(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 955 584**

(51) Int. CI.:

H04L 9/40 (2012.01)
H04L 67/02 (2012.01)
H04W 12/02 (2009.01)
G06F 21/60 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.02.2019 PCT/EP2019/053784**

(87) Fecha y número de publicación internacional: **22.08.2019 WO19158681**

(96) Fecha de presentación y número de la solicitud europea: **15.02.2019 E 19704023 (1)**

(97) Fecha y número de publicación de la concesión europea: **09.08.2023 EP 3752947**

(54) Título: **Protección de un mensaje transmitido entre dominios de la red central**

(30) Prioridad:

16.02.2018 EP 18382092

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.12.2023

(73) Titular/es:

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

(72) Inventor/es:

SAARINEN, PASI;
MARTINEZ DE LA CRUZ, PABLO;
DE-GREGORIO-RODRIGUEZ, JESUS-ANGEL y
JOST, CHRISTINE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Protección de un mensaje transmitido entre dominios de la red central

Sector técnico

La presente solicitud se refiere, en general, a un sistema de comunicación inalámbrica y, más particularmente, a la protección de un mensaje transmitido entre diferentes dominios de la red central de un sistema de comunicación inalámbrica.

Antecedentes

El dominio de red de servicio de un usuario incluye el equipo y las funciones de la red central que son locales para el punto de acceso del usuario. El dominio de la red doméstica del usuario incluye el equipo y las funciones de la red central que son independientes de la ubicación del punto de acceso del usuario. El dominio de la red doméstica del usuario puede, por ejemplo, gestionar la información de suscripción del usuario y/o los servicios locales específicos. Cuando el dominio de la red de servicio del usuario es diferente del dominio de la red doméstica del usuario, el dominio de la red de servicio y el dominio de la red doméstica se comunican entre sí, por ejemplo, para la autenticación del usuario, para datos/servicios específicos del usuario, etc. En estos y otros casos, la comunicación entre diferentes dominios de la red central debe ser protegida (por ejemplo, con protección de confidencialidad y/o integridad), para garantizar que la comunicación no sea inspeccionada o modificada por partes no autorizadas.

Algunos contextos complican la protección de la comunicación entre dominios. En primer lugar, un proveedor de intercambio de interconexión de redes que soporte la interconexión entre diferentes dominios de la red central puede necesitar, de hecho, leer y/o modificar parte de la comunicación para ofrecer ciertos servicios valiosos a los operadores de red. En segundo lugar, garantizar la protección adecuada de la comunicación entre dominios frente a los formatos de comunicación en evolución amenaza con imponer una sobrecarga administrativa y operativa poco práctica. El documento de ERICSSON: “Comment contribution to S3-180223 (LS to CT3 CT4 on SBI Design and its Security Implications)”, vol. SA WG3, no. Gotemburgo (Suecia); 20180122 a 20180126, 17 de enero de 2018 (2018-01-17), se considera un documento relevante del estado de la técnica.

Compendio

La invención está definida en las reivindicaciones independientes 1, 9, 17 y 18.

Algunas realizaciones en el presente documento aprovechan una política de protección para la protección de seguridad entre dominios de un mensaje transmitido entre diferentes dominios de la red central de un sistema de comunicación inalámbrica. La política de protección puede indicar cuál o cuáles de la una o varias partes de la protección de seguridad entre dominios del mensaje debe ser aplicada o eliminada, por ejemplo, de modo que esa protección pueda ser aplicada o eliminada selectivamente solo en ciertas partes del mensaje. En realidad, en algunas realizaciones, la política de protección incluye información que indica a cuál o cuáles de la una o varias partes del contenido de un campo en el mensaje se debe aplicar o eliminar la protección de seguridad entre dominios. De esta manera, la protección se puede aplicar o eliminar de manera selectiva a cierta parte o a ciertas partes del contenido de un campo determinado, en lugar de al contenido del campo en su totalidad.

Alternativa o adicionalmente, en algunas realizaciones, una política de protección para la protección de seguridad entre dominios de un mensaje puede ser recibida y/o actualizada dinámicamente. Por ejemplo, en una realización, la política de protección aplicable para un determinado mensaje (por ejemplo, de un tipo específico) puede descubrirse y/o recuperarse dinámicamente en respuesta a la recepción del mensaje. En otra realización, la política de protección aplicable para el mensaje determinado puede estar incluida en el propio mensaje o asociada de otro modo con el mismo.

