

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 943 849**

51 Int. Cl.:

H04W 12/069 (2011.01)

H04L 9/40 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **03.09.2019** **PCT/EP2019/073411**

87 Fecha y número de publicación internacional: **21.01.2021** **WO21008716**

96 Fecha de presentación y número de la solicitud europea: **03.09.2019** **E 19762949 (6)**

97 Fecha y número de publicación de la concesión europea: **01.03.2023** **EP 4000296**

54 Título: **Técnica para el manejo de certificados en un dominio de red de núcleo**

30 Prioridad:

17.07.2019 EP 19382607

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

16.06.2023

73 Titular/es:

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

72 Inventor/es:

MARTINEZ DE LA CRUZ, PABLO y
GARCIA GARCIA, FRANCISCO JAVIER

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 943 849 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

Técnica para el manejo de certificados en un dominio de red de núcleo

Campo técnico

- 5 La presente descripción se refiere en general a los sistemas de comunicaciones móviles y, en particular, a un dominio de red central de una red de comunicaciones móviles. Más detalladamente, la descripción se refiere a aparatos que proporcionan funciones de repositorio de red y funciones de red en un dominio de red central, a un sistema de dominio de red central, a métodos correspondientes y a un producto de programa informático.

Antecedentes

- 10 El Proyecto de Asociación de 3ª Generación (3GPP) está desarrollando especificaciones técnicas (TS) para los sistemas de comunicaciones de 5ª Generación (5G). La especificación técnica TS 23.501 V15.4.0 (2018-12) de 3GPP define los aspectos arquitectónicos de una arquitectura 5G basada en servicios (SBA). Según esta SBA, la función de red (NF) usa interacciones basadas en servicios para consumir servicios de otras NF. El descubrimiento de servicios y de las NF que los producen es proporcionado por una función de repositorio de red (NRF).
- 15 Las NF que producen servicios registran, actualizan o dan de baja sus perfiles en la NRF. Las NF que consumen servicios descubren los servicios que ofrecen las instancias productoras NF consultando a la NRF sobre las instancias NF que ofrecen servicios de un tipo dado. Las NF pueden suscribirse y darse de baja de los cambios en el estado de las NF registradas en la NRF. En función de dichas suscripciones, la NRF notificará a las NF los cambios de estado de otras NF. El documento TR 33.855 V1.6.0 de 3GPP describe aspectos de seguridad de la arquitectura basada en servicios (SBA) 5G.
- 20 Los mecanismos de seguridad de la SBA también se especifican en el documento TS 33.501 V15.3.1 de 3GPP. Por ejemplo, la Sección 13.1 de este documento define que las NF admitirán seguridad de capa de transporte (TLS) con tanto certificados del lado del servidor como del lado del cliente. Este modo TLS generalmente se denomina TLS mutuo (mTLS).
- 25 La TLS usa certificados X.509 que contienen una clave pública y están firmados digitalmente por una autoridad de certificación (CA). La CA tiene un certificado, que puede estar firmado por otra CA. Una CA raíz es una CA cuyo certificado no está firmado por ninguna otra CA. Una cadena de certificados comienza con una CA raíz, incluye todas las CA intermedias (pero no la CA raíz) y finaliza con el certificado de cliente o servidor, y cada certificado se firma en relación con la clave pública codificada en el certificado anterior.
- 30 Una parte que recibe un certificado X.509 debe validarlo. La validación implica atravesar la cadena de certificados y validar todas las firmas de los certificados. Cuando todas las firmas son válidas, el certificado se considera válido.
- Cuando un certificado de una NF consumidora de servicios es validado con éxito por una NF productora de servicios, la NF productora de servicios autentica la NF consumidora de servicios. Luego, la NF productora de servicios necesita autorizar a la NF consumidora de servicios, es decir, verificar que la NF consumidora de servicios tenga derecho a consumir los servicios ofrecidos por la NF productora de servicios.
- 35 Según el documento TS 33.501, la autorización basada en token se puede usar opcionalmente. Cuando no se use, la NF productora de servicios verificará las autorizaciones de las NF consumidoras de servicios en función de las políticas locales.
- 40 Cuando se usa mTLS, la gestión del ciclo de vida de los certificados de CA se vuelve obligatoria. Hacer dicha gestión a escala es una tarea compleja, requiere integraciones costosas e introduce complejidades. Por otro lado, cuando no se usa la autorización basada en token y la autorización se basa en políticas locales, es necesario configurar listas de control de acceso (ACL) o mecanismos equivalentes en las NF productoras de servicios y, al instanciar una nueva instancia NF en la red, las ACL de todas las NF productoras de servicios deben actualizarse, lo que también es complejo y costoso.

Compendio

- 45 Existe la necesidad de una técnica que proporcione un manejo eficiente de los certificados de CA en un dominio de red central.
- 50 Según un primer aspecto, se proporciona un aparato configurado para proporcionar una función de repositorio de red, NRF, en un dominio de red central de una red de comunicaciones móviles, en donde la NRF está configurada para registrar los perfiles de la función de red, NF, para el descubrimiento de NF, y en donde se han emitido certificados de NF a las NF, cada certificado de NF incluye una clave pública de la NF respectiva y al menos una firma de al menos una autoridad de certificación, CA. El aparato está configurado para recibir, de una NF que se registra que tiene un certificado de NF, información de perfil que comprende una identidad de NF de la NF que se registra, un tipo de NF de la NF que se registra y al menos un certificado de CA de al menos una CA que firmó el certificado de NF emitido a la NF que se registra. El aparato está además configurado para almacenar la información de perfil recibida en un

repositorio.

Como ejemplo, los perfiles de NF de algunas o todas las NF pueden extenderse cada uno por un atributo que contiene uno o más o todos los certificados de CA que se requieren para validar el certificado de la NF asociada con el perfil de NF correspondiente. La validación puede ocurrir en particular durante un procedimiento de establecimiento de enlace mutuo entre una NF consumidora de servicios y una NF productora de servicios. El procedimiento de establecimiento de enlace puede ajustarse al protocolo TLS.

En una variante, el certificado de NF emitido a la NF que se registra incluye además un identificador de NF que es diferente de la identidad de NF de la NF que se registra. En esta variante, la información de perfil recibida puede comprender además el identificador de NF. Como ejemplo, los perfiles de NF de algunas o todas las NF pueden extenderse cada uno por un atributo adicional que contiene el identificador de NF de la NF asociada con el perfil de NF correspondiente. El identificador de NF se puede usar con fines de validación durante un procedimiento de establecimiento de enlace mutuo entre una NF consumidora de servicios y una NF productora de servicios.

Como ejemplo, el identificador de NF puede ser el identificador particular que se incluye en un campo de sujeto del certificado de NF. En algunos casos, el identificador de NF puede tomar la forma de uno de un nombre de dominio completo, FQDN, y un identificador de un marco de identidad de producción seguro para todos, SPIFFE.

A diferencia del identificador de NF, la identidad de NF "regular" puede hacer que una NF (que está asociada con el perfil de NF que incluye esta identidad de NF) se pueda descubrir o distinguir en el dominio de red central.

El aparato puede configurarse para recibir una solicitud de descubrimiento que indique al menos un tipo de NF. En una implementación de este tipo, el aparato puede configurarse además para acceder al repositorio para identificar uno o más perfiles de NF que coincidan al menos con el tipo de NF indicado y para enviar una respuesta de descubrimiento que incluye información de descubrimiento del uno o más perfiles de NF coincidentes. La información de descubrimiento incluye en algunos casos al menos el uno o más certificados de CA almacenados para el perfil de NF respectivo.

El aparato puede configurarse además para recibir, de una primera NF, una solicitud de actualización que incluye información actualizada del certificado de CA. Luego, el aparato puede actualizar la información de perfil de la primera NF en función de la información de certificado de CA actualizada. En particular, el aparato puede configurarse para identificar una o más segundas NF asociadas con la primera NF a través de una suscripción de notificaciones y enviar al menos una parte de la información actualizada del certificado de CA a la una o más segundas NF identificadas.

El aparato puede configurarse además para recibir, de una primera NF, una solicitud de actualización que incluye información actualizada del identificador de NF. Luego, el aparato puede actualizar la información de perfil de la primera NF en función de la información actualizada del identificador de NF. En particular, el aparato puede configurarse para identificar una o más segundas NF asociadas con la primera NF a través de una suscripción de notificaciones y enviar al menos una parte de la información actualizada del identificador de NF a la una o más segundas NF identificadas.

Según un segundo aspecto, se proporciona un aparato configurado para proporcionar una función de red, NF, en un dominio de red central de una red de comunicaciones móviles, en donde se ha emitido un certificado de NF a la NF, el certificado de NF que incluye una clave pública de la NF y al menos una firma de al menos una autoridad de certificación, CA. El aparato del segundo aspecto está configurado para obtener al menos un certificado de CA de la al menos una CA que firmó el certificado de NF emitido a la NF, y para enviar información de perfil a una función de repositorio de red, NRF, configurada para registrar perfiles de NF para el descubrimiento de NF en el dominio de red central, la información de perfil comprende una identidad de NF de la NF que se registra, un tipo de NF de la NF que se registra y el al menos un certificado de CA.

El certificado de NF emitido a la NF que se registra puede incluir además un identificador de NF que es diferente de la identidad de NF de la NF que se registra. La información de perfil recibida puede comprender además el identificador de NF, por ejemplo, en forma de un atributo (por ejemplo, además de un atributo que define el al menos un certificado de CA).

El aparato del segundo aspecto puede configurarse para enviar, a otra NF, el certificado de NF en un procedimiento de establecimiento de enlace con la otra NF. El procedimiento de establecimiento de enlace puede ajustarse a TLS (por ejemplo, mTLS).

El aparato del segundo aspecto puede configurarse para enviar, a la NRF, una solicitud de descubrimiento que indique al menos un tipo de NF. El aparato puede configurarse además para recibir, de la NRF, una respuesta de descubrimiento que incluye información de descubrimiento de uno o más perfiles de NF que coincidan al menos con el tipo de NF, la información de descubrimiento incluye el al menos un certificado de CA almacenado para el perfil de NF respectivo (y, opcionalmente, el identificador de NF asociado). El aparato puede almacenar la información de descubrimiento en un almacenamiento.

En particular, el aparato puede configurarse además para recibir, de otra NF para la cual se ha recibido anteriormente información de descubrimiento de la NRF, el certificado de NF emitido a esa otra NF, para leer el al menos un certificado de CA incluido en la información de descubrimiento del almacenamiento y para validar el certificado de NF usando el certificado de CA leído del almacenamiento. El certificado de NF se puede recibir en el contexto de un procedimiento de establecimiento de enlace con la otra NF (por ejemplo, conforme a TLS).

El aparato del segundo aspecto puede configurarse para extraer un primer identificador de NF del certificado de NF recibido, para extraer un segundo identificador de NF de la información de perfil y para validar el primer identificador de NF en función del segundo identificador de NF. Como ejemplo, se puede validar que el primer identificador de NF y el segundo identificador de NF sean idénticos.

El aparato del segundo aspecto puede configurarse para recibir, de la NRF, al menos una parte de la información actualizada del certificado de CA para una NF que está asociada con la NF que se recibe a través de una suscripción de notificaciones y para la cual se ha recibido y almacenado anteriormente información de descubrimiento. En este caso, el aparato puede configurarse además para actualizar la información de descubrimiento almacenada en función de la información actualizada del certificado de CA recibida. Se puede realizar el mismo procedimiento para la información actualizada del identificador de NF.

El aparato del segundo aspecto puede configurarse para determinar la información actualizada del certificado de CA para la NF y enviar, a la NRF, un mensaje de actualización que incluye la información actualizada del certificado de CA para la NF. Se puede realizar el mismo procedimiento para la información actualizada del identificador de NF.

En algunas implementaciones, el aparato del segundo se configura como una NF consumidora de servicios. En otras implementaciones, se configura como una NF productora de servicios.

También se proporciona un sistema de red central que comprende el aparato del primer aspecto (es decir, la NRF) y el aparato del segundo aspecto (es decir, la NF).

Además, se presenta un método para proporcionar una función de repositorio de red, NRF, en un dominio de red central de una red de comunicaciones móviles, estando configurada la NRF para registrar perfiles de función de red, NF, para el descubrimiento de NF, en donde se han emitido certificados de NF a las NF, cada certificado de NF incluye una clave pública de la NF respectiva y al menos una firma de al menos una autoridad de certificación, CA. El método comprende recibir, de una NF que se registra que tiene un certificado de NF, información de perfil que comprende una identidad de NF de la NF que se registra, un tipo de NF de la NF que se registra y al menos un certificado de CA de al menos una CA que firmó el certificado de NF emitido a la NF que se registra. El método también comprende almacenar la información de perfil recibida en un repositorio.

El método anterior puede ser realizado por el aparato del primer aspecto (es decir, la NRF).

Además, se presenta un método para proporcionar una función de red, NF, en un dominio de red central de una red de comunicaciones móviles, en donde se ha emitido un certificado de NF a la NF, el certificado de NF incluye una clave pública de la NF y al menos una firma de al menos una autoridad de certificación, CA. El método comprende obtener el al menos un certificado de CA de la al menos una CA que firmó el certificado de NF emitido a la NF, y enviar información de perfil a una función de repositorio de red, NRF, configurada para registrar perfiles de función de red, NF, para el descubrimiento de NF en el dominio de red central, la información de perfil comprende una identidad de NF de la NF que se registra, un tipo de NF de la NF que se registra, y al menos un certificado de CA.

El método anterior puede ser realizado por el aparato del segundo aspecto (es decir, la NF).

También se proporciona un producto de programa informático que comprende partes de código de programa configuradas para ejecutar el método presentado en la presente memoria cuando el producto de programa informático es ejecutado por uno o más procesadores. El producto del programa informático puede almacenarse en un medio de grabación legible por ordenador o puede proporcionarse para su descarga a través de una conexión de red.

Breve descripción de los dibujos

Aspectos, detalles y ventajas adicionales de la presente descripción se harán evidentes a partir de la descripción detallada de las realizaciones ejemplares a continuación y a partir de los dibujos, en donde:

la Fig. 1 es un diagrama que ilustra una realización del sistema de red de la presente descripción;

las Figs. 2A, 2B son diagramas de bloques que ilustran dos realizaciones de aparatos de NRF de la presente descripción;

las Figs. 3A, 3B son diagramas de bloques que ilustran realizaciones de dos aparatos de NF según la presente descripción;

la Fig. 4 ilustra diagramas de flujo de realizaciones del método de la presente descripción; y

las Figs. 5A-D son diagramas de señalización de diagramas esquemáticos que ilustran realizaciones adicionales de la presente descripción.

Descripción detallada

En la siguiente descripción, con fines de explicación y no de limitación, se establecen detalles específicos para proporcionar una comprensión completa de la presente descripción. Será evidente para un experto en la técnica que la presente descripción puede practicarse en otras realizaciones que se aparten de estos detalles específicos.

Si bien, por ejemplo, la siguiente descripción se centra en una configuración de red central ejemplar según las especificaciones 5G, la presente descripción no se limita a este respecto. La presente descripción también podría implementarse en otras redes de comunicaciones inalámbricas celulares o no celulares que tengan un dominio de red central.

Si bien, por lo tanto, las realizaciones se describirán específicamente con referencia a las entidades de red central 5G, se apreciará que la presente descripción también podría implementarse en otros tipos de red y por otras entidades de red que tengan funcionalidades similares. Además, si bien, la información relacionada con el certificado se explicará en el contexto de tipos ejemplares de protocolos de seguridad y procedimientos de establecimiento de enlace tales como TLS, será evidente que la presente descripción no está restringida en este sentido.

Los expertos en la técnica apreciarán además que las etapas, servicios y funciones que se explican en la presente memoria pueden implementarse usando circuitos de hardware individuales, usando software que funcione junto con un microprocesador programado o un ordenador de uso general, usando uno o más circuitos integrados de aplicación específica (ASIC) y/o usando uno o más procesadores de señales digitales (DSP). También se apreciará que cuando la presente descripción se describe en términos de un método, también puede incorporarse en uno o más procesadores y una o más memorias acopladas al uno o más procesadores, en donde la una o más memorias almacenan uno o más programas informáticos que realizan las etapas, servicios y funciones descritos en la presente memoria cuando son ejecutados por uno o más procesadores.

En la siguiente descripción de realizaciones ejemplares, los mismos números de referencia indican componentes iguales o similares.

La Fig. 1 ilustra una realización de un sistema 100 de red en el que se puede implementar la presente descripción. Como se muestra en la Fig. 1, el sistema 100 de red comprende un dominio 102 de red central operado por un operador de red móvil. Diferentes dispositivos 104 terminales, tal como un dispositivo 104A terminal de tipo UE (por ejemplo, un teléfono inteligente) y dos dispositivos 104B, 104C terminales de tipo IoT (por ejemplo, un automóvil y un dispositivo portátil), son atendidos por el dominio 102 de red central a través de un dominio de red de acceso. El dominio de red de acceso no se muestra en la Fig. 1.

A continuación, se supondrá que el dominio 102 de red central cumple con las especificaciones 5G. Por esta razón, la siguiente descripción del dominio 102 de red central hará referencia a los elementos típicos de red central 5G, sin limitar la presente descripción a los mismos. El dominio de red de acceso también puede cumplir con las especificaciones 5G y, opcionalmente, proporcionar compatibilidad adicional para dispositivos terminales 4G y 3G.

El dominio 102 de red central comprende múltiples entidades de red. En la Fig. 1, se ilustran principalmente las entidades de red que participan en los procedimientos relacionados con NRF. Esas entidades de red comprenden diferentes NF 107 y una NRF 106 central configurada para atender a las NF 107 con respecto al descubrimiento de servicios de NF y al descubrimiento de las NF 107 que los proporcionan.

En el contexto de las siguientes realizaciones, una NF 107 es una función de procesamiento que tiene un comportamiento funcional definido e interfaces definidas. Una NF 107 puede implementarse como un elemento de red en un hardware dedicado, como una instancia de software que se ejecuta en un hardware dedicado o como una función virtualizada instanciada en una plataforma adecuada, por ejemplo, en una infraestructura en la nube. A continuación, el término "NF" generalmente indica una instancia de NF identificable que tiene una identidad de NF dedicada (y que es de un tipo de NF dedicado).

Las NF 107 ilustrados en la Fig. 1 pueden tomar diversas formas, tales como funciones de plano de usuario (UPF) 107A, 107B, 107C. Cada NF 107A, 107B, 107C de tipo UPF está asociada con uno de los dispositivos 104A, 104B, 104C terminales, respectivamente, y maneja el tráfico de datos asociado. Se apreciará que cada UPF 107A, 107B, 107C puede, en principio, manejar tráfico de datos para múltiples de los dispositivos 104A, 104B, 104C terminales dependiendo de la configuración de la red.

Las NF 107A, 107B, 107C y otras NF 107D, 107E, podrán registrar, actualizar o dar de baja su respectivo perfil de NR en la NRF 106 y suscribirse y darse de baja en la NRF 106 para ser notificados sobre cambios de estado de las NF 107 registradas en la NRF 106. Para estos (y otros) procedimientos, la NRF 106 proporciona el llamado servicio *Nnrf_GestiónNF* (*Nnrf_NFManagement*) en una implementación 5G ejemplar (consulte la Sección 5.2 del documento TS 29.510 V.15.2.0 (2018-12) de 3GPP). Además, las NF 107 también pueden consultar la NRF 106 para descubrir servicios proporcionados por otras NF 107 y cómo consumirlos. Para estos procedimientos, la NRF 106 proporciona

el llamado servicio Nnrf_DescubrimientoNF (Nnrf_NFDiscovery) en una implementación 5G ejemplar (consulte la Sección 5.3 del documento TS 29.510).

Cada una de las NF 107 está asociada con un perfil de NF. El perfil de NF de una NF particular define una pluralidad de atributos de NF, tal como una identidad única de la NF 107 particular así como su tipo (que será indicativo, por ejemplo, por el tipo de servicio proporcionado por esa NF). La NRF 106 comprende un repositorio 106A de datos para almacenar información relacionada con el perfil recibida de las NF 107. Cada NF 107 también comprende un almacenamiento de datos local.

Según la Sección 13.1 del documento TS 33.501, las NF 107 admitirán TLS con certificados de NF tanto del lado del servidor como del lado del cliente. Como se entiende en la presente memoria, las NF 107 productoras de servicios están ubicadas en el lado del servidor, mientras que las NF 107 consumidoras de servicios están ubicadas en el lado del cliente. Cada certificado de NF incluye una clave pública de la respectiva NF y al menos una firma de al menos una CA.

Las Figs. 2A y 2B ilustran dos realizaciones de la NRF 106 de la Fig. 1. En la realización ilustrada en la Fig. 2A, la NRF 106 comprende un procesador 202 y una memoria 204 acoplados al procesador 202. La NRF 106 comprende además una interfaz 206 de entrada opcional y una interfaz 208 de salida opcional. La memoria 204 almacena código de programa que controla el funcionamiento del procesador 202. La memoria 204, o un almacenamiento diferente, también almacena el repositorio 106B de datos.

El procesador 202 está adaptado para recibir, por ejemplo a través de la interfaz 206 de entrada y de una NF que se registra que tiene un certificado de NF, información de perfil que comprende una identidad de NF de la NF que se registra, un tipo de NF de la NF que se registra y al menos un certificado de CA de al menos una CA que firmó el certificado de NF emitido a la NF que se registra. El procesador 202 está además configurado para almacenar información de perfil recibida en el repositorio 106A de datos como se ilustra en la Fig. 1.

La Fig. 2B muestra una realización en la que la NRF 106 se implementa en una configuración modular. Como se muestra en la Fig. 2B, la NRF 106 comprende un módulo 210 de recepción configurado para recibir, de una NF que se registra, información de perfil que comprende una identidad de NF de la NF que se registra, un tipo de NF de la NF que se registra y al menos un certificado de CA de al menos una CA que firmó el certificado de NF emitido a la NF que se registra. La NRF 106 comprende además un módulo 212 de almacenamiento configurado para almacenar la información de perfil recibida en el repositorio de datos.

Las figs. 3A y 3B ilustran dos realizaciones de una NF 107 de la Fig. 1 que está configurada para registrar su perfil de NF en la NRF 106. En la realización ilustrada en la Fig. 3A, la NF 107 comprende un procesador 302 y una memoria 304 acoplados al procesador 302. La NF 107 comprende además una interfaz 306 de entrada opcional y una interfaz 308 de salida opcional. La memoria 304 almacena el código de programa que controla el funcionamiento del procesador 302. La memoria 304, o un almacenamiento diferente, también puede almacenar la información relacionada con el certificado de CA para la propia NF 107 u obtenida de otras NF 107.

El procesador 302 de la NF 107 está adaptado para obtener, por ejemplo a través de la interfaz 306 de entrada, al menos un certificado de CA de al menos una CA que firmó un certificado de NF emitido a la NF 107. El procesador 302 está además adaptado para enviar, por ejemplo, a través de la interfaz 308 de salida, información de perfil a la NRF 106 que está configurada para registrar perfiles de NF para el descubrimiento de NF en el dominio 102 de red central. La información de perfil que se envía comprende una identidad de NF de la NF 107 que se registra, un tipo de NF de la NF 107 que se registra, y al menos un certificado de CA.

La Fig. 3B muestra una realización en la que la NF 107 se implementa en una configuración modular. Como se muestra en la Fig. 3B, la NF 107 comprende un módulo 310 de obtención configurado para obtener el al menos un certificado de CA de la al menos una CA que firmó el certificado de NF emitido a la NF 107. La NF 107 comprende además un módulo 312 de envío configurado para enviar información de perfil a la NRF 106 que está configurada para registrar perfiles de NF para el descubrimiento de NF en el dominio 102 de red central. La información de perfil comprende la identidad de NF de la NF 107 que se registra, el tipo de NF de la NF 107 que se registra y el al menos un certificado de CA.

La figura 4 ilustra en las realizaciones del método de la presente descripción dos diagramas 400, 410 de flujo. La realización del método del diagrama 400 de flujo puede realizarse mediante cualquiera de las realizaciones de la NF de las Figs. 3A y 3B. La realización del método del diagrama 410 de flujo puede realizarse mediante cualquiera de las realizaciones de NRF de las Figs. 2A y 2B.

El método ilustrado en el diagrama 400 de flujo comprende una etapa 402 de obtener, mediante la NF 107 que se registra, el al menos un certificado de CA de la al menos una CA que firmó el certificado de NF emitido a la NF 107 que se registra. El al menos un certificado de CA ha sido obtenido por la NF 107 que se registra como parte de la configuración de NF. Aunque esta configuración es específica del proveedor, generalmente se usan interfaces de gestión de configuración (CM) de propósito general tal como NETCONF para este propósito.

En la etapa 404, la NF 107 que se registra envía información de perfil a la NRF 106 para que su perfil de NF pueda registrarse allí para el descubrimiento de NF en el dominio 102 de red central. La información de perfil comprende (al menos) la identidad de NF de la NF 107 que se registra, el tipo de NF de la NF 107 que se registra, y el al menos un certificado de CA obtenido en la etapa 402.

- 5 Volviendo ahora al diagrama 410 de flujo, la NRF 106 recibe en la etapa 406, de la NF 107 que se registra, la información de perfil enviada en la etapa 404. Como se explicó anteriormente, la información de perfil comprende (al menos) la identidad de NF de la NF 107 que se registra, el tipo de NF de la NF 107 que se registra, y el al menos un certificado de CA de la al menos una CA que firmó el certificado de NF emitido a la NF 107 que se registra. Luego, en la etapa 408, la NRF 106 almacena la información de perfil recibida en su repositorio 106A de datos.
- 10 A continuación, las realizaciones generales anteriores se describirán con mayor detalle con referencia a las realizaciones de señalización ilustradas en las Figs. 5A a 5D. Estos diagramas de señalización se basan en una implementación de señalización 5G ejemplar como se define, entre otros, en el documento TS 29.510. El contenido de los perfiles de NF heredados ejemplares se define en las secciones 6.1.6.2.2 y 6.1.6.2.3 del documento TS 29.510, y se extenderá en las siguientes realizaciones por uno o ambos de los siguientes dos atributos:

Nombre del Atributo	Tipo de datos	PAG	Cardinalidad	Descripción
caCertificados (caCertificates)	matriz(cadena de caracteres)	O	0.. N	Certificados para las CA usados por los certificados de NF
identificador (identifier)	cadena de caracteres	O	0..1	Identificador usado por la NF

- 15 El atributo *caCertificados* es un atributo opcional que contiene una lista de hasta N certificados de CA que se usarán para verificar el certificado usado por una NF 107. El formato de este atributo es una matriz de cadenas de caracteres. Cada cadena de caracteres puede incluir el contenido de un certificado de CA.

- 20 En una variante, cada cadena de caracteres representa un certificado DER (Reglas de codificación distintivas) codificado en Base64 PEM (Correo electrónico mejorado por privacidad), delimitado entre "-----INICIO CERTIFICADO-----" y "-----FIN CERTIFICADO-----". Son posibles otros formatos de codificación para el atributo *caCertificados*, siempre que sean compatibles con la codificación JSON (Notación de objetos de JavaScript) que generalmente se usa para los perfiles de NF.

- 25 El atributo *identificador* es un atributo opcional que contiene el identificador usado para identificar una instancia de NF en su certificado de CA. El formato es una cadena de caracteres. Cabe señalar que este atributo *identificador* es un atributo diferente y proporcionado además del atributo *nfIDInstancia* (*nfInstanceID*) o del atributo *IDInstanciaservicio* (*serviceInstanceID*) en perfiles de NF heredados.

En una variante, el atributo *identificador* es un FQDN. Los FQDN se pueden construir según la Sección 28.2 del documento TS 23.003 V15.6.0 (2018-12) de 3GPP. Un ejemplo de FQDN es:

- 30 `<id-instancia-nf>.<tipo-instancia-nf>.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

donde:

- `<id-instancia-nf>` es un identificador único para la instancia de NF. No existirán dos identificadores iguales para un tipo de NF en una red móvil terrestre pública (PLMN)
- `<nf-tipo-de-instancia>` es el tipo de NF, por ejemplo, Gestión de datos unificados (UDM)
- `<MNC>` y `<MCC>` corresponden al código de red móvil (MNC) y al código de país móvil (MCC) de la PLMN del operador.

En otra variante, el atributo *identificador* es un identificador de SPIFFE. A continuación se muestra un ejemplo de identificador SPIFFE:

`spiffe://5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org/<tipo-de-instancia-nf>/<id-instancia-nf>`

- 40 donde:

- `<id-instancia-nf>` es un identificador único para la instancia de NF. No existirán dos identificadores iguales para un tipo de NF en una PLMN.
- `<tipo-de-instancia-nf>` es el tipo de NF, por ejemplo, UDM.

- *<MNC>* y *<MCC>* corresponden al MNC y MCC de la PLMN del operador.

En otra variante adicional, el atributo *identificador* es un valor opaco. Un ejemplo de atributo *identificador* opaco se muestra a continuación:

36f01027-4d6f-45e6-8e60-1e14d464344e

- 5 La Fig. 5A representa una realización de señalización en el contexto del registro de cualquiera de las NF 107 ilustradas en la Fig. 1 en la NFR 106. La NF 107 representada en la Fig. 5A puede ser un productor de servicios o un consumidor de servicios, o puede tener ambos roles dependiendo de los requisitos vigentes.

- 10 Como condición previa, se asume que la NF 107 ha sido aprovisionada, por ejemplo durante la configuración, con el certificado de CA raíz y, opcionalmente, uno o más certificados de CA intermedios que se han usado para firmar el certificado de la NF 107. Este aprovisionamiento puede haber ocurrido en el contexto de la etapa S402 ilustrada en la Fig. 4.

La realización de señalización de la Fig. 5A comprende las siguientes etapas:

- 15 En una etapa 1100 inicial, la NF 107 crea su perfil de NF. El perfil de NF incluye, entre otros, su tipo de NF (por ejemplo, UDR), su identidad de NF única (por ejemplo, *IDInstancianf* o *IDInstanciaservicio*) y al menos uno de los siguientes atributos:

- atributo *caCertificados*: contiene los certificados de CA raíz y/o intermedios que se requieren para validar el certificado de NF 107 (por ejemplo, codificado como se explicó anteriormente).
 - atributo *identificador*: contiene un identificador de NF (por ejemplo, como se explicó anteriormente). En algunas variantes, el identificador de NF coincide con el valor de los campos Nombre del Sujeto (Subject Name) o Nombres Alternativos del Sujeto (Subject Alternative Names) del certificado de la NF 107.
- 20

En algunas implementaciones, el atributo *identificador* puede omitirse. En otras implementaciones, el atributo *caCertificados* puede omitirse. En caso de que se omita uno de estos atributos, no se pueden realizar ciertos procesos de seguridad (tales como se analiza a continuación con referencia a la Fig. 5C). Como tal, para máxima seguridad, ambos atributos pueden usarse por defecto.

- 25 En la etapa 1101, la NF 107 se registra en la NFR 106 enviando una solicitud *Nnrf_GestiónNF_RegistrarNF* (*Nnrf_NFManagement_NFRegister*) (consulte la etapa S404 en la Fig. 4). La solicitud incluye el perfil de NF creado anteriormente en la etapa 1100.

La NFR 106 recibe el perfil de NF (consulte la etapa S406 en la Fig. 4) y almacena el perfil de NF recibido en su repositorio 106A de datos (consulte la etapa S408 en la Fig. 4).

- 30 Luego, en la etapa 1102, la NFR 106 devuelve una respuesta *Nnrf_GestiónNF_RegistrarNF* (*Nnrf_NFManagement_NFRegister*) a la NF 107. Esta respuesta informa a la NF 107 que el perfil de NF ha sido recibido y almacenado correctamente por la NF 107.

- 35 La Fig. 5B representa una realización de señalización en el contexto del descubrimiento de NF por una NF 107 que asume el papel de un consumidor de servicios. A continuación, se supondrá a modo de ejemplo que la NF 107D de la Fig. 1 actúa como consumidor de servicios, mientras que el NF 107E actúa como productor de servicios. Como se explicó anteriormente con referencia a la Fig. 5A, la NFR 106 tendrá almacenados en su repositorio 106A de datos los perfiles de NF (con los tipos de NF asociados y los certificados de CA) de todas las NF 107 que pueden actuar como productores de servicios para otras NF 107.

- 40 En la etapa 1200, la NF 107D consumidora de servicios determina el uno o más tipos de NF (es decir, tipos de servicios) con los que requiere interactuar, y para cada uno de ellos repite las etapas 1201 a 1205.

En la etapa 1201, la NF 107D consumidora de servicios envía una solicitud *Nnrf_DescubrimientoNF* (*Nnrf_NFDiscovery*) a la NRF 107. Esta solicitud indica al menos un tipo de NF particular como criterio de selección. En algunos casos, la solicitud puede incluir uno o más criterios de selección u otra información.

- 45 Luego, en la etapa 1202, la NFR 106 consulta su repositorio 106A de datos para hacer coincidir los perfiles de NF de una o más NF 107E productoras de servicios y devuelve una respuesta *Nnrf_DescubrimientoNF* (*Nnrf_NFDiscovery*). Esta respuesta contiene los perfiles de NF que coincidan con el uno o más criterios indicados en la etapa 1201. Los perfiles de NF devueltos en la etapa 1202 pueden incluir, entre otros, los atributos *caCertificados* e *identificador* respectivos. De esta forma, la NF 107D consumidora de servicios recibe el uno o más certificados de CA almacenados para cada NF 107E productora de servicios en el repositorio 106A de datos de la NRF 106 para su uso futuro.

50

La NF 107D consumidora de servicios procesa los perfiles de NF recibidos en la etapa 1203. Para cada perfil de NF, la NF 107D consumidora de servicios:

- extrae el contenido del atributo *caCertificados*, y para cada certificado de CA, almacena el contenido extraído en un registro seguro de la implementación de TLS; y
- 5 • extrae el contenido del atributo *identificador* y lo almacena internamente (y generalmente por separado de los contenidos extraídos del atributo *caCertificados*).

En una etapa 1204 adicional, la NF 107D consumidora de servicios envía una solicitud (opcional) *Nnrf_GestiónNF_SuscribirEstadoNF* (*Nnrf_NFManagement_NFStatusSubscribe*) a la NRF 106. En esta solicitud de suscripción, la NF 107D consumidora de servicios indica un tipo de NF, para recibir cambios en el estado de las NF 107E productoras de servicios para los que se han obtenido perfiles de NF en la etapa 1202, y aprender unos nuevos que coincidan con el tipo de NF indicado.

En la etapa 1205, la NRF 106 procesa la solicitud de suscripción y devuelve una respuesta *Nnrf_GestiónNF_SuscribirEstadoNF* (*Nnrf_NFManagement_NFStatusSubscribe*). La respuesta de suscripción notifica a la NF 107D consumidora de servicios que la solicitud de suscripción se ha recibido y procesado correctamente.

15 Al final del procedimiento de señalización ilustrado en la Fig. 5B, la NF 107D consumidora de servicios tiene todas las identidades de NF, certificados de CA e identificadores de NF de todas las NF 107E productoras de servicios de las que potencialmente necesitan consumir servicios. El mismo procedimiento de señalización puede ser ejecutado por una NF 107E productora de servicios, esta vez indicando los tipos de NF a los que la NF 107E productora de servicios deberá proporcionar sus servicios. Al final del procedimiento de señalización correspondiente, la NF 107E productora de servicios tiene todas las identidades de NF, certificados de CA y los identificadores de NF de todas las NF 107D consumidoras de servicios que consumirán sus servicios.

Algunas NF 107 pueden tener tanto roles de consumidor de servicios como de productor de servicios simultáneamente, por ejemplo, la UDM actúa como un productor de servicio hacia una función de servidor de autenticación (AUSF) y como un consumidor hacia un repositorio de datos unificado (UDR). En tales casos, el procedimiento de señalización 25 ilustrado en la Fig. 5B puede ser ejecutado dos veces por una NF 107 dada (una vez como un consumidor de servicios y otra vez como un productor de servicios).

La Fig. 5C representa una realización de señalización en el contexto de la invocación del servicio NF por una NF 107D consumidora de servicios en relación con una NF 107E productora de servicios. La NF 107E productora de servicios ha sido descubierta anteriormente por la NF 107D consumidora de servicios usando señalización de descubrimiento/suscripción como se ilustra en la Fig. 5B.

En la etapa 1300, la NF 107D consumidora de servicios inicia una conexión de protocolo de transferencia de hipertexto 2 (HTTP/2) hacia la NF 107E productora de servicios. La conexión está protegida con mTLS, por lo que comienza el procedimiento de establecimiento de enlace TLS (consulte el cuadro entre líneas discontinuas).

35 En la etapa 1301, la NF 107D consumidora de servicios envía un mensaje de saludo de cliente (Client Hello) a la NF 107E productora de servicios, y en la etapa 1302, la NF 107E productora de servicios envía un mensaje de saludo de servidor (Server Hello) a la NF 107E consumidora de servicios, que incluye (entre otros parámetros) el certificado de la NF 107E productora de servicios ("certificado de servidor" en la Fig. 5C).

40 Luego, en la etapa 1303, la NF 107D consumidora de servicios valida el certificado de servidor proporcionado por la NF 107E productora de servicios. En este contexto, la implementación de TLS accede al registro seguro para obtener el uno o más certificados de CA que se almacenaron en la etapa 1203 de la Fig. 5B para la NF 107E productora de servicios. La verificación como tal se realiza según el protocolo X.509, generalmente atravesando la cadena de certificados desde el certificado de CA raíz a través de los certificados de CA intermedios hasta el certificado de NF y validando todas las firmas de certificados, y no se describirá con mayor detalle en la presente memoria. A continuación, se supondrá que la validación se ha realizado con éxito, ya que todas las firmas de la cadena de certificados podrían validarse con éxito.

Después de una validación exitosa, la NF 107D consumidora de servicios en la etapa 1304 envía un mensaje a la NF 107E productora de servicios. Este mensaje incluye, entre otros parámetros, el certificado de la NF 107D consumidora de servicios ("certificado de cliente" en la Fig. 5C).

50 En la etapa 1305, la NF 107E productora de servicios valida (con éxito) el certificado de cliente proporcionado por la NF 107D consumidora de servicios. Con este fin, la implementación de TLS accede al registro seguro para obtener el uno o más certificados de CA que se almacenaron en la etapa 1203 de la Fig. 5B para la NF 107D consumidora de servicios. La NF 107E productora de servicios almacena los detalles del certificado de cliente para su uso posterior.

En la etapa 1306, la NF 107E productora de servicios envía un mensaje de Servidor Finalizado a la NF 107D consumidora de servicios y finaliza la fase de establecimiento de enlace de TLS. A partir de este momento, la conexión HTTP/2 está protegida y la autenticación mTLS se completó con éxito.

En la etapa 1307, la NF 107D productora de servicios envía una solicitud de Servicio de NF a la NF 107E productora de servicios para consumir uno de sus servicios.

En la etapa 1308, la NF 107E productora de servicios autoriza a la NF 107D consumidora de servicios antes de habilitar el consumo de sus servicios. Para ello, la NF 107E productora de servicios:

- 5 • extrae los campos Nombre del Sujeto y Nombres Alternativos del Sujeto del certificado de cliente tal como se recibió y almacenó en las etapas 1304 y 1305, respectivamente; y
- itera sobre los perfiles de NF de los tipos de NF que consumen sus servicios (por ejemplo, como se recibió anteriormente de la NFR 106 durante la señalización de descubrimiento ilustrada en la Fig. 5B) y compara el atributo *identificador* en cada perfil de NF con los campos Nombre del Sujeto o Nombre Alternativo del Sujeto del certificado de cliente.

Si se encuentra una coincidencia, la NF 107D consumidora de servicios ha sido autorizada con éxito y la NF 107E productora de servicios devuelve una respuesta de invocación del servicio en la etapa 1309. Si, por otro lado, no se encuentra ninguna coincidencia, la NF 107D consumidora de servicios no es autorizada, y la NF 107E productora de servicios devuelve una respuesta de error en la etapa 1310. El mensaje de error indica que la solicitud de servicio recibida en la etapa 1307 no fue autorizada.

Se apreciará que las etapas 1301 a 1306 así como las etapas 1307 a 1309 se basan en el nuevo atributo *caCertificados* y el nuevo atributo *identificador*, respectivamente. En caso de que solo se implemente uno de estos atributos, seguirá habiendo beneficios de implementación o seguridad en comparación con las implementaciones heredadas.

La Fig. 5D representa una realización de señalización en el contexto de la actualización de certificados de CA (por ejemplo, debido a su vencimiento), que pertenece a la gestión del ciclo de vida (LCM). Los certificados de CA que necesitan actualizarse se han comunicado previamente en el dominio 102 de red central como se analizó anteriormente con referencia a las Figs. 5A y 5B. El mismo procedimiento de señalización será aplicado por cada NF 107, independientemente de su rol como consumidor de servicios o como productor de servicios. Como condición previa del procedimiento de señalización ilustrado en la Fig. 5D, la NF 107 ha sido aprovisionada con al menos un certificado de CA raíz y/o intermedio actualizado o nuevo.

A continuación se supondrá que debido a una operación LCM, los certificados de CA deben actualizarse para, por ejemplo, una NF 107E productora de servicios. La NF 107E productora de servicios actualiza así su perfil de NF con un nuevo valor para el atributo *caCertificados* en la etapa 1400.

En la etapa 1401, la NF 107E productora de servicios envía una solicitud de ActualizarNF (NFUpdate) a la NRF 106. La solicitud indica el nuevo valor para el atributo *caCertificados*, potencialmente con atributos de perfil de NF adicionales que han cambiado. En algunas implementaciones se envía el perfil de NF completo, en otras implementaciones solo los valores de los atributos que han cambiado.

En la etapa 1402, la NRF 106 almacena el perfil de NF actualizado en el repositorio 106A de datos y devuelve una respuesta ActualizarNF (NFUpdate) a la NF 107E productora de servicios.

En la etapa 1403, la NRF 106 determina todas las NF 107D consumidoras de servicios que tienen una suscripción activa a los cambios en la NF 107E productora de servicios particular que envió el mensaje de solicitud en la etapa 1402, o en general a los cambios en los tipos de NF productoras de servicio al que pertenece la NF 107E productora de servicios particular que envió el mensaje de solicitud en la etapa 1402.

Luego, para cada NF 107D consumidora de servicios determinada en la etapa 1403, la NRF 106 envía una solicitud NotificarEstadoNF (NFStatusNotify) en la etapa 1404. La solicitud incluye el atributo *caCertificados* modificado recibido en la etapa 1401 e indica el atributo *identificador* de la NF 107E productora de servicios asociado a la misma.

En la etapa 1405, una NF 107D consumidora de servicios particular recibe la solicitud y devuelve una respuesta NotificarEstadoNF (NFStatusNotify) a la NRF 106. La respuesta realiza el acuse de recibo adecuado de la solicitud.

Además, en la etapa 1406, la NF 107D consumidora de servicios extrae los contenidos del atributo *caCertificados* del mensaje recibido en la etapa 1405 y los almacena en el registro seguro de la implementación de TLS.

Al final del procedimiento de señalización ilustrado en la Fig. 5D, cada NF 107D consumidora de servicios afectada ha actualizado su(s) certificado(s) de CA almacenados para la NF 107E productora de servicios que inició el procedimiento. En la otra dirección, también las NF 107D consumidoras de servicios actualizan sus respectivos atributos *caCertificados* y las NF 107E productoras de servicios reciben las notificaciones de actualización correspondientes de la NRF 106 y actualizan en consecuencia, su registro seguro respectivo de la implementación de TLS. El mismo procedimiento de señalización se aplica a los cambios en el atributo *identificador* de los perfiles de NF de las NF 107D consumidoras de servicios.

Como se ha hecho evidente a partir de las Figs. 5A a 5D, la extensión del perfil de NF con uno o ambos de los atributos *caCertificados* e *identificador* da como resultado diversas modificaciones de los procedimientos de señalización heredados. Estas modificaciones incluyen la creación de un perfil de NF para una NF 107 con los atributos *caCertificados* y/o *identificador* (etapa 1100 en la Fig. 5A y etapa 1400 en la Fig. 5D), el almacenamiento de los certificados de CA contenidos en el atributo *caCertificados* en el registro seguro de la implementación de TLS, y el almacenamiento del atributo *identificador* internamente (etapa 1203 en la Fig. 5B y etapa 1406 en la Fig. 5D), la búsqueda y coincidencia del atributo *identificador* en el perfil de NF con los campos Nombre del Sujeto y/o Nombres Alternativos del Sujeto del certificado de cliente (etapa 1308 en la Fig. 5C), y otros.

Como se apreciará, el envío de certificados e identificadores de NF en el contexto de las realizaciones anteriores puede exponer desafíos de seguridad si no se hace con cuidado. Sin embargo, las conexiones entre las NF 107 y la NFR 106 están protegidas usando mTLS, por lo tanto, los certificados de CA y los identificadores de NF intercambiados durante el registro, el descubrimiento y la señalización de notificación están protegidos contra posibles escuchas o manipulaciones por parte de posibles atacantes. Además, la NFR 106 se considera confiable, por lo que se implementará de manera que los perfiles de NF que contiene no puedan ser revelados o manipulados por posibles atacantes.

La técnica que se presenta en la presente memoria facilita la distribución de material criptográfico (certificados de CA) necesarios para validar certificados usados, por ejemplo, en conexiones protegidas con mTLS. También proporciona un método de autorización simple en función de políticas locales (cuando no se usa autorización basada en token) y, generalmente, no requiere configuración en las diferentes NF. Como resultado, se facilita el funcionamiento de un sistema 5G o similar, lo que permite un fácil escalado y reduce la probabilidad de errores por intervención manual y errores de configuración.

Se apreciará que la presente descripción se ha descrito con referencia a realizaciones ejemplares que pueden variar en muchos aspectos. Como tal, la presente invención solo está limitada por las reivindicaciones que siguen.

REIVINDICACIONES

1. Un aparato (106) configurado para proporcionar una función de repositorio de red, NRF, en un dominio (102) de red central de una red de comunicaciones móvil, estando configurado la NRF para registrar perfiles de función de red, NF, para el descubrimiento de NF, en donde los certificados de NF han sido emitidos a las NF (107), cada certificado de NF incluye una clave pública de la respectiva NF y una firma de una autoridad de certificación, CA, estando configurado el aparato (106) para:
5 recibir (210), de una NF (107) que se registra que tiene un certificado de NF, información de perfil que comprende
 - una identidad de NF de la NF (107) que se registra,
 - un tipo de NF de la NF (107) que se registra, y10 - un certificado de CA de una CA que firmó el certificado de NF emitido a la NF (107) que se registra; y almacenar (212) la información de perfil recibida en un repositorio (106A).
2. El aparato de la reivindicación 1, en donde el certificado de NF emitido a la NF (107) que se registra incluye además un identificador de NF que es diferente de la identidad de NF de la NF (107) que se registra, y en donde la información de perfil recibida comprende además el identificador de NF.
15
3. El aparato de la reivindicación 2, en donde el identificador de NF toma la forma de un nombre de dominio cualificado completo, FQDN, y un identificador de marco de identidad de producción seguro para todos, SPIFFE.
4. El aparato de cualquiera de las reivindicaciones anteriores, configurado para
20 recibir una solicitud de descubrimiento que indique al menos un tipo de NF;
acceder al repositorio (106A) para identificar uno o más perfiles de NF que coincidan al menos con el tipo de NF indicado; y
enviar una respuesta de descubrimiento que incluye información de descubrimiento del uno o más perfiles de NF coincidentes, incluyendo la información de descubrimiento al menos el certificado de CA almacenado para el perfil de NF respectivo.
25
5. El aparato de cualquiera de las reivindicaciones anteriores, configurado para recibir, de una primera NF (107E), una solicitud de actualización que incluye información actualizada del certificado de CA; y
30 actualizar la información de perfil de la primera NF (107E) en función de la información actualizada del certificado de CA.
6. Un aparato (107) configurado para proporcionar una función de red, NF, en un dominio (102) de red central de una red de comunicaciones móviles, en donde se ha emitido un certificado de NF a la NF (107), el certificado de NF que incluye una clave pública de la NF (107) y una firma de una autoridad de certificación, CA, estando configurado el aparato para:
35 obtener (310) el certificado de CA de la CA que firmó el certificado de NF emitido a la NF (107);
enviar (312) información de perfil a una función de repositorio de red, NRF, (106) configurada para registrar perfiles de NF para el descubrimiento de NF en el dominio de red central, comprendiendo la información de perfil
 - una identidad de NF de la NF (107) que se registra,
 - un tipo de NF de la NF (107) que se registra, y40 - el certificado de CA.
7. El aparato de la reivindicación 6, en donde el certificado de NF emitido a la NF (107) que se registra incluye además un identificador de NF que es diferente de la identidad de NF de la NF (107) que se registra, y en donde la información de perfil recibida comprende además el identificador de NF.
45

8. El aparato de la reivindicación 6 o 7, configurado para
enviar, a otra NF (107D/E), el certificado de NF en un procedimiento de establecimiento de enlace con la otra NF (107D/E).
9. El aparato de cualquiera de las reivindicaciones 6 a 8, configurado para
- 5 enviar, a la NRF (106), una solicitud de descubrimiento que indica al menos un tipo de NF;
recibir, de la NRF (106), una respuesta de descubrimiento que incluye información de descubrimiento de uno o más perfiles de NF que coincidan al menos con el tipo de NF, incluyendo la información de descubrimiento el certificado de CA almacenado para el perfil de NF respectivo; y
almacenar la información de descubrimiento en un almacenamiento.
- 10 10. El aparato de la reivindicación 9, configurado para
recibir, de la NRF (106), al menos una parte de la información actualizada del certificado de CA para una NF (107) que está asociada con la NF que se recibe a través de una suscripción de notificación y para la cual la información de descubrimiento ha sido recibida y almacenada anteriormente; y
actualizar la información de descubrimiento almacenada en función de la información actualizada del certificado de CA recibida.
- 15 11. El aparato de cualquiera de las reivindicaciones 7 a 10, configurado para
determinar la información actualizada del certificado de CA para la NF (107); y
enviar, a la NRF (106), un mensaje de actualización que incluye la información actualizada del certificado de CA para la NF (107).
- 20 12. El aparato de cualquiera de las reivindicaciones 7 a 11, configurado
como una NF (107D) que consume servicios, o como una NF (107E) que produce servicios.
13. Un método realizado por una función de repositorio de red, NRF, (106) en un dominio (106) de red central de una red de comunicaciones móvil, el método que se lleva a cabo para registrar perfiles de función de red, NF, para el descubrimiento de NF, en donde los certificados de NF han sido emitido a las NF (107), cada certificado de NF incluye una clave pública de la respectiva NF (107) y una firma de una autoridad de certificación, CA, el método que comprende:
- 25 recibir (406), de una NF (107) que se registra que tiene un certificado de NF, información de perfil que comprende
 - una identidad de NF de la NF (107) que se registra,
 - un tipo de NF de la NF (107) que se registra, y
- 30 - un certificado de CA de una CA que firmó el certificado de NF emitido a la NF (107) que se registra; y
almacenar (408) la información de perfil recibida en un repositorio (106A).
14. El método de la reivindicación 13, realizado por el aparato de cualquiera de las reivindicaciones 1 a 5.
15. Un método realizado por una función de red, NF, (107) en un dominio (102) de red central de una red de comunicaciones móviles, el método que se lleva a cabo para registrar perfiles de NF para el descubrimiento de NF, en donde se ha emitido un certificado de NF a la NF (107), el certificado de la NF que incluye una clave pública de la NF (107) y una firma de una autoridad de certificación, CA, el método que comprende:
- 35 obtener (402) el certificado de CA de la CA que firmó el certificado de NF emitido a la NF (107); y
enviar (404) información de perfil a una función de repositorio de red, NRF, (106) configurada para registrar perfiles de NF para el descubrimiento de NF en el dominio (102) de red central, comprendiendo la información de perfil
- 40 - una identidad de NF de la NF (107) que se registra,
- un tipo de NF de la NF (107) que se registra, y
- el certificado de CA.
16. El método de la reivindicación 15, realizado por el aparato de cualquiera de las reivindicaciones 6 a 12.

17. Un producto de programa informático que comprende partes de código de programa para realizar el método de cualquiera de las reivindicaciones 13 a 16 cuando las partes de código de programa son realizadas por uno o más procesadores (202, 302).

100

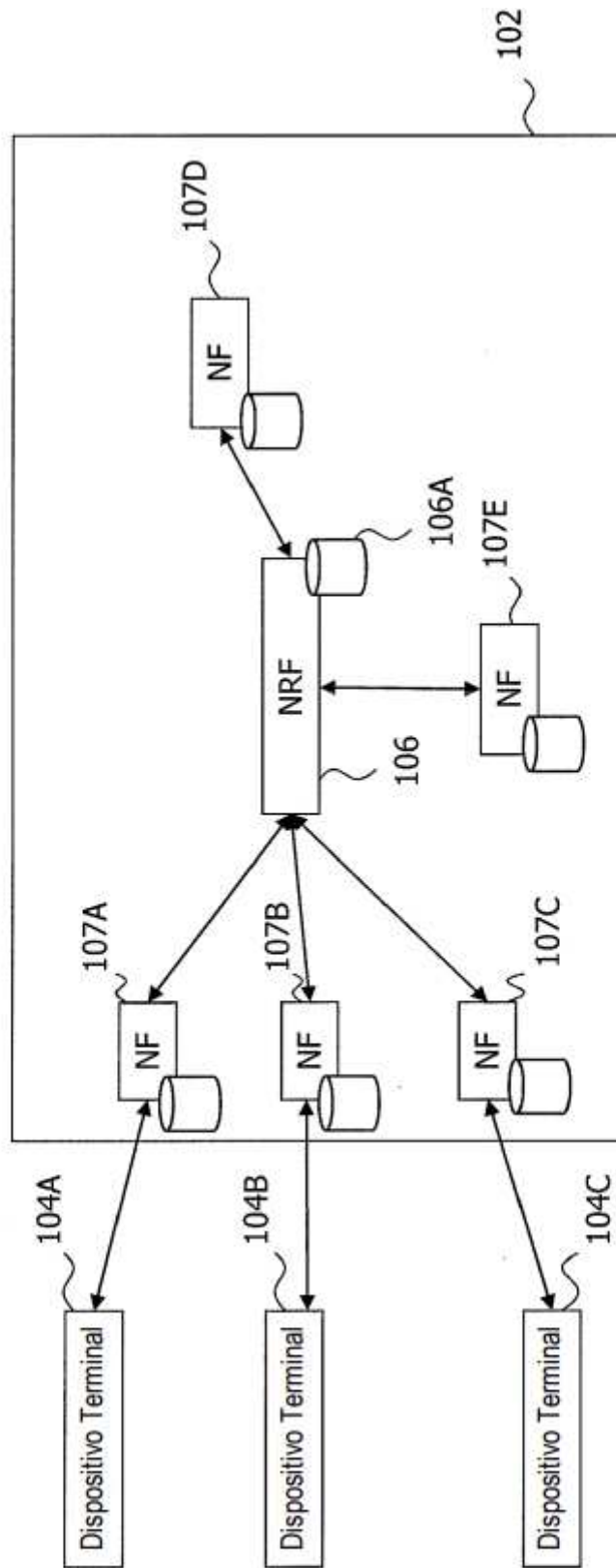


Fig. 1

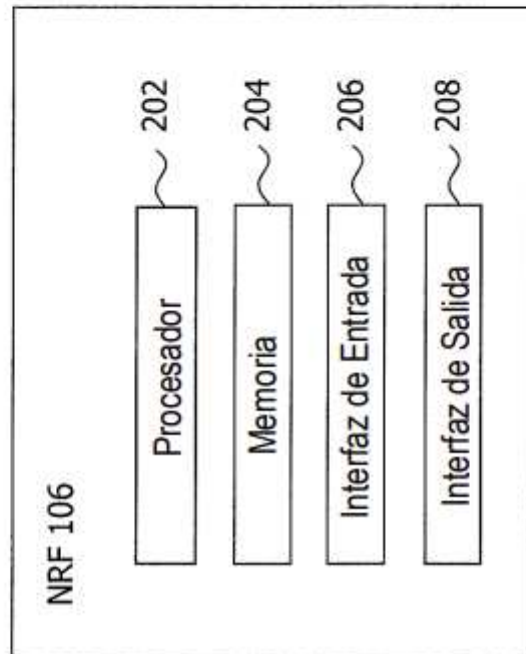


Fig. 2A

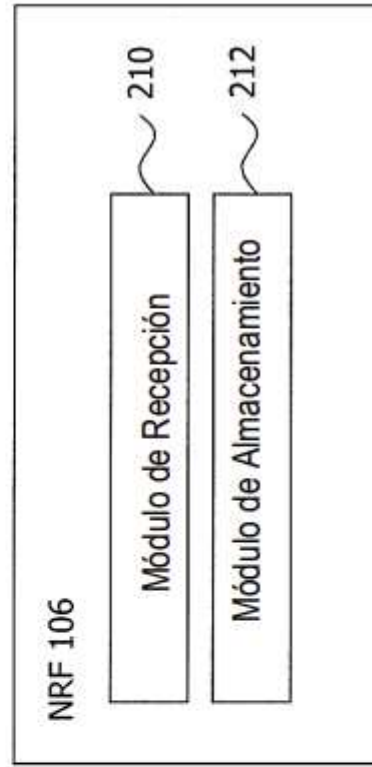


Fig. 2B

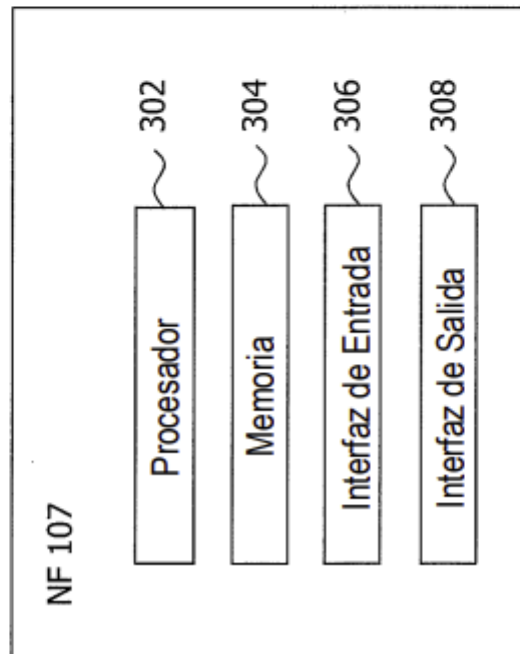


Fig. 3A

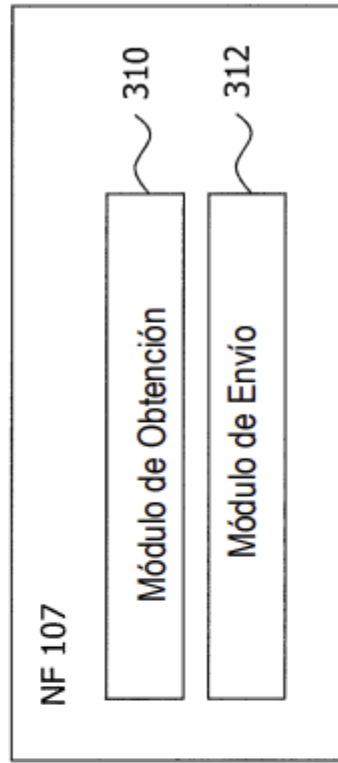


Fig. 3B

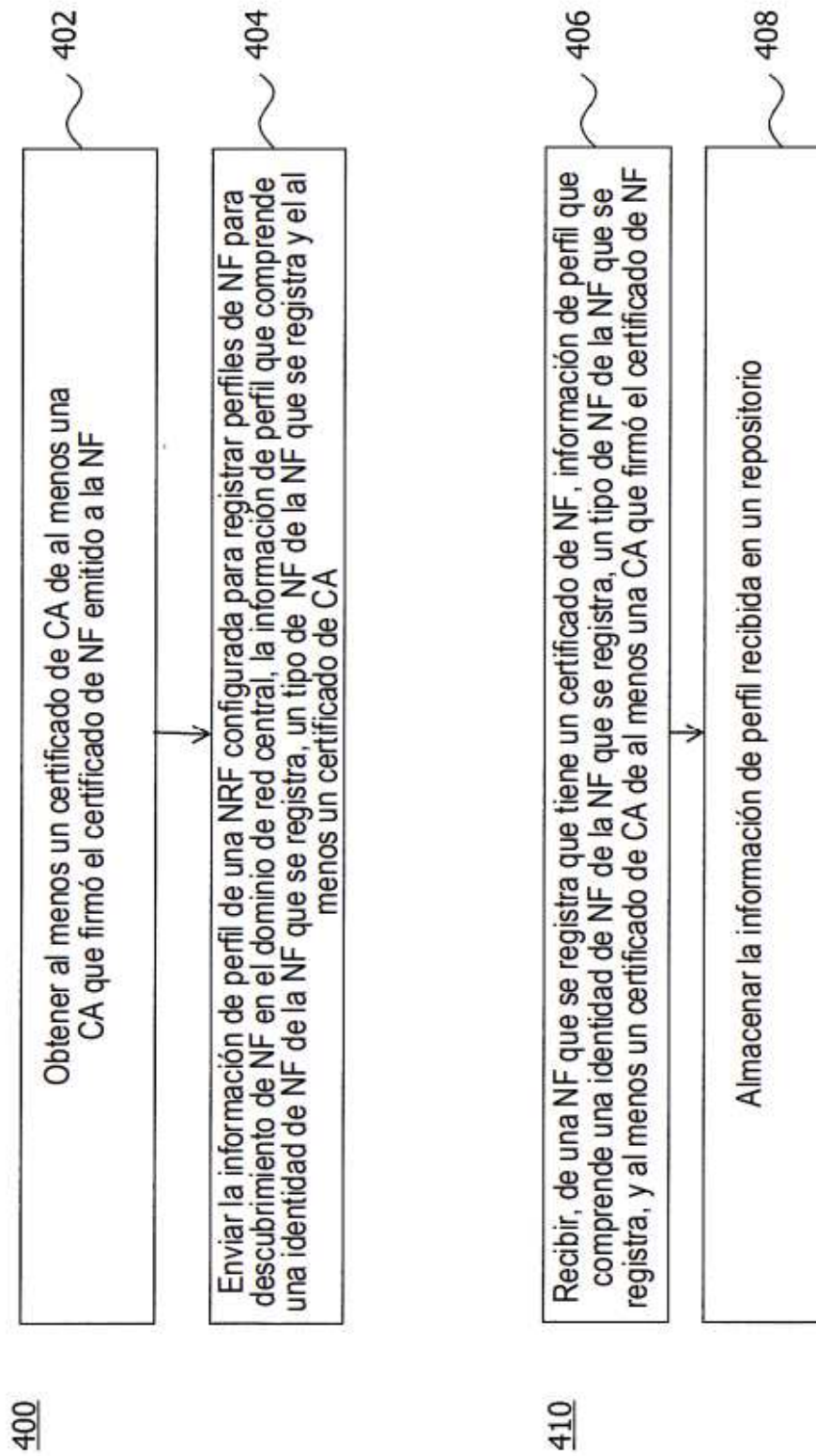


Fig. 4

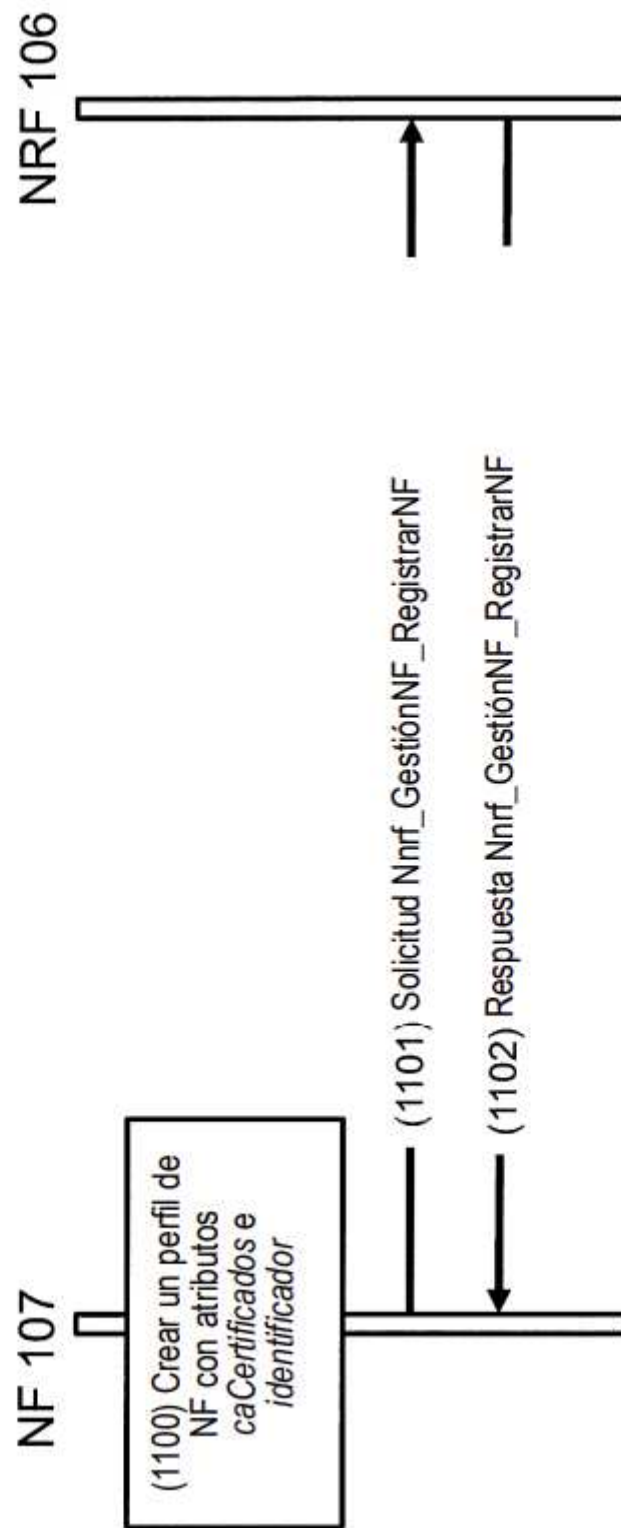


Fig. 5A

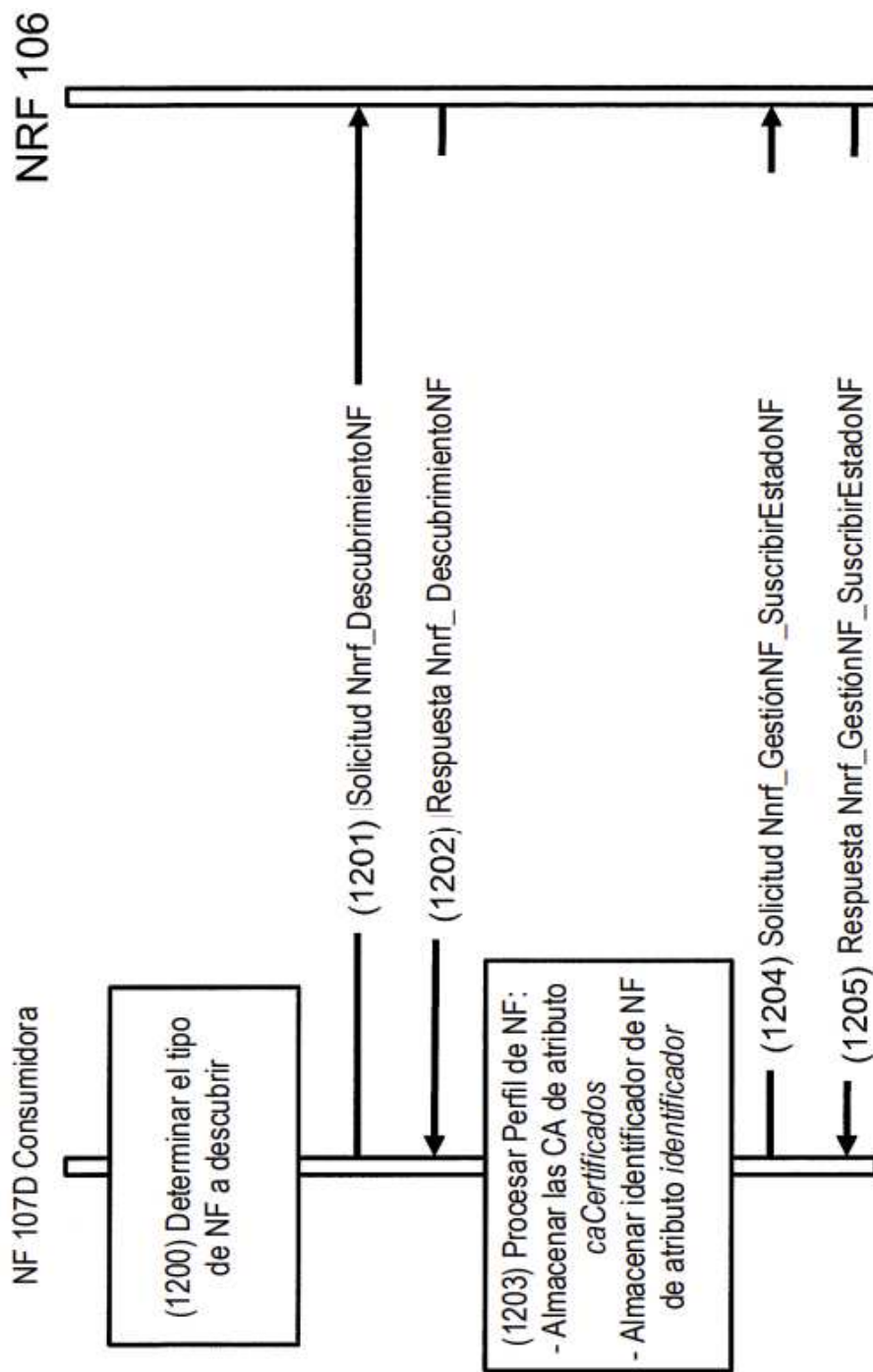


Fig. 5B

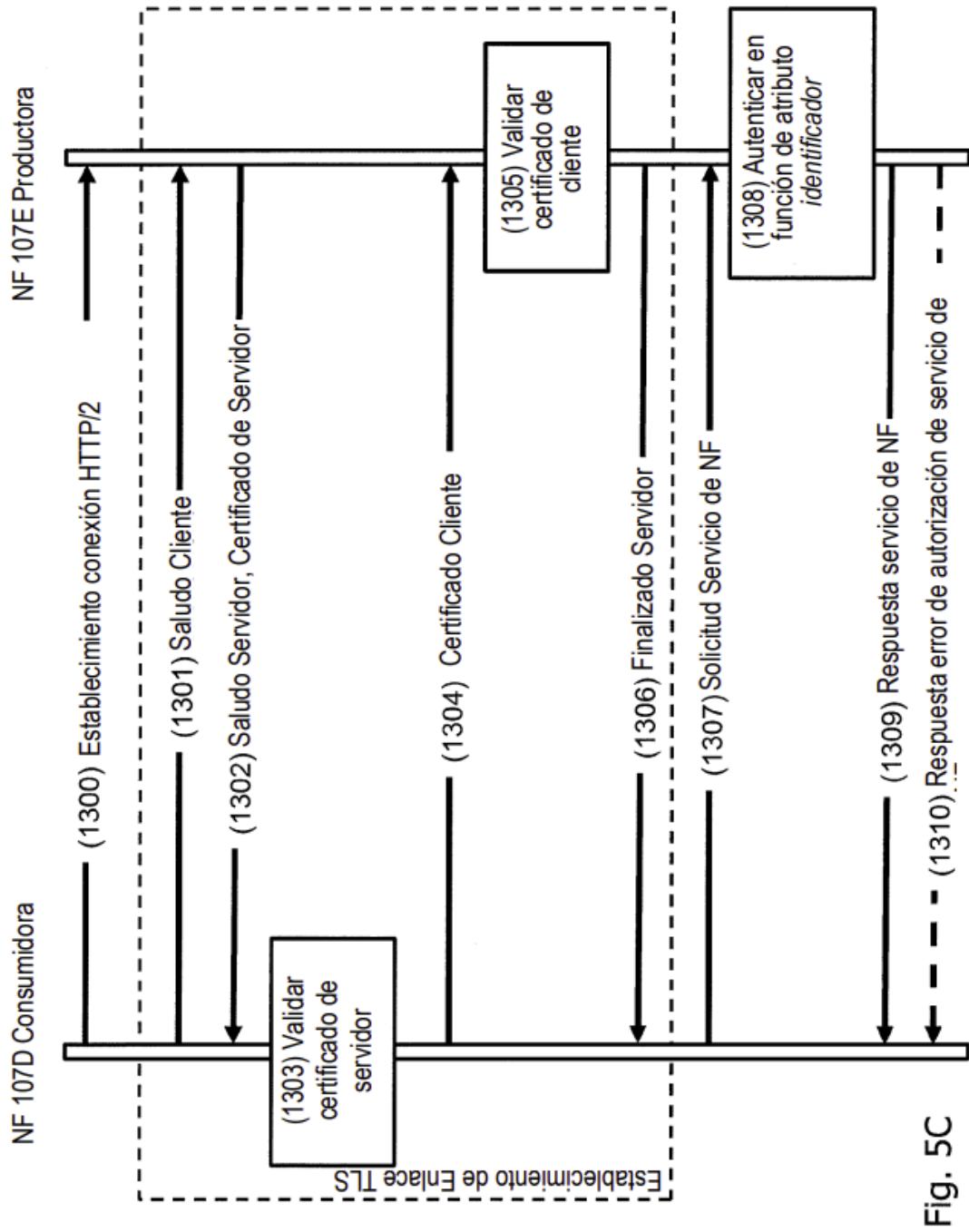


Fig. 5C

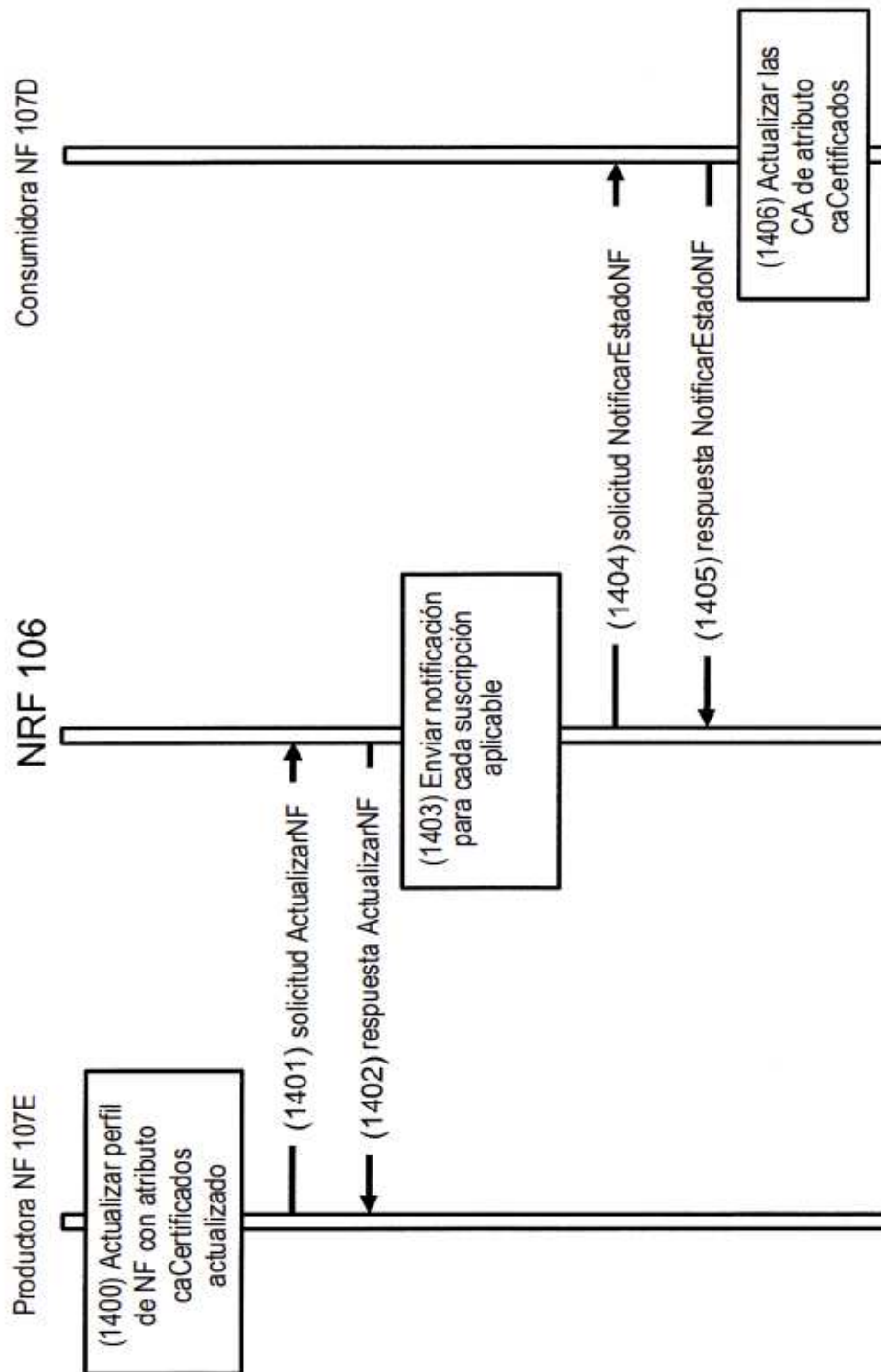


Fig. 5D