envío de al menos parte de la información recibida desde el UE a una NRF 66 y la recepción de la información de NF (por ejemplo, identificación AUSF/SIDF/UDM) e información de enrutamiento. En otras realizaciones, la determinación comprende el uso de información local para identificar la NF (por ejemplo, identificación AUSF/SIDF/UDM) y la información de enrutamiento.

En algunas realizaciones, la información recibida del UE y utilizada para el descubrimiento y/o selección de NF es el SUCI completo. En otras realizaciones, la información recibida del UE y utilizada para el descubrimiento y/o selección de NF es parte del SUCI, por ejemplo, el campo de identificador de clave pública HN.

10 En algunas realizaciones, el campo de identificador de clave pública HN contiene SDC. En otras realizaciones, el SDC es un campo separado en SUCI/SUPI.

15 En vista de las modificaciones y variaciones anteriores, la fig. 7A muestra otro método 100 realizado por el equipo 26 de red en una red 10 de comunicación inalámbrica. El método 100 comprende la recepción de al menos una parte de un identificador oculto de suscripción para un abonado 13 (Bloque 110). El identificador oculto de suscripción puede contener un identificador permanente de suscripción oculto para el abonado 13, tal como un SUPI oculto. Independientemente, el identificador oculto de al menos una parte de la suscripción recibida indica un código 32 de subdominio. El código de subdominio indica un cierto subdominio, de entre múltiples subdominios de una red doméstica del abonado 13, al cual está asignado el abonado 13. El método 100 también puede comprender la determinación, en base al código 32 de subdominio, de una instancia de una función de red de proveedor para proporcionar un servicio a ser consumido por el abonado 13 (Bloque 120). En algunas realizaciones, por ejemplo, esta determinación se realiza entre múltiples instancias de la función de red de proveedor en la red doméstica asignadas respectivamente para proporcionar el servicio a ser consumido por abonados asignados a diferentes subdominios. En una o más realizaciones, la determinación también se basa en un identificador de red doméstica que identifica la red doméstica.

25 En algunas realizaciones, el método 100 también puede comprender la recepción de información que configura el equipo 26 de red para asociar el código 32 de subdominio con una o más instancias de la función de red de proveedor asignada para proporcionar el servicio a los abonados asignados a cierto subdominio (Bloque 105).

30 La fig. 7B muestra otro método 150 realizado por el equipo 26 de red en una red 10 de comunicación inalámbrica. El método 150 comprende la recepción de al menos una parte de un identificador oculto de suscripción para un abonado 13 (Bloque 160). El identificador oculto de suscripción puede contener un identificador de suscripción oculto para el abonado 13. El método 150 también puede comprender la determinación a partir de al menos una parte del identificador oculto de suscripción de un código 32 de subdominio que indica un cierto subdominio, de entre múltiples subdominios de una red doméstica del abonado 13, al que está asignado el abonado 13 (Bloque 170). El método 150 también puede comprender la selección, basándose en el código 32 de subdominio y de entre múltiples instancias de una función de red de proveedor en la red doméstica asignada respectivamente para proporcionar un servicio a los abonados asignados a diferentes subdominios, una instancia de la función de red de proveedor para proporcionar el servicio al abonado 13 (Bloque 180).

35 En algunas realizaciones, el método 150 también puede comprender la recepción de información que configura el equipo 26 de red para asociar el código 32 de subdominio con una o más instancias de la función de red de proveedor asignada para proporcionar el servicio a los abonados asignados a cierto subdominio. (Bloque 155).

40 En algunas realizaciones, el método comprende además solicitar o realizar el descubrimiento de las múltiples instancias de la función de red de proveedor en la red doméstica.

En algunas realizaciones, el método comprende además la recepción de una solicitud de descubrimiento para descubrir una o más instancias de la función de red de proveedor en la red doméstica para proporcionar el servicio al abonado y responder a la solicitud de descubrimiento con la instancia seleccionada de la función de red de proveedor.

45 En algunas realizaciones, el equipo de red implementa una función de repositorio de red, NRF.

En algunas realizaciones, el equipo de red sirve como proxy para una instancia de una función de red de consumidor que va a consumir el servicio para el abonado o sirve como proxy para una o más de las instancias de la función de red de proveedor.

50 En algunas realizaciones, el equipo de red implementa una instancia de una función de red de consumidor que va a consumir el servicio para el abonado, y el método comprende además el consumo del servicio, desde la instancia seleccionada de la función de red de proveedor, para el abonado.

En algunas realizaciones, la función de red de consumidor es una función de gestión de acceso y movilidad, AMF, o una función de servidor de autenticación, AUSF.

En algunas realizaciones, el método comprende además la recepción de información que configura el equipo de red

para asociar el código de subdominio con una o más instancias de la función de red de proveedor asignada para proporcionar el servicio a abonados asignados a cierto subdominio.

- 5 En algunas realizaciones, la información incluye cierto código de subdominio e información de enrutamiento para una o más instancias de la función de red de proveedor, de tal manera que la información configura el equipo de red para asociar el código de subdominio con la información de enrutamiento.
- En algunas realizaciones, la información de enrutamiento es un Protocolo de Internet, una dirección IP, un nombre de servidor, un nombre de dominio o un identificador de recurso uniforme, de la instancia seleccionada.
- En algunas realizaciones, diferentes subdominios de la red doméstica se indican mediante diferentes códigos de subdominio específicos del operador de red y/o generados aleatoriamente.
- 10 En algunas realizaciones, diferentes subdominios de la red doméstica corresponden a diferentes ubicaciones geográficas o lógicas, y el código de subdominio es un identificador de una ubicación geográfica o lógica con la que se corresponde el determinado subdominio.
- En algunas realizaciones, diferentes subdominios de la red doméstica corresponden a diferentes segmentos o subredes de la red doméstica, y el código de subdominio es un identificador de un determinado segmento o subred con el que se corresponde dicho subdominio.
- 15 En algunas realizaciones, diferentes subdominios de la red doméstica están asociados con diferente información de enrutamiento, y el código de subdominio es un identificador asociado con la información de enrutamiento para cierto subdominio.
- En algunas realizaciones, cada subdominio de la red doméstica está asociado con uno o más rangos de identificadores de suscripción, y el código de subdominio es un identificador de uno o más rangos de identificadores de suscripción asociados con el subdominio determinado.
- 20 En algunas realizaciones, la determinación del código de subdominio comprende la determinación del código de subdominio a partir de un campo en al menos una parte del identificador oculto de suscripción, y el campo es, bien un campo de código de subdominio dedicado a indicar un código de subdominio o bien un campo configurable para indicar tanto el código de subdominio como la información de cifrado que identifica un parámetro basado en el cual se ha cifrado el identificador oculto del abonado.
- 25 En algunas realizaciones, el campo es un campo de clave pública de red doméstica configurable para indicar tanto un código de subdominio como una clave pública de red doméstica basada en la cual se ha cifrado el identificador oculto del abonado, el campo es un campo de identificador de esquema de cifrado configurable para indicar tanto un código de subdominio como un esquema de cifrado basado en el cual se ha cifrado el identificador oculto del abonado, o un campo que es diferente al campo de clave pública de la red doméstica y diferente al campo de identificador de esquema de cifrado.
- 30 En algunas realizaciones, el campo es un campo de código de subdominio dedicado a indicar un código de subdominio.
- En algunas realizaciones, el campo se puede configurar para indicar tanto el código de subdominio como la información de cifrado.
- 35 En algunas realizaciones, el campo es un campo de clave pública de la red doméstica y en donde la información de cifrado identifica una clave pública de la red doméstica basada en la cual se ha cifrado el identificador oculto del abonado.
- En algunas realizaciones, el campo se puede configurar para indicar tanto el código de subdominio como la información de cifrado mediante la concatenación del código de subdominio con la información de cifrado.
- 40 En algunas realizaciones, el campo se puede configurar para indicar tanto el código de subdominio como la información de cifrado indicando el código de subdominio y la información de cifrado en un orden definido, con cero o más delimitadores entre el código de subdominio y la Información de cifrado.
- En algunas realizaciones, la determinación del código de subdominio comprende la extracción del código de subdominio del campo separado de la información de cifrado.
- 45 En algunas realizaciones, la extracción del código de subdominio comprende la aplicación de una expresión regular al campo que separa el código de subdominio de la información de cifrado.
- En algunas realizaciones, la función de red de proveedor es una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.
- 50 En algunas realizaciones, el método comprende además el envío de una solicitud de autenticación, para la autenticación del abonado, a la instancia seleccionada de la función de red de proveedor, en donde la solicitud de

autenticación incluye la al menos una parte del identificador oculto del abonado.

La fig. 8 muestra un método 200 realizado por el equipo 40 de red en una red 10 de comunicación inalámbrica según otras realizaciones. El método 200 incluye la obtención de un código 32 de subdominio que indica un cierto subdominio, de entre múltiples subdominios de una red doméstica de un abonado 13, al que está asignado el
 5 abonado 13 (Bloque 210). El método 200 también puede incluir la transmisión de información que configura otro equipo 26 de red para asociar el código 32 de subdominio con una determinada instancia de una función de red de proveedor entre múltiples instancias de la función de red de proveedor en la red doméstica que se asignan respectivamente para proporcionar una servicio (a consumir) para abonados asignados a diferentes subdominios de la red doméstica (Bloque 220).

10 En algunas realizaciones, la información incluye el código de subdominio y la información de enrutamiento para la instancia determinada, de tal manera que la información configura el otro equipo de red para asociar el código de subdominio con la información de enrutamiento.

En algunas realizaciones, la información de enrutamiento es un Protocolo de Internet, una dirección IP, un nombre de servidor, un nombre de dominio o un identificador de recurso uniforme, de la instancia determinada.

15 En algunas realizaciones, el equipo de red implementa una función de operación y mantenimiento, la instancia determinada de la función de red de proveedor, o un proxy para la instancia determinada de la función de red de proveedor.

En algunas realizaciones, la función de red de proveedor es una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.

20 En algunas realizaciones, el otro equipo de red implementa una instancia de una función de red de consumidor que es o es capaz de consumir el servicio para un abonado, implementa una función de repositorio de red, sirve como proxy para una instancia de una función de red de consumidor que es para consumir o es capaz de consumir el servicio para un abonado, o sirve como proxy para una o más de las instancias de la función de red de proveedor.

25 En algunas realizaciones, el otro equipo de red implementa una función de gestión de movilidad y acceso, AMF, una función de servidor de autenticación, AUSF, o una función de repositorio de red.

En algunas realizaciones, diferentes subdominios de la red doméstica se indican mediante diferentes códigos de subdominio específicos del operador de red y/o generados aleatoriamente.

30 En algunas realizaciones, diferentes subdominios de la red doméstica corresponden a diferentes ubicaciones geográficas o lógicas, y el código de subdominio es un identificador de una ubicación geográfica o lógica con la que se corresponde el determinado subdominio.

En algunas realizaciones, diferentes subdominios de la red doméstica corresponden a diferentes segmentos o subredes de la red doméstica, y el código de subdominio es un identificador de un determinado segmento o subred con el que se corresponde dicho subdominio.

35 En algunas realizaciones, diferentes subdominios de la red doméstica están asociados con diferente información de enrutamiento, y el código de subdominio es un identificador asociado con la información de enrutamiento para cierto subdominio.

En algunas realizaciones, cada subdominio de la red doméstica está asociado con uno o más rangos de identificadores de suscripción, y el código de subdominio es un identificador de uno o más rangos de identificadores de suscripción asociados con el subdominio determinado.

40 En algunas realizaciones, el método comprende además generar un campo que indica el código de subdominio, en el que el campo es, bien un campo de código de subdominio dedicado a indicar un código de subdominio o bien un campo configurable para indicar tanto el código de subdominio como la información de cifrado que identifica un parámetro en base al cual se cifrará un identificador oculto de abonado para el abonado.

45 En algunas realizaciones, bien el campo es un campo de clave pública de red doméstica configurable para indicar tanto un código de subdominio como una clave pública de red doméstica basada en la cual se ha cifrado el identificador oculto del abonado, bien el campo es un campo de identificador de esquema de cifrado configurable para indicar tanto un código de subdominio como un esquema de cifrado basado en el cual se ha cifrado el identificador oculto del abonado, o bien un campo que es diferente al campo de clave pública de la red doméstica y diferente al campo del identificador del esquema de cifrado.

50 En algunas realizaciones, el campo es un campo de código de subdominio dedicado a indicar un código de subdominio.

En algunas realizaciones, la generación del campo comprende la generación del campo para indicar tanto el código de subdominio como la información de cifrado.

En algunas realizaciones, el campo es un campo de clave pública de la red doméstica y la información de cifrado identifica una clave pública de la red doméstica basada en la cual se cifra el identificador oculto del abonado.

5 En algunas realizaciones, la generación del campo comprende la generación del campo para indicar tanto el código de subdominio como la información de cifrado mediante la concatenación del código de subdominio con la información de cifrado.

En algunas realizaciones, la generación del campo comprende la generación del campo para indicar el código de subdominio y la información de cifrado en un orden definido, con cero o más delimitadores entre el código de subdominio y la información de cifrado.

En algunas realizaciones, la información que configura el otro equipo de red incluye el campo.

10 La fig. 9 muestra un método 300 realizado por el equipo 40 de red en una red 10 de comunicación inalámbrica según otras realizaciones. El método 300 incluye la obtención de un código 32 de subdominio que indica un cierto subdominio, de entre múltiples subdominios de una red doméstica de un abonado 13, al que está asignado el abonado 13 (Bloque 310). El método 300 también puede incluir la transmisión de información que configura un equipo 12 de usuario del abonado 13, o una tarjeta 12A de circuito integrado asociada con el abonado 13, con el código 32 de subdominio obtenido (Bloque 320).

En algunas realizaciones, el equipo de red implementa una función de operación y mantenimiento, una instancia de una función de red de proveedor en la red doméstica que ha de proporcionar o es capaz de proporcionar un servicio para el abonado, o un proxy para una o más instancias de la función de red de proveedor.

20 En algunas realizaciones, la función de red de proveedor es una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.

En algunas realizaciones, diferentes subdominios de la red doméstica se indican mediante diferentes códigos de subdominio específicos del operador de red y/o generados aleatoriamente.

25 En algunas realizaciones, diferentes subdominios de la red doméstica corresponden a diferentes ubicaciones geográficas o lógicas, y el código de subdominio es un identificador de una ubicación geográfica o lógica con la que se corresponde el determinado subdominio.

En algunas realizaciones, diferentes subdominios de la red doméstica corresponden a diferentes segmentos o subredes de la red doméstica, y el código de subdominio es un identificador de un determinado segmento o subred con el que se corresponde dicho subdominio.

30 En algunas realizaciones, diferentes subdominios de la red doméstica están asociados con diferente información de enrutamiento, y el código de subdominio es un identificador asociado con la información de enrutamiento para cierto subdominio.

En algunas realizaciones, cada subdominio de la red doméstica está asociado con uno o más rangos de identificadores de suscripción, y el código de subdominio es un identificador de uno o más rangos de identificadores de suscripción asociados con el subdominio determinado.

35 En algunas realizaciones, el método comprende además la generación de un campo que indica el código de subdominio, y el campo es, bien un campo de código de subdominio dedicado a indicar un código de subdominio o bien un campo configurable para indicar tanto el código de subdominio como la información de cifrado que identifica un parámetro en base al cual se cifrará un identificador oculto de abonado para el abonado.

40 En algunas realizaciones, el campo es un campo de clave pública de red doméstica configurable para indicar tanto un código de subdominio como una clave pública de red doméstica basada en la cual se ha cifrado el identificador oculto del abonado, el campo es un campo de identificador de esquema de cifrado configurable para indicar tanto un código de subdominio como un esquema de cifrado basado en el cual se ha cifrado el identificador oculto del abonado, o un campo que es diferente al campo de clave pública de la red doméstica y diferente al campo de identificador de esquema de cifrado.

45 En algunas realizaciones, el campo es un campo de código de subdominio dedicado a indicar un código de subdominio.

En algunas realizaciones, la generación del campo comprende la generación del campo para indicar tanto el código de subdominio como la información de cifrado.

50 En algunas realizaciones, el campo es un campo de clave pública de la red doméstica y en el que la información de cifrado identifica una clave pública de la red doméstica basada en la cual se cifrará el identificador oculto del abonado.

En algunas realizaciones, la generación del campo comprende la generación del campo para indicar tanto el código

de subdominio como la información de cifrado mediante la concatenación del código de subdominio con la información de cifrado.

5 En algunas realizaciones, la generación del campo comprende la generación del campo para indicar el código de subdominio y la información de cifrado en un orden definido, con cero o más delimitadores entre el código de subdominio y la información de cifrado.

En algunas realizaciones, dicha transmisión comprende la transmisión del campo al equipo de usuario o a la tarjeta de circuito integrado.

10 La fig. 10 muestra un método 400 realizado por un equipo 12 de usuario o una tarjeta 12A de circuito integrado asociada a un abonado 13. El método 400 comprende la recepción, desde el equipo 40 de red en una red 10 de comunicación inalámbrica, de información que configura el equipo 12 de usuario o la tarjeta 12A de circuito integrado con un código 32 de subdominio que indica un cierto subdominio, de entre múltiples subdominios de una red doméstica de abonado 13, al que está asignado el abonado 13 (Bloque 410). En algunas realizaciones, el método 400 también puede comprender la generación de un identificador oculto de suscripción para incluir un campo que indica el código 32 de subdominio (Bloque 420) y la transmisión de un mensaje que incluye el identificador oculto de suscripción (Bloque 430).

15 En algunas realizaciones, el equipo de red implementa una función de operación y mantenimiento, una instancia de una función de red de proveedor en la red doméstica que ha de proporcionar o es capaz de proporcionar un servicio para el abonado, o un proxy para una o más instancias de la función de red de proveedor.

20 En algunas realizaciones, la función de red de proveedor es una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.

En algunas realizaciones, diferentes subdominios de la red doméstica se indican mediante diferentes códigos de subdominio específicos del operador de red y/o generados aleatoriamente.

25 En algunas realizaciones, diferentes subdominios de la red doméstica corresponden a diferentes ubicaciones geográficas o lógicas, y el código de subdominio es un identificador de una ubicación geográfica o lógica con la que se corresponde el determinado subdominio.

En algunas realizaciones, diferentes subdominios de la red doméstica corresponden a diferentes segmentos o subredes de la red doméstica, y el código de subdominio es un identificador de un determinado segmento o subred con el que se corresponde dicho subdominio.

30 En algunas realizaciones, diferentes subdominios de la red doméstica están asociados con diferente información de enrutamiento, y el código de subdominio es un identificador asociado con la información de enrutamiento para cierto subdominio.

En algunas realizaciones, cada subdominio de la red doméstica está asociado con uno o más rangos de identificadores de suscripción, y el código de subdominio es un identificador de uno o más rangos de identificadores de suscripción asociados con el subdominio determinado.

35 En algunas realizaciones, la recepción del código de subdominio comprende la recepción de un campo que indica el código de subdominio, y el campo es, bien un campo de código de subdominio dedicado a indicar un código de subdominio o bien un campo configurable para indicar tanto el código de subdominio como información de cifrado que identifica un parámetro basado en el cual se cifrará un identificador oculto de abonado para el abonado.

40 En algunas realizaciones, bien el campo es un campo de clave pública de red doméstica configurable para indicar tanto un código de subdominio como una clave pública de red doméstica basada en la cual se ha cifrado el identificador oculto del abonado, bien el campo es un campo de identificador de esquema de cifrado configurable para indicar tanto un código de subdominio como un esquema de cifrado basado en el cual se ha cifrado el identificador oculto del abonado, o bien un campo que es diferente al campo de clave pública de la red doméstica y diferente al campo del identificador del esquema de cifrado.

45 En algunas realizaciones, el campo es un campo de código de subdominio dedicado a indicar un código de subdominio.

En algunas realizaciones, el campo se puede configurar para indicar tanto el código de subdominio como la información de cifrado.

50 En algunas realizaciones, el campo es un campo de clave pública de la red doméstica y en donde la información de cifrado identifica una clave pública de la red doméstica basada en la cual se cifrará el identificador oculto de abonado.

En algunas realizaciones, el campo se puede configurar para indicar tanto el código de subdominio como la información de cifrado mediante la concatenación del código de subdominio con la información de cifrado.

En algunas realizaciones, el campo se puede configurar para indicar tanto el código de subdominio como la información de cifrado indicando el código de subdominio y la información de cifrado en un orden definido, con cero o más delimitadores entre el código de subdominio y la información de cifrado. En algunas realizaciones, el método comprende además la generación del identificador oculto de suscripción para incluir el campo y la transmisión de un mensaje que incluye el identificador oculto de suscripción.

Obsérvese que en algunas realizaciones, una clave pública puede referirse a una clave pública sin procesar, mientras que en otras realizaciones, una clave pública se refiere a una clave pública sin procesar combinada con un certificado que vincula esta clave pública a la dirección del nodo que tiene acceso a la clave privada para la clave pública.

Una SMF en la presente memoria puede incluir algunas o todas las siguientes funcionalidades. Algunas o todas las funciones de SMF pueden ser soportadas en una sola instancia de SMF. La funcionalidad SMF puede incluir la gestión de sesiones (por ejemplo, establecimiento, modificación y liberación de sesiones, incluyendo el mantenimiento de túneles entre UPF y el nodo de red de acceso), asignación y gestión de direcciones IP de UE (incluyendo la autorización opcional), selección y control de la función UP, configuración de dirección de tráfico en la UPF para enrutar el tráfico al destino adecuado, terminación de interfaces hacia funciones de control de políticas, control de parte de la aplicación de políticas y calidad de servicio (QoS), interceptación legal (para eventos SM e interfaz al sistema de interceptación legal), terminación de partes SM de mensajes NAS, notificación de datos de enlace descendente, inicio de información SM específica de AN, envío mediante AMF sobre N2 a AN, determinación del modo de continuidad de servicio y sesión (SSC) de una sesión (para sesión de PDU de tipo IP), funcionalidad de itinerancia, manejo de aplicación local para aplicar acuerdos de nivel de servicio QoS (SLA) (red móvil terrestre pública visitada, VPLMN), recopilación de datos de carga e interfaz de carga (VPLMN), interceptación legal (en VPLMN para eventos SM e interfaz con el sistema LI) y soporte para interacción con DN externo para transporte de señalización para autorización/autenticación de sesión de PDU por DN externo.

Por el contrario, una función de Gestión de Acceso y Movilidad (AMF) puede incluir algunas o todas las siguientes funcionalidades. Algunas o todas las funciones de AMF pueden ser soportadas en una sola instancia de AMF: la terminación de la interfaz CP de la red de acceso por radio (RAN) (N2), la terminación de NAS (N1), la protección de integridad y cifrado de NAS, la gestión de registro, la gestión de conexión, la gestión de accesibilidad, la gestión de movilidad, la interceptación legal (para eventos AMF e interfaz con el sistema LI), el proxy transparente para enrutamiento de mensajes SM, la autenticación de acceso, la autorización de acceso, la función de anclaje de seguridad (SEA o SEAF) y la gestión de contexto de seguridad (SCM) que recibe una clave de la SEA que utiliza para derivar claves específicas de la red de acceso. Con respecto particular a la SEA, interactúa con la función del servidor de autenticación (AUSF) y el UE, y recibe la clave intermedia que se ha establecido como resultado del proceso de autenticación del UE. En caso de autenticación basada en USIM, la AMF recupera el material de seguridad de la AUSF.

Obsérvese además que las realizaciones en la presente memoria pueden utilizar cualquiera de uno o más protocolos de comunicación conocidos en la técnica o que pueden desarrollarse, como IEEE 802.xx, Acceso múltiple por división de código (CDMA), CDMA de banda ancha (WCDMA), Sistema global para telecomunicaciones móviles (GSM), Evolución a Largo Plazo (LTE), WiMax, Radio Nueva (NR) o similares. Por consiguiente, aunque a veces se describen en la presente memoria en el contexto de 5G, los principios y conceptos dados a conocer en la presente memoria son aplicables a sistemas 4G y otros.

Un equipo de usuario como se utiliza en la presente memoria es cualquier tipo de dispositivo capaz de comunicarse con otro nodo de radio de forma inalámbrica a través de señales de radio. Por lo tanto, un equipo de usuario puede referirse a un dispositivo inalámbrico, una estación móvil, un portátil, un teléfono inteligente, un dispositivo de máquina a máquina (M2M), un dispositivo de comunicaciones de tipo máquina (MTC), un dispositivo de Internet de las cosas (IoT) de banda estrecha, etc. Dicho esto, debería observarse que el equipo de usuario no tiene necesariamente un "usuario" en el sentido de una persona individual que posee y/u opera el equipo de usuario. También se puede hacer referencia a un equipo de usuario como un dispositivo de comunicación inalámbrica, un dispositivo de radio, un dispositivo de comunicación por radio, un terminal inalámbrico o simplemente un terminal; a menos que el contexto indique lo contrario, el uso de cualquiera de estos términos pretende incluir UE o dispositivos de dispositivo a dispositivo, dispositivos de tipo máquina o dispositivos capaces de comunicarse de máquina a máquina, sensores equipados con un dispositivo inalámbrico, ordenadores de mesa habilitados para conexión inalámbrica, terminales móviles, teléfonos inteligentes, equipos portátiles integrados (LEE), equipo montado en un portátil (LME), dongles USB, equipo inalámbrico en las instalaciones del cliente (CPE), etc.. En la exposición de la presente memoria, los términos dispositivo máquina a máquina (M2M), dispositivo de comunicación de tipo máquina (MTC), sensor inalámbrico, y sensor, también pueden utilizarse. Debería comprenderse que estos dispositivos, pueden ser UE, pero generalmente pueden configurarse para transmitir y/o recibir datos sin interacción humana directa.

En un escenario IOT, un equipo de usuario como se describe en la presente memoria puede ser, o puede estar compuesto por, una máquina o dispositivo que realiza monitorización o mediciones, y transmite los resultados de tales mediciones de monitorización a otro dispositivo o red. Ejemplos particulares de tales máquinas son medidores de potencia, maquinaria industrial o aparatos electrodomésticos o personales, por ejemplo, refrigeradores, televisores, dispositivos que se pueden llevar puestos personales tales como relojes, etc. En otros escenarios, un equipo de usuario como se describe en la presente memoria puede estar incluido en un vehículo y puede monitorizar

y/o informar sobre el estado operativo del vehículo u otras funciones asociadas con el vehículo.

Como se utiliza en la presente memoria, "equipo de red" se refiere a equipo capaz, configurado, dispuesto y/u operable para comunicarse directa o indirectamente con un equipo de usuario y/o con otro equipo en el sistema 10 de comunicación inalámbrica que habilita y/o proporciona acceso inalámbrico al equipo de usuario. Los ejemplos de equipos de red incluyen, entre otros, equipos de red central en una red central (por ejemplo, equipos que implementan una AMF o SMF).

El equipo 26 de red de la presente memoria puede realizar el procesamiento de la presente memoria implementando cualquier medio o unidad funcional. En una realización, por ejemplo, el equipo 26 de red comprende circuitos respectivos configurados para realizar las etapas que se muestran en la fig. 7. Los circuitos a este respecto pueden comprender circuitos dedicados a realizar cierto procesamiento funcional y/o uno o más microprocesadores junto con la memoria. En realizaciones que emplean memoria, que puede comprender uno o varios tipos de memoria, tales como memoria de solo lectura (ROM), memoria de acceso aleatorio, memoria caché, dispositivos de memoria flash, dispositivos de almacenamiento óptico, etc., la memoria almacena código de programa que, cuando es ejecutado por uno o más microprocesadores, lleva a cabo las técnicas descritas en la presente memoria. Es decir, en algunas realizaciones, la memoria del equipo 26 de red contiene instrucciones ejecutables por los circuitos de procesamiento por lo que el equipo 26 de red está configurado para llevar a cabo el procesamiento en la presente memoria.

La fig. 11A ilustra detalles adicionales del equipo 26 de red según una o más realizaciones. Como se muestra, el equipo 26 de red incluye un circuitos 500 de procesamiento y circuitos 510 de comunicaciones. Los circuitos 510 de comunicaciones están configurados para comunicarse con otro equipo en la red 10 (por ejemplo, otro equipo de red y/o equipo 12 de usuario y/o ICC 12A). Los circuitos 500 de procesamiento están configurados para realizar el procesamiento descrito anteriormente, por ejemplo, en la fig. 7A y/o 7B, tal como ejecutando instrucciones almacenadas en la memoria 520. Los circuitos 500 de procesamiento en este sentido pueden implementar ciertos medios o unidades funcionales.

La fig. 11B, a este respecto, ilustra detalles adicionales del equipo 26 de red según una o más realizaciones. Como se muestra, el equipo 26 de red puede incluir una unidad o módulo 530 de recepción para recibir al menos una parte de un identificador oculto de suscripción para un abonado, en donde el identificador oculto de suscripción contiene un identificador oculto de suscripción para el abonado. También se puede incluir una unidad o módulo 540 de determinación para determinar a partir de al menos una parte del identificador oculto de suscripción un código de subdominio que indica un cierto subdominio, entre múltiples subdominios de una red doméstica del abonado, al que está asignado el abonado. Además, puede incluirse una unidad o módulo 550 de selección para seleccionar, basándose en el código de subdominio y entre múltiples instancias de una función de red de proveedor en la red doméstica asignada respectivamente para proporcionar un servicio para abonados asignados a diferentes subdominios, un instancia de la función de red de proveedor para proporcionar el servicio al abonado.

El equipo 40 de red de este documento puede realizar el procesamiento en la presente memoria implementando cualquier medio o unidad funcional. En una realización, por ejemplo, el equipo 40 de red comprende circuitos respectivos configurados para realizar las etapas que se muestran en la fig. 8 y/o en la fig. 9. Los circuitos en este sentido pueden comprender circuitos dedicados a realizar cierto procesamiento funcional y/o uno o más microprocesadores junto con la memoria. En realizaciones que emplean memoria, que puede comprender uno o varios tipos de memoria, tales como memoria de solo lectura (ROM), memoria de acceso aleatorio, memoria caché, dispositivos de memoria flash, dispositivos de almacenamiento óptico, etc., la memoria almacena código de programa que, cuando es ejecutado por uno o más microprocesadores, lleva a cabo las técnicas descritas en la presente memoria. Es decir, en algunas realizaciones, la memoria del equipo 40 de red contiene instrucciones ejecutables por los circuitos de procesamiento por lo que el equipo 40 de red está configurado para llevar a cabo el procesamiento en la presente memoria.

La fig. 12A ilustra detalles adicionales del equipo 40 de red según una o más realizaciones. Como se muestra, el equipo 40 de red incluye circuitos 600 de procesamiento y circuitos 510 de comunicaciones. Los circuitos 510 de comunicaciones están configurados para comunicarse con otro equipo en la red 10 (por ejemplo, otro equipo de red y/o equipo 12 de usuario y/o ICC 12A). Los circuitos 600 de procesamiento están configurados para realizar el procesamiento descrito anteriormente, por ejemplo, en la fig. 8, tal como por ejemplo mediante la ejecución de instrucciones almacenadas en la memoria 620. Los circuitos 600 de procesamiento en este sentido pueden implementar ciertos medios o unidades funcionales.

La fig. 12B, a este respecto, ilustra detalles adicionales del equipo 40 de red según una o más realizaciones. Como se muestra, el equipo 40 de red puede incluir una unidad o módulo 630 de obtención para obtener un código de subdominio que indica un determinado subdominio, de entre múltiples subdominios de una red doméstica de un abonado, al que está asignado el abonado. También se puede incluir una unidad o módulo 640 de transmisión para transmitir información que configura otro equipo de red para asociar el código de subdominio con una determinada instancia de una función de red de proveedor entre múltiples instancias de la función de red de proveedor en la red doméstica que se asignan respectivamente para proporcionar un servicio para abonados asignados a diferentes subdominios de la red doméstica.

La fig. 13A ilustra detalles adicionales del equipo 40 de red según aún otras realizaciones. Como se muestra, el equipo 40 de red incluye circuitos 700 de procesamiento y circuitos 710 de comunicaciones. Los circuitos 710 de comunicaciones están configurados para comunicarse con otro equipo en la red 10 (por ejemplo, otro equipo de red y/o equipo 12 de usuario y/o ICC 12A). Los circuitos 700 de procesamiento están configurados para realizar el procesamiento descrito anteriormente, por ejemplo, en la fig. 9, tal como ejecutando instrucciones almacenadas en la memoria 720. Los circuitos 700 de procesamiento en este sentido pueden implementar ciertos medios o unidades funcionales.

La fig. 13B, a este respecto, ilustra detalles adicionales del equipo 40 de red según una o más realizaciones. Como se muestra, el equipo 40 de red puede incluir una unidad o módulo 730 de obtención para obtener un código de subdominio que indica un cierto subdominio, de entre múltiples subdominios de una red doméstica de un abonado, al que está asignado el abonado. También se puede incluir una unidad o módulo 740 de transmisión para transmitir información que configura un equipo de usuario del abonado, o una tarjeta de circuito integrado asociada al abonado, con el código de subdominio obtenido.

El equipo 12 de usuario y/o al ICC 12A en la presente memoria pueden realizar el procesamiento en la presente memoria implementando cualquier medio o unidad funcional. En una realización, por ejemplo, el equipo 12 de usuario y/o la ICC 12A comprenden circuitos respectivos configurados para realizar las etapas que se muestran en la fig. 10. Los circuitos a este respecto pueden comprender circuitos dedicados a realizar cierto procesamiento funcional y/o uno o más microprocesadores junto con la memoria. En realizaciones que emplean memoria, que puede comprender uno o varios tipos de memoria, tales como memoria de solo lectura (ROM), memoria de acceso aleatorio, memoria caché, dispositivos de memoria flash, dispositivos de almacenamiento óptico, etc., la memoria almacena código de programa que, cuando es ejecutado por uno o más microprocesadores, lleva a cabo las técnicas descritas en la presente memoria. Es decir, en algunas realizaciones la memoria del equipo 12 de usuario y/o ICC 12A contiene instrucciones ejecutables por los circuitos de procesamiento por lo que el equipo 12 de usuario y/o ICC 12A está configurado para llevar a cabo el procesamiento en la presente memoria.

La fig. 14A ilustra detalles adicionales del equipo 12 de usuario y/o de la ICC 12A según una o más realizaciones. Como se muestra, el equipo 12 de usuario y/o la ICC 12A incluye circuitos 800 de procesamiento y circuitos 810 de comunicaciones. Los circuitos 810 de comunicaciones están configurados para comunicarse con otro equipo en la red 10 (por ejemplo, equipo de red y/u otro equipo de usuario y/o CCI). Los circuitos 800 de procesamiento están configurados para realizar el procesamiento descrito anteriormente, por ejemplo, en la fig. 10, tal como por ejemplo mediante la ejecución de instrucciones almacenadas en la memoria 820. Los circuitos 800 de procesamiento en este sentido pueden implementar ciertos medios o unidades funcionales.

La fig. 14B a este respecto ilustra detalles adicionales del equipo 12 de usuario y/o de la ICC 12A según una o más realizaciones. Como se muestra, el equipo 12 de usuario y/o la ICC 12A pueden incluir una unidad o módulo 830 de recepción para recibir, desde un equipo de red en una red de comunicación inalámbrica, información que configura el equipo de usuario o la tarjeta de circuito integrado con un código de subdominio que indica un determinado subdominio, de entre múltiples subdominios de una red doméstica del abonado, al que está asignado el abonado. En algunas realizaciones, se incluye además una unidad o módulo 840 de generación para generar un identificador oculto de suscripción para incluir un campo que indica el código de subdominio y una unidad o módulo 850 de transmisión para transmitir un mensaje que incluye el identificador oculto de suscripción.

Los expertos en la técnica también apreciarán que las realizaciones de la presente memoria incluyen además programas informáticos correspondientes.

Un programa informático comprende instrucciones que, cuando se ejecutan en al menos un procesador (por ejemplo, del equipo 26 de red, equipo 40 de red, equipo 12 de usuario o ICC 12A), hacen que el procesador lleve a cabo cualquiera de los procesamientos respectivos descritos anteriormente. Un programa informático en este sentido puede comprender uno o más módulos de código correspondientes a los medios o unidades descritos anteriormente.

Las realizaciones incluyen además un portador que contiene dicho programa informático. Este portador puede comprender uno de entre una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por ordenador.

Por supuesto, la presente invención puede llevarse a cabo de otras maneras distintas de las establecidas específicamente en la presente memoria sin desviarse del alcance de la invención que se define exclusivamente por las reivindicaciones adjuntas.

REIVINDICACIONES

1.- Un método realizado por el equipo (26) de red en una red de comunicación inalámbrica, comprendiendo el método:

la recepción (110) de al menos una parte de un identificador (34) oculto de suscripción para un abonado (13), en donde el identificador (34) oculto de suscripción contiene un identificador (20) permanente de suscripción oculta para el abonado (13), en donde la al menos una parte recibida del identificador (34) oculto de suscripción indica un código (32) de subdominio, en donde el código (32) de subdominio indica un cierto subdominio, de entre múltiples subdominios (30-1, 30 -2,...30-N) de una red doméstica del abonado (13), al que está asignado el abonado (13);

la determinación (120), basada en el código (32) de subdominio y entre múltiples instancias (24-1, 24-2, 24-M) de una función de red de proveedor en la red doméstica asignada respectivamente para proporcionar un servicio a ser consumido por abonados asignados a diferentes subdominios, una instancia de la función de red de proveedor para proporcionar el servicio a ser consumido por el abonado (13).

2.- El método de la reivindicación 1, en donde la determinación de la instancia de la función de red de proveedor para proporcionar el servicio a ser consumido por el abonado (13) también se basa en un identificador de red local.

3.- El método de cualquiera de las reivindicaciones 1-2, que comprende además la recepción de una solicitud de descubrimiento para descubrir una o más instancias de la función de red de proveedor en la red doméstica para proporcionar el servicio a ser consumido por el abonado (13) y responder a la solicitud de descubrimiento con la instancia seleccionada de la función de red de proveedor.

4.- El método de cualquiera de las reivindicaciones 1-3, en donde el equipo (26) de red implementa una función de repositorio de red, NRF.

5.- El método de cualquiera de las reivindicaciones 1-4, en donde la función de red de proveedor es una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.

6.- Un método realizado por un equipo de red en una red de comunicación inalámbrica, comprendiendo el método:

la obtención (210) de un código (32) de subdominio que indica un determinado subdominio, de entre múltiples subdominios (30-1, 30-2,...30-N) de una red doméstica de un abonado (13), al que está asignado el abonado (13); y

la transmisión (220) de información que configura otros equipos (26) de red para asociar el código (32) de subdominio con una determinada instancia de una función de red de proveedor entre múltiples instancias (24-1, 24-2,... 24-M) de la función de red de proveedor en la red doméstica que se asignan respectivamente para proporcionar un servicio a ser consumido por abonados asignados a diferentes subdominios (30-1, 30-2,... 30-N) de la red doméstica.

7.- El método de la reivindicación 6, en donde la información incluye el código (32) de subdominio e información de enrutamiento para la instancia determinada, de tal manera que la información configura el otro equipo (26) de red para asociar el código (32) de subdominio con la información de enrutamiento.

8.- El método de cualquiera de las reivindicaciones 6-7, en donde el equipo de red implementa una función de operación y mantenimiento, la instancia determinada de la función de red de proveedor, o un proxy para la instancia determinada de la función de red de proveedor.

9.- El método de cualquiera de las reivindicaciones 6-8, en donde la función de red de proveedor es una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.

10.- El método de cualquiera de las reivindicaciones 6-9, en donde el otro equipo (26) de red implementa una función de repositorio de red.

11.- Un método realizado por un equipo de usuario o una tarjeta de circuito integrado asociada con un abonado (13), comprendiendo el método:

La recepción (410), desde un equipo de red en una red de comunicación inalámbrica, de información que configura el equipo de usuario o la tarjeta de circuito integrado con un código (32) de subdominio que indica un determinado subdominio, de entre múltiples subdominios (30 -1, 30-2,...30-N) de una red doméstica del abonado (13), al que está asignado el abonado (13); y

La transmisión (430) de un mensaje que incluye un identificador (34) oculto de suscripción, en donde el identificador (34) oculto de suscripción contiene un identificador (20) permanente de suscripción oculta para el abonado (13) e indica el código (32) de subdominio, y en donde el mensaje se transmite a una entidad de red

para determinar una instancia de la función de red de proveedor para proporcionar el servicio a ser consumido por el abonado (13) en base al código (32) de subdominio.

5 12.- El método de la reivindicación 11, en donde el equipo de red implementa una función de operación y mantenimiento, una instancia de una función de red de proveedor en la red doméstica que va a proporcionar o es capaz de proporcionar un servicio a ser consumido por el abonado (13), o un proxy para una o más instancias de la función de red de proveedor.

13.- El método de la reivindicación 12, en donde la función de red de proveedor es una función de gestión de datos unificados, una función de revelación de identificador de suscripción o una función de servidor de autenticación.

10 14.- El equipo (26) de red configurado para su uso en una red de comunicación inalámbrica, el equipo (26) de red configurado para:

15 recibir al menos una parte de un identificador (34) oculto de suscripción para un abonado (13), en donde el identificador (34) oculto de suscripción contiene un identificador (20) permanente de suscripción oculta para el abonado (13), en donde la al menos una parte recibida del identificador (34) oculto de suscripción indica un código (32) de subdominio, en donde el código (32) de subdominio indica un cierto subdominio, de entre múltiples subdominios (30-1, 30-2,...30-N) de una red doméstica del abonado (13), al que está asignado el abonado (13);

20 determinar, basándose en el código (32) de subdominio y de entre múltiples instancias (24-1, 24-2,... 24-M) de una función de red de proveedor en la red doméstica asignada respectivamente para proporcionar un servicio a ser consumido por abonados asignados a diferentes subdominios, una instancia de la función de red de proveedor para proporcionar el servicio a ser consumido por el abonado (13).

15.- El equipo de red configurado para su uso en una red de comunicación inalámbrica, el equipo de red configurado para:

25 obtener un código (32) de subdominio que indique un determinado subdominio, de entre múltiples subdominios (30-1, 30-2,...30-N) de una red doméstica de un abonado (13), al que está asignado el abonado (13); y

transmitir información que configura otros equipos (26) de red para asociar el código (32) de subdominio con una determinada instancia de una función de red de proveedor entre múltiples instancias (24-1, 24-2,... 24-M) de la función de red de proveedor en la red doméstica que se asignan respectivamente para proporcionar un servicio a ser consumido por abonados asignados a diferentes subdominios (30-1, 30-2,... 30-N) de la red doméstica.

30 16.- Un equipo de usuario o una tarjeta de circuito integrado configurada para asociarse a un abonado (13), el equipo de usuario o tarjeta de circuito integrado configurado para:

35 recibir, desde equipos de red en una red de comunicación inalámbrica, información que configura el equipo de usuario o la tarjeta de circuito integrado con un código (32) de subdominio que indica un determinado subdominio, de entre múltiples subdominios (30-1, 30-2,...30-N) de una red doméstica del abonado (13), al que está asignado el abonado (13); y

transmitir un mensaje que incluye un identificador (34) oculto de suscripción, donde el identificador (34) oculto de suscripción contiene un identificador (20) permanente de suscripción oculta para el abonado (13) e indica el subdominio, y en donde el mensaje se transmite a una entidad de red para determinar una instancia de la función de red de proveedor para proporcionar el servicio a ser consumido por el abonado (13).

40 17.- Un programa informático que comprende instrucciones que, cuando las ejecuta al menos un procesador del equipo (26, 40) de red, hace que el equipo (26, 40) de red realice el método de cualquiera de las reivindicaciones 1-10.

45 18.- Programa informático que comprende instrucciones que, al ser ejecutado por al menos un procesador de un equipo (12) de usuario o tarjeta (12A) de circuito integrado configurado para asociarse a un abonado (13), hace que el equipo (12) de usuario o la tarjeta (12A) de circuito integrado realice el método de cualquiera de las reivindicaciones 11-13.

19.- Un portador que contiene el programa informático de cualquiera de las reivindicaciones 17-18, en donde el portador es una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por ordenador.

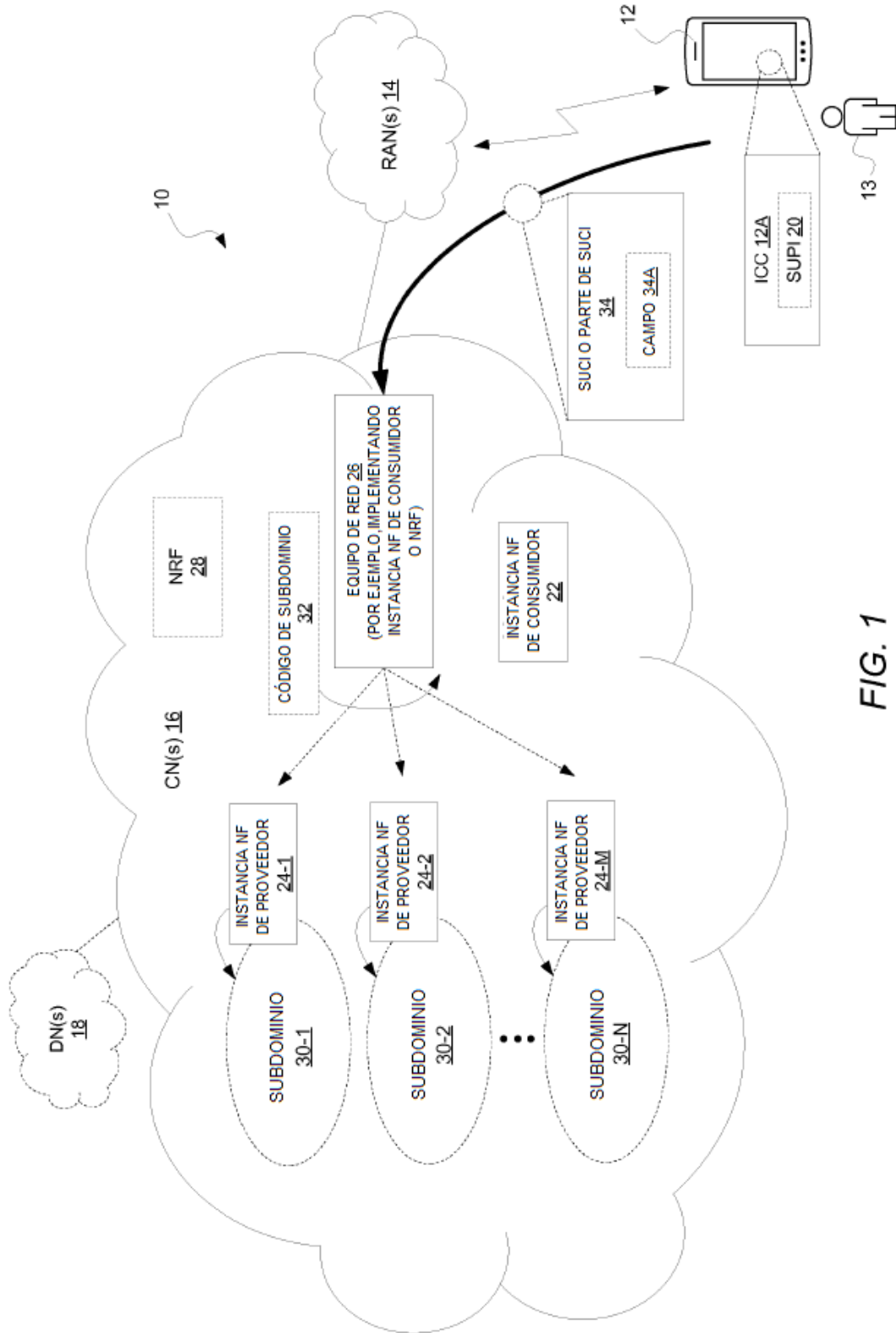


FIG. 1



FIG. 2A

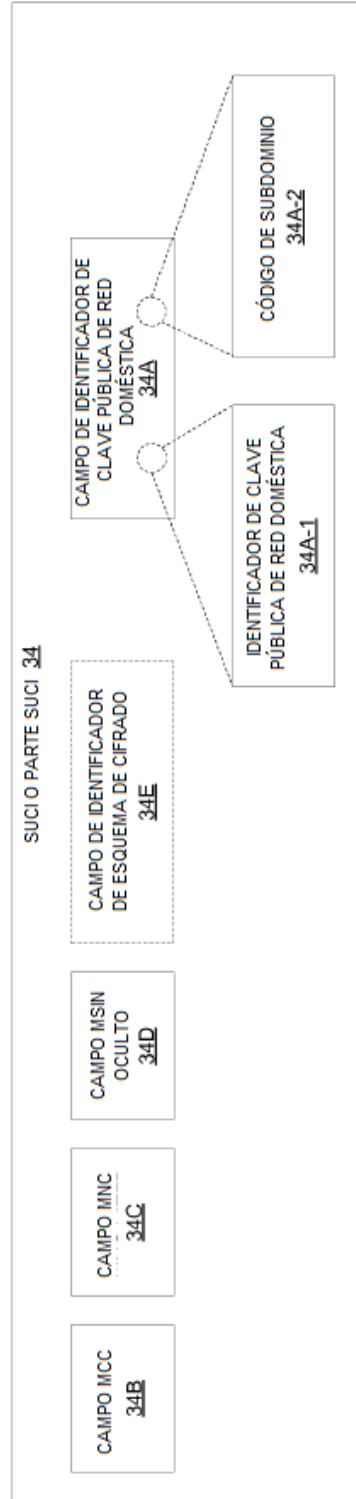


FIG. 2B

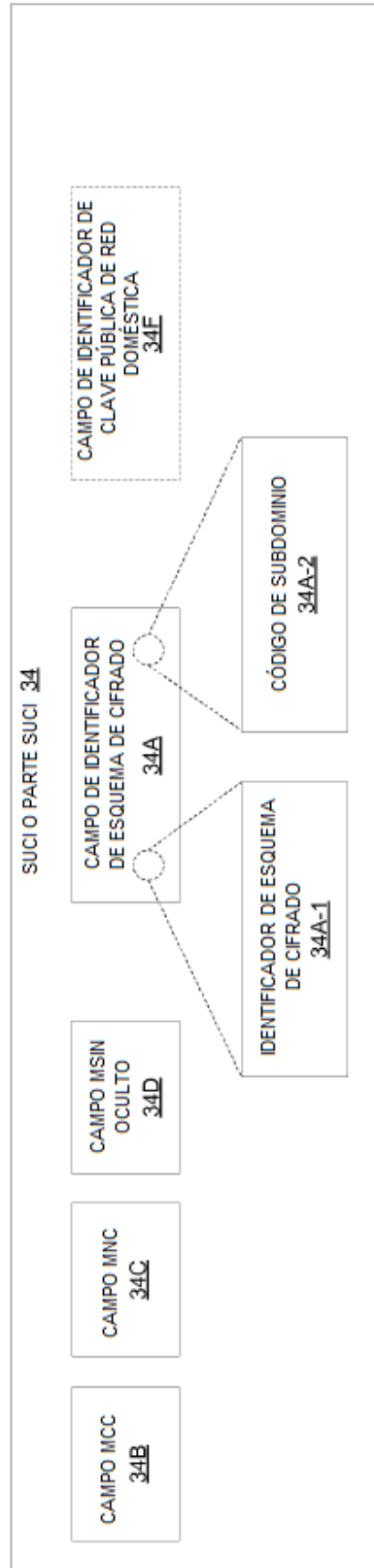


FIG. 2C

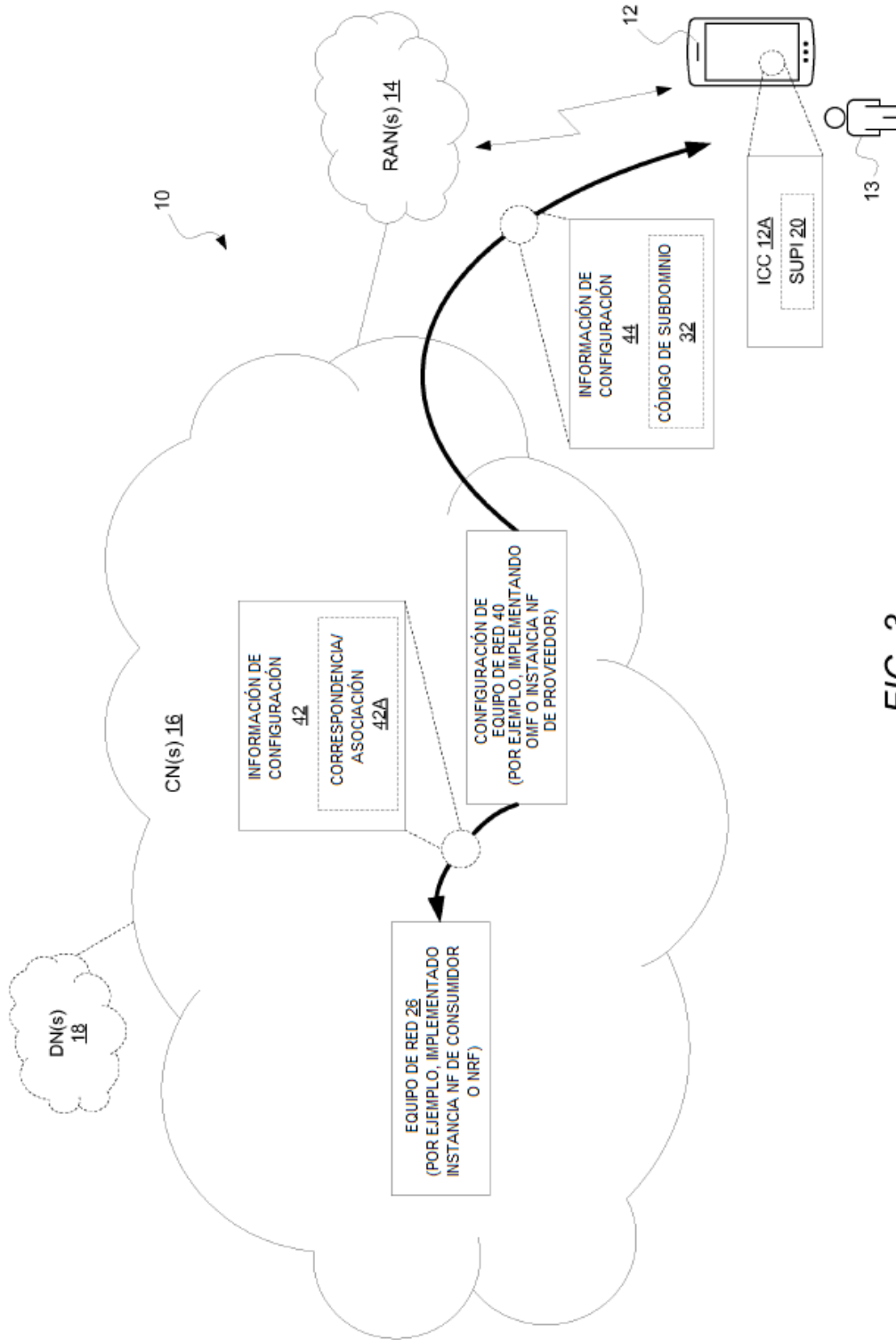


FIG. 3

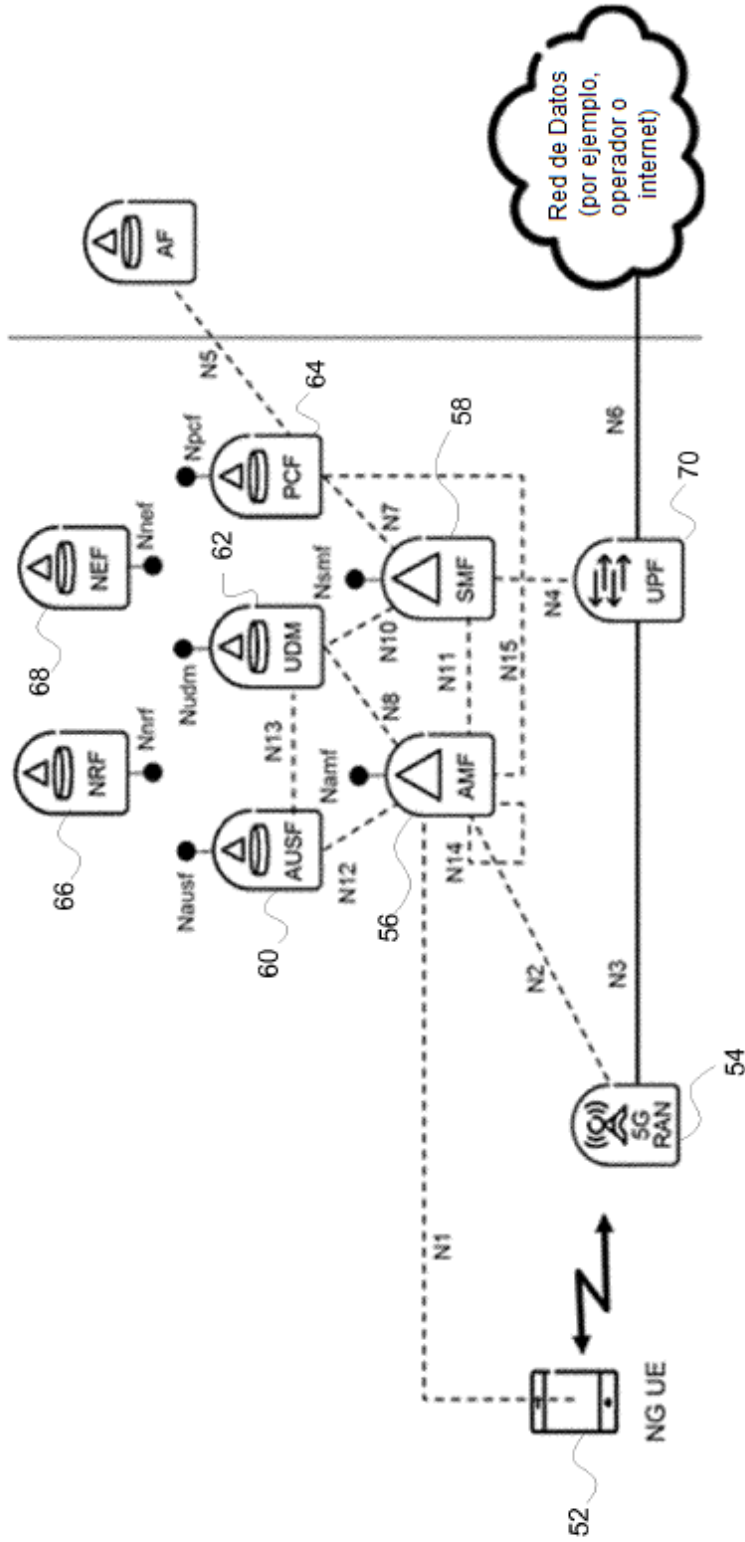


FIG. 4

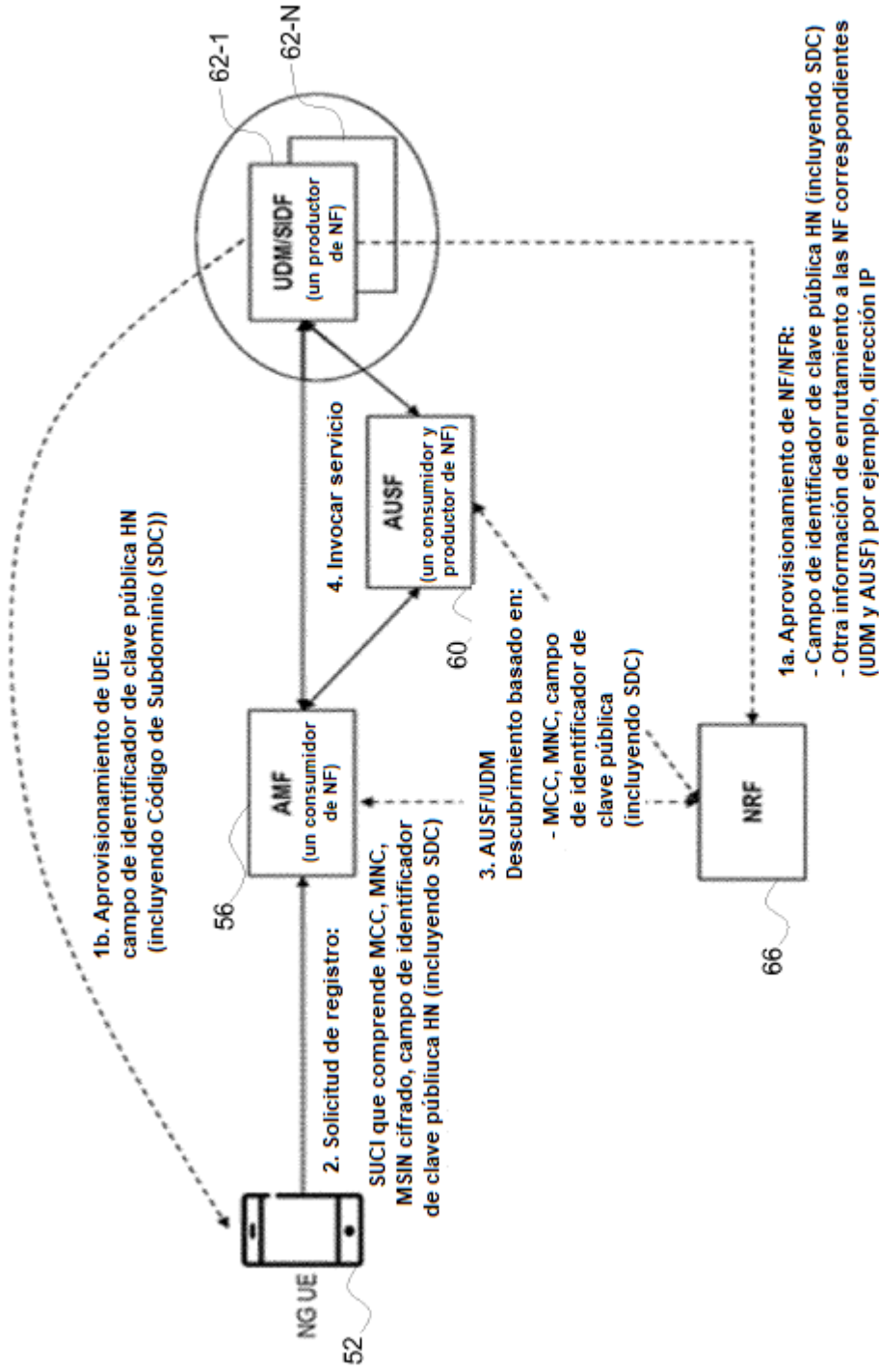


FIG. 5

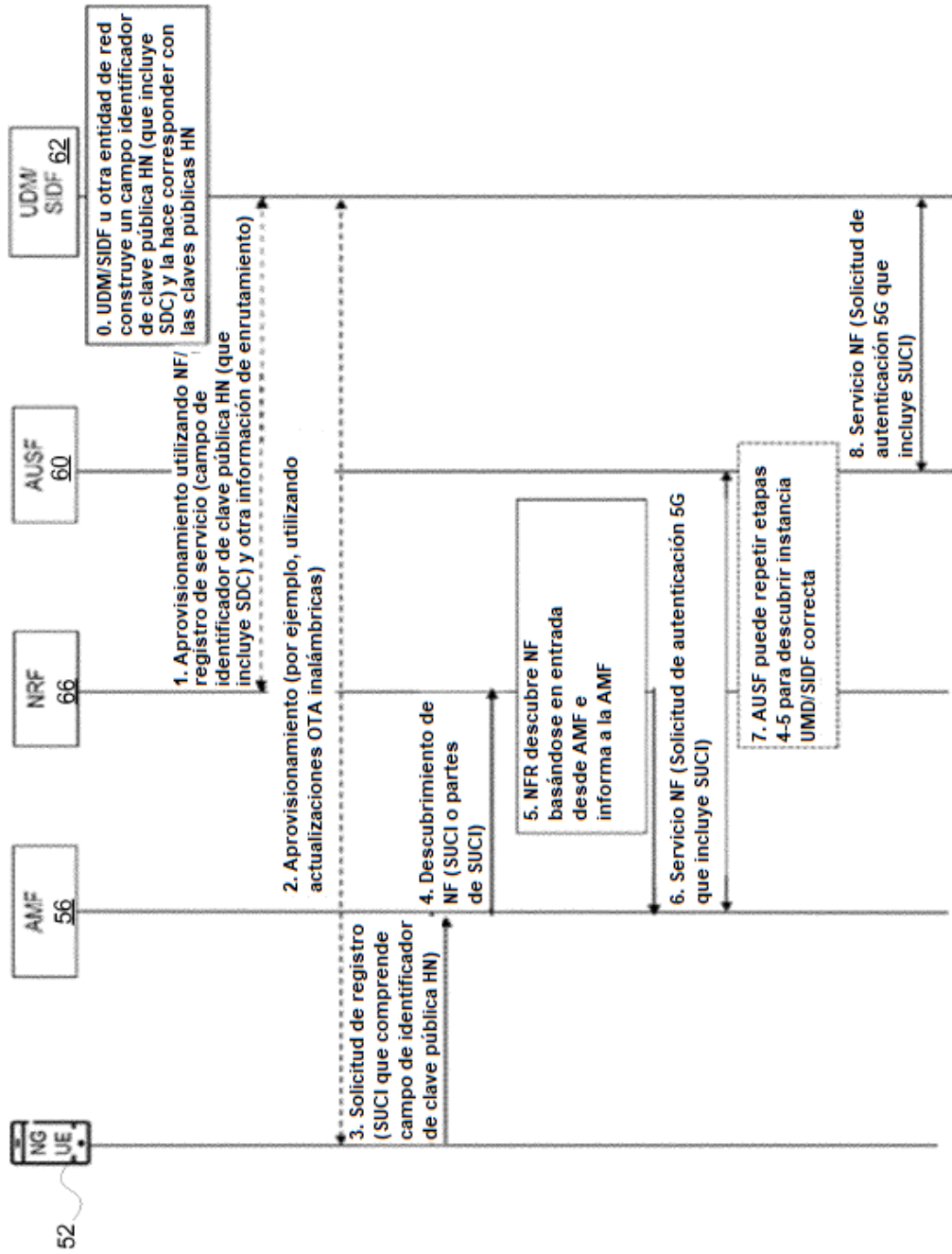


FIG. 6

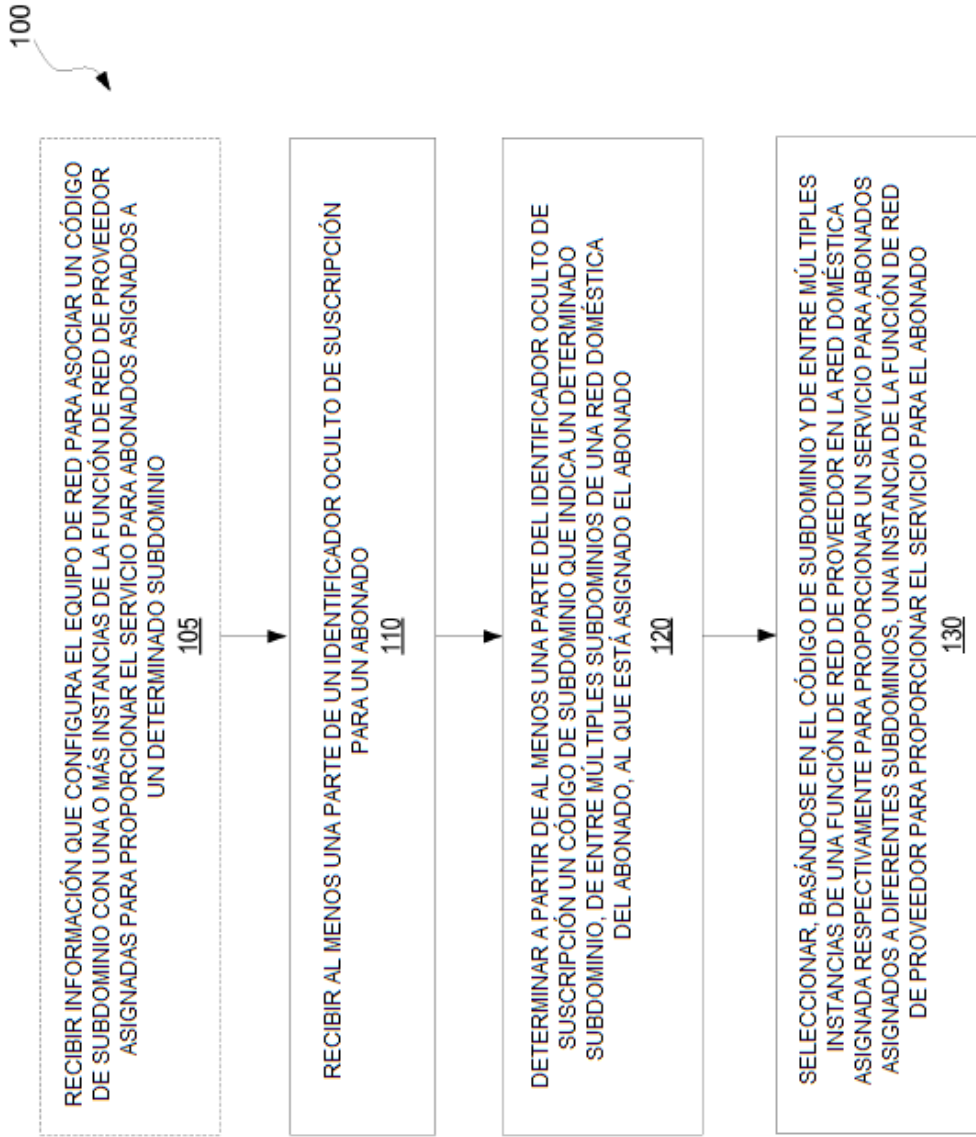


FIG. 7A

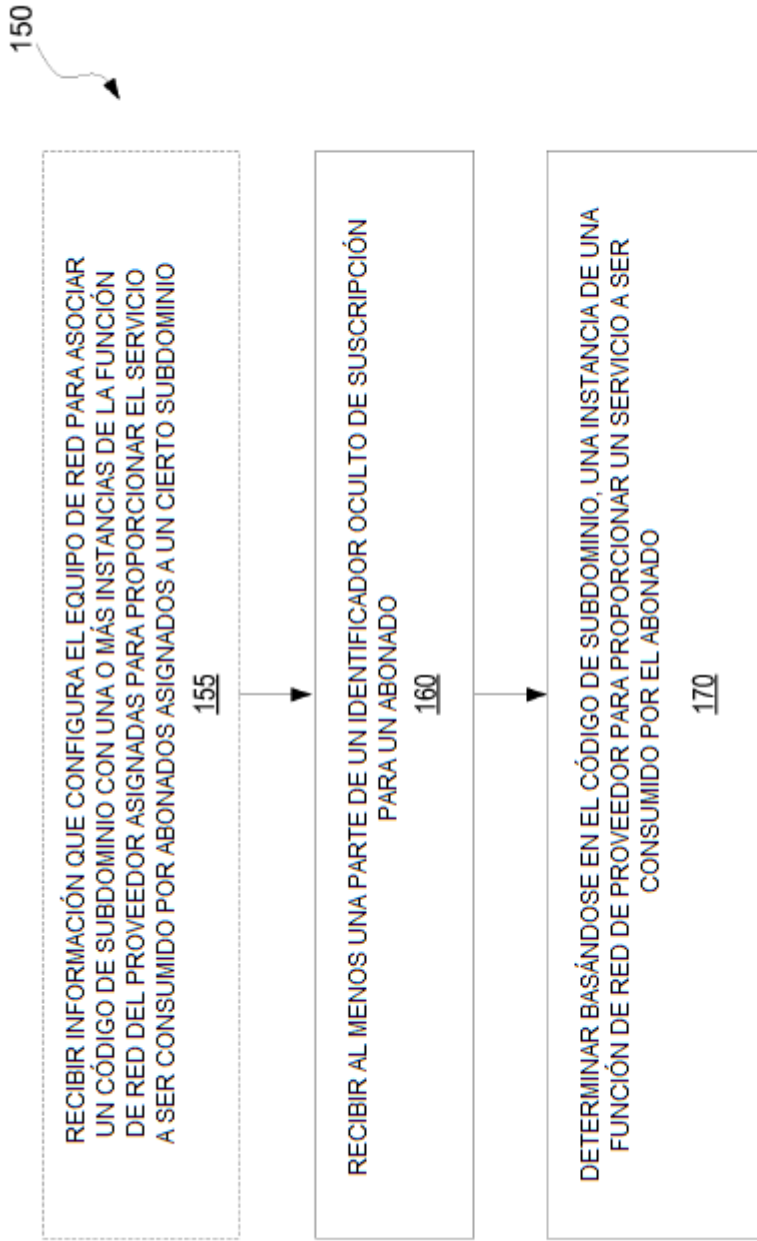


FIG. 7B

200

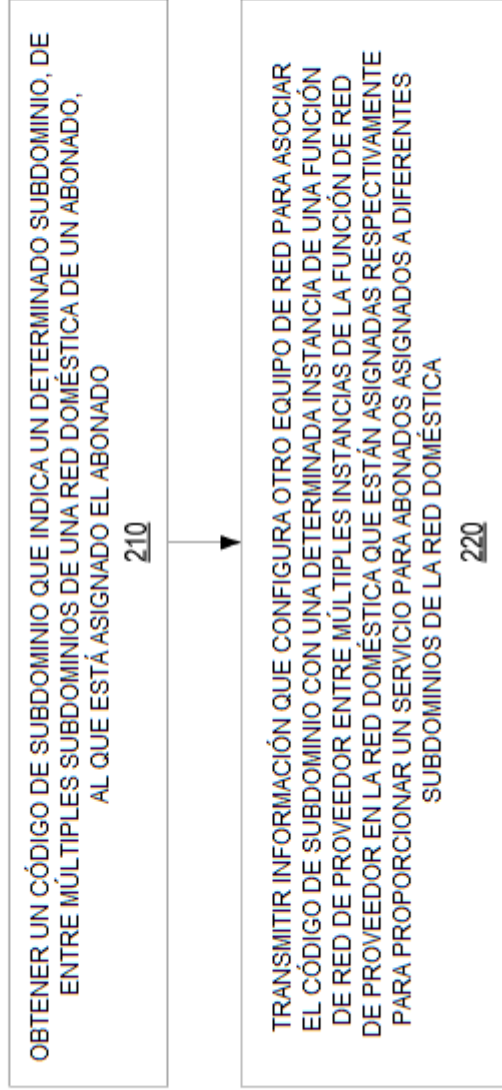


FIG. 8

300

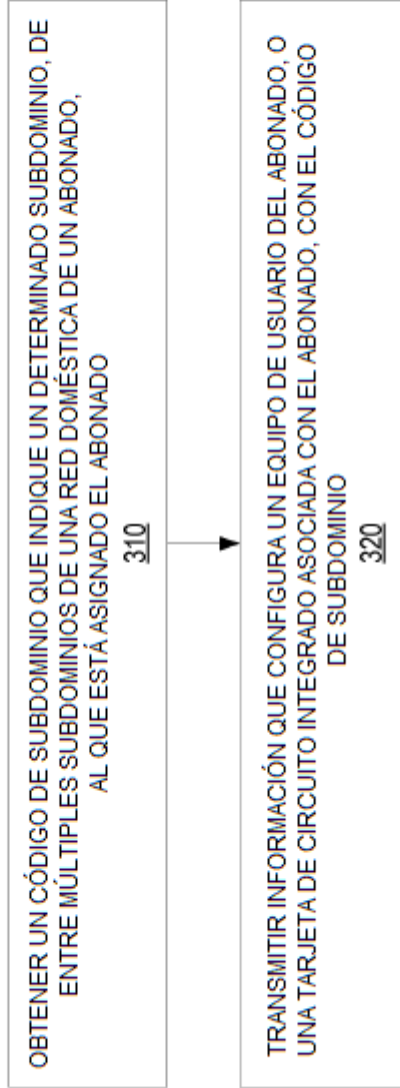


FIG. 9

400

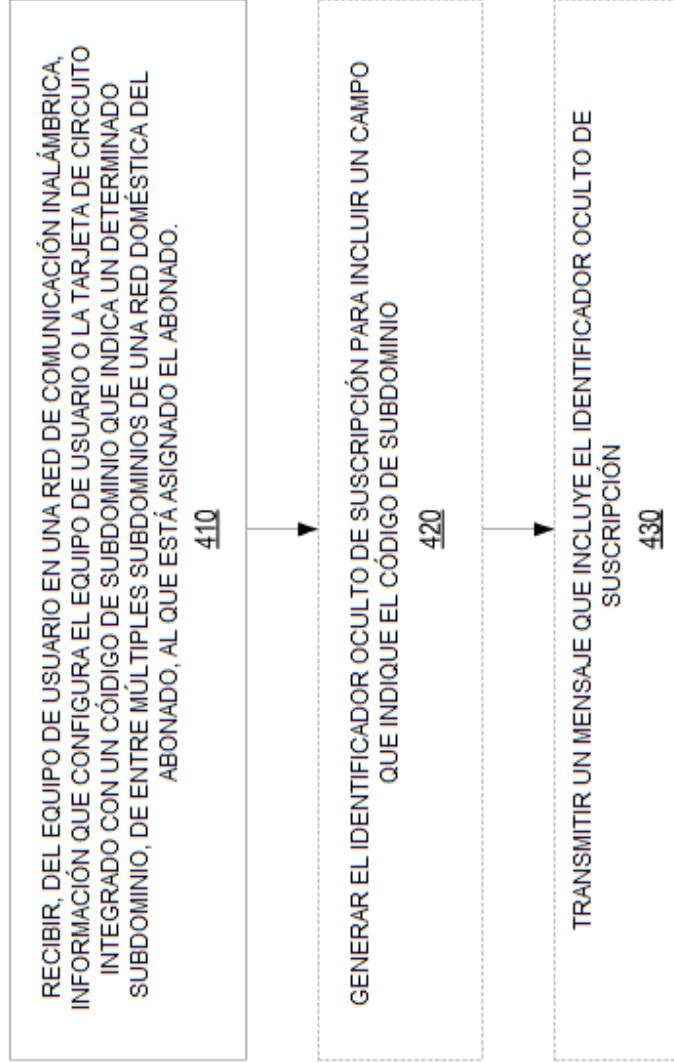


FIG. 10

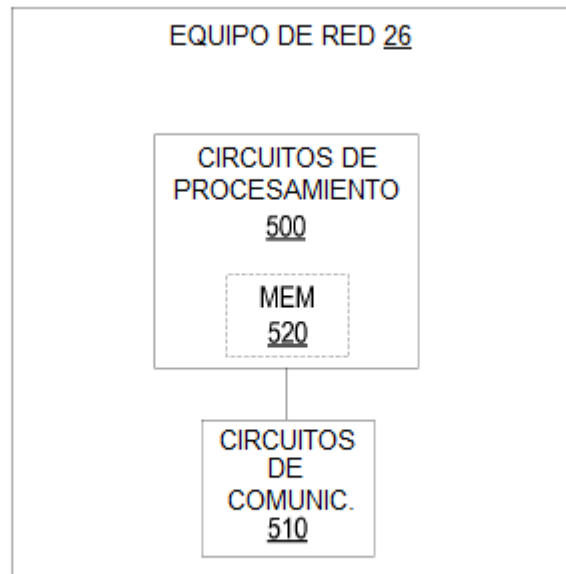


FIG. 11A



FIG. 11B

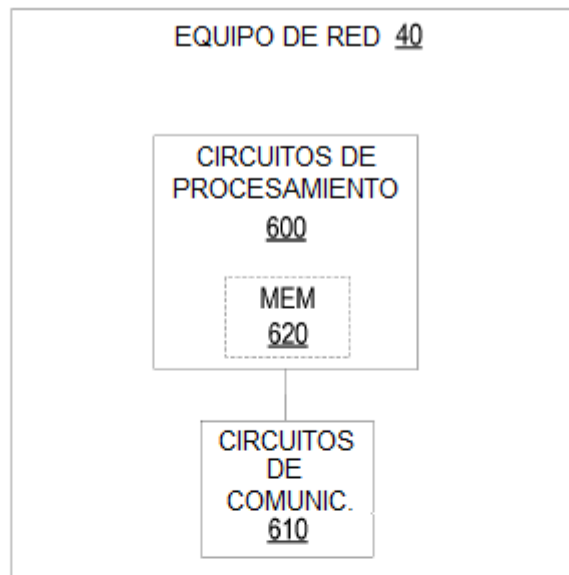


FIG. 12A

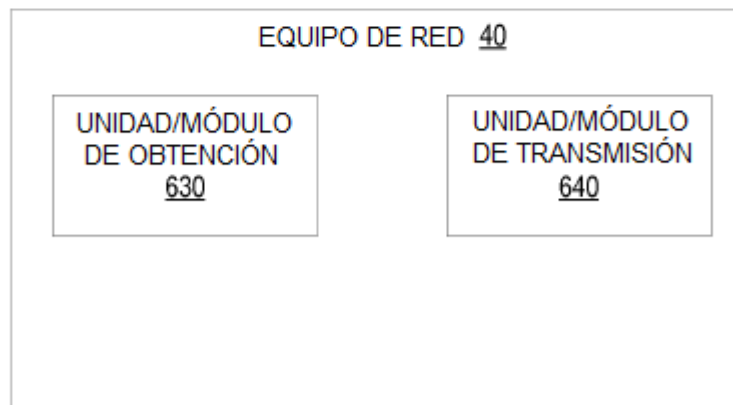


FIG. 12B

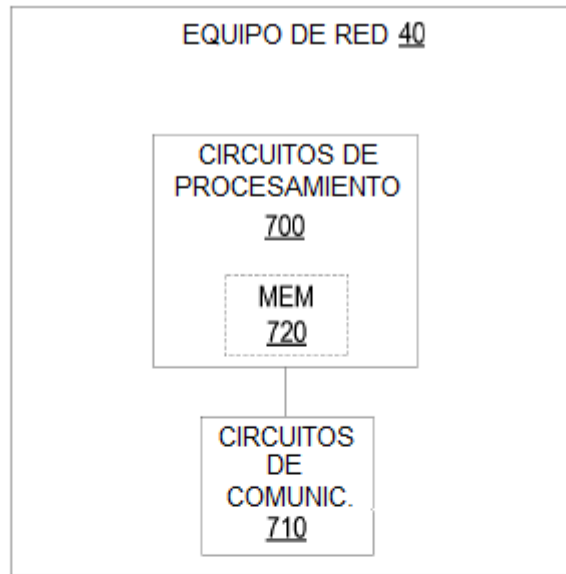


FIG. 13A

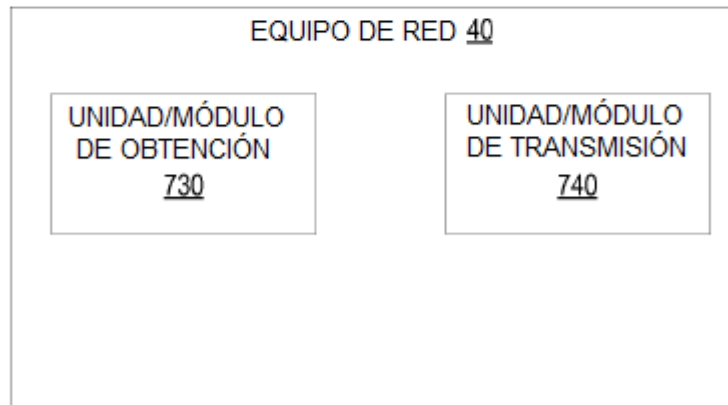


FIG. 13B

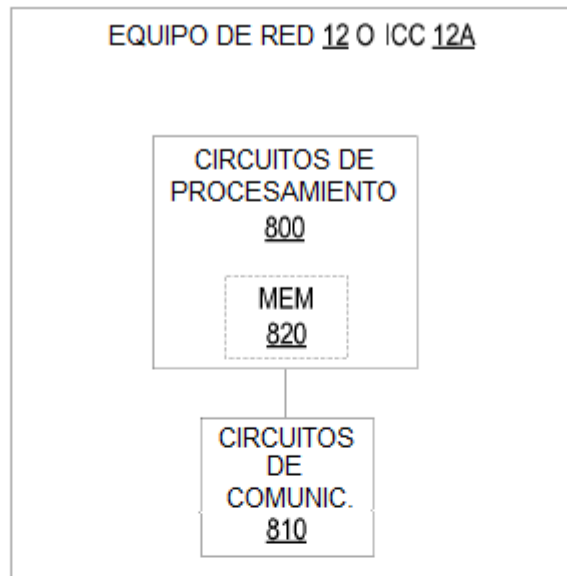


FIG. 14A

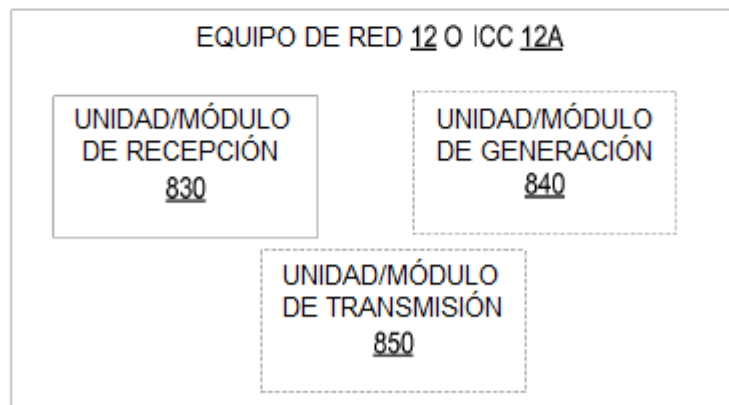


FIG. 14B