La protección de seguridad selectiva entre dominios de ciertas partes de un mensaje (por ejemplo, una o varias partes más del contenido de un campo determinado) según algunas realizaciones en el presente documento puede permitir, ventajosamente, que un proveedor de intercambio de interconexión de redes lea y/o modifique el mensaje según sea necesario para ofrecer servicios a los operadores de red. Alternativa o adicionalmente, la recepción dinámica y/o la capacidad de actualización de la política de protección según algunas realizaciones pueden proporcionar, ventajosamente, una protección flexible que evoluciona junto con los cambios de formateo del mensaje (por ejemplo, atribuibles a la evolución de las funciones de red en la red central), aun minimizando o al menos reduciendo la sobrecarga administrativa y/u operativa que, de otro modo, sería necesaria para dicha flexibilidad.

Más particularmente, las realizaciones del presente documento incluyen un procedimiento realizado por un equipo de la red en uno de múltiples dominios diferentes de la red central, de un sistema de comunicación inalámbrica. El procedimiento puede comprender, asimismo, recibir un mensaje que ha sido, o será, transmitido entre los diferentes dominios de la red central. El procedimiento también puede comprender aplicar protección de seguridad entre dominios o eliminar la protección de seguridad entre dominios de una o varias partes del mensaje (por ejemplo, una o varias partes del contenido de un campo en el mensaje) según una política de protección. En algunas realizaciones, la política de protección indica a cuál o cuáles de la una o varias partes del mensaje se le va a aplicar o eliminar una protección

de seguridad entre dominios. Por ejemplo, en una realización, la política de protección incluye información que indica a cuál o cuáles de la una o varias partes del contenido de un campo en el mensaje se va a aplicar o eliminar la protección de seguridad entre dominios. En algunas realizaciones, el equipo de red puede obtener la política de protección recibiendo la política de protección, por ejemplo, dinámicamente, en respuesta a una solicitud de descubrimiento. En algunas realizaciones, el procedimiento comprende, además, reenviar el mensaje, con protección de seguridad entre dominios aplicada o eliminada a una o varias partes, hacia un destino del mensaje.

En algunas realizaciones, el mensaje es un mensaje de Protocolo de transferencia de hipertexto (Hypertext Transfer Protocol, HTTP) y el campo es un campo HTTP. Por ejemplo, en algunas realizaciones, el mensaje de HTTP es un mensaje de solicitud de HTTP y el campo es un campo de ruta, y en el que el contenido del campo de ruta es una solicitud de identificador uniforme de recursos, URI (Uniform Resource Identifier).

En algunas realizaciones, la información incluye una o varias expresiones regulares que indican la una o varias partes. Alternativa o adicionalmente, en algunas realizaciones, la información incluye uno o varios punteros de notación de objetos de JavaScript, JSON (JavaScript Object Notation), que indican la una o varias partes.

En algunas realizaciones, la política de protección indica además, para cada una de la una o varias partes, un tipo de protección de seguridad entre dominios a aplicar o eliminar. En este caso, para cada una de la una o varias partes, el tipo de protección de seguridad entre dominios a aplicar o eliminar puede comprender protección de confidencialidad y/o protección de integridad.

En algunas realizaciones, la política de protección se incluye en el mensaje. En estas y otras realizaciones, el procedimiento puede comprender, además, recibir la política de protección desde equipos de red en una ruta que toma el mensaje desde un origen del mensaje hasta el destino del mensaje. En otras realizaciones, el procedimiento puede comprender, además, en respuesta a la recepción del mensaje, transmitir una solicitud de descubrimiento a una función de depósito de red, NRF (Network Repository Function), solicitar el descubrimiento de la política de protección para proteger el mensaje y recibir la política de protección en respuesta a la solicitud de descubrimiento.

Las realizaciones en el presente documento también incluyen un procedimiento realizado por los equipos de red para facilitar la protección de un mensaje transmitido entre diferentes dominios de la red central de un sistema de comunicación inalámbrica. El procedimiento puede comprender la obtención de una política de protección. En algunas realizaciones, la política de protección indica a cuál o cuáles de la una o varias partes del mensaje se le va a aplicar o eliminar la protección de seguridad entre dominios. Por ejemplo, en una realización, la política de protección incluye información que indica a cuál o cuáles de la una o varias partes del contenido de un campo en el mensaje se le va a aplicar o eliminar la protección de seguridad entre dominios. Independientemente, el procedimiento también puede comprender transmitir la política de protección. Por ejemplo, en algunas realizaciones, el procedimiento comprende transmitir la política de protección al equipo de red, en un dominio diferente de la red central, configurado para aplicar protección de seguridad entre dominios o eliminar la protección de seguridad entre dominios de la una o varias partes según la política de protección.

En algunas realizaciones, el procedimiento lo realiza un equipo de red que implementa una función de depósito de red, NRF. En este caso, el procedimiento puede comprender, además, recibir una solicitud de descubrimiento solicitando el descubrimiento de la política de protección para proteger el mensaje, y transmitir la política de protección en respuesta a la solicitud de descubrimiento. En otras realizaciones, el procedimiento puede ser realizado por un equipo de red en una ruta que toma el mensaje desde un origen del mensaje hasta el destino del mensaje. En estas y otras realizaciones, la política de protección puede estar incluida en el mensaje.

En algunas realizaciones, el mensaje es un mensaje de Protocolo de Transferencia de Hipertexto (HTTP) y el campo es un campo HTTP. Por ejemplo, en algunas realizaciones, el mensaje de HTTP es un mensaje de solicitud de HTTP y el campo es un campo de ruta, y en el que el contenido del campo de ruta es un identificador uniforme de recursos, URI.

En algunas realizaciones, la información incluye una o varias expresiones regulares que indican una o varias partes. Alternativa o adicionalmente, en algunas realizaciones, la información incluye uno o varios punteros de notación de objetos de JavaScript, JSON, que indican la una o varias partes

En algunas realizaciones, la política de protección indica, además, para cada una de la una o varias partes, un tipo de protección de seguridad entre dominios a aplicar o eliminar. En este caso, para cada una de la una o varias partes, el tipo de protección de seguridad entre dominios a aplicar o eliminar puede comprender protección de confidencialidad y/o protección de integridad.

Las realizaciones en el presente documento también incluyen los correspondientes aparatos, programas informáticos y portadoras (por ejemplo, medios no transitorios legibles por un ordenador). Por ejemplo, las realizaciones del presente documento también incluyen equipos de red configurados para su uso en uno de múltiples dominios diferentes de la red central de un sistema de comunicación inalámbrica. El equipo de red comprende circuitería de comunicación y circuitería de procesamiento. La circuitería de procesamiento puede ser configurada para recibir, a través de la circuitería de comunicación, un mensaje que ha sido, o será, transmitido entre el diferentes dominios de la red central. La circuitería de procesamiento también se puede configurar para aplicar protección de seguridad entre

dominios o eliminar la protección de seguridad entre dominios de una o varias partes del contenido de un campo en el mensaje según una política de protección que incluye información que indica a cuál o cuáles de la una o varias partes del contenido se va a aplicar o eliminar la protección de seguridad entre dominios. La circuitería de procesamiento puede ser configurada, además, para reenviar el mensaje, con protección de seguridad entre dominios aplicada o eliminada a la una o varias partes, hacia un destino del mensaje a través de la circuitería de comunicación.

Las realizaciones incluyen, además, un equipo de red que comprende una circuitería de comunicación y una circuitería de procesamiento. La circuitería de procesamiento está configurada para obtener una política de protección que incluye información que indica a cuál o cuáles de la una o varias partes del contenido de un campo en un mensaje se va a aplicar o eliminar la protección de seguridad entre dominios, en donde el mensaje se va a transmitir entre diferentes dominios de la red central de un sistema de comunicación inalámbrica. La circuitería de procesamiento también está configurada para transmitir la política de protección a través de la circuitería de comunicación.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques de un sistema de comunicación inalámbrica, según algunas realizaciones.

La figura 2A es un diagrama de bloques de un campo en un mensaje al que se aplica la protección de seguridad entre dominios, según algunas realizaciones.

La figura 2B es un diagrama de bloques del contenido de un campo, de ejemplo, en un mensaje al que se aplica la protección de seguridad entre dominios, según algunas realizaciones.

La figura 3 es un diagrama de flujo de llamadas de un proceso para que uno o varios servidores proxy obtengan una política de protección, según algunas realizaciones.

La figura 4 es un diagrama de flujo de llamadas de un proceso para que uno o varios servidores proxy obtengan una política de protección, según otras realizaciones.

La figura 5 es un diagrama de flujo lógico de un procedimiento realizado por un equipo de red, según algunas realizaciones.

La figura 6 es un diagrama de flujo lógico de un procedimiento realizado por un equipo de red, según otras realizaciones.

La figura 7 es un diagrama de bloques de un sistema de comunicación inalámbrica, según algunas realizaciones.

La figura 8 es un diagrama de flujo de llamadas de un proceso para proteger un mensaje que se transmite entre dominios de la red central, según algunas realizaciones.

La figura 9A es un diagrama de bloques de un equipo de red, según algunas realizaciones.

La figura 9B es un diagrama de bloques de un equipo de red, según otras realizaciones.

La figura 10A es un diagrama de bloques de un equipo de red, según otras realizaciones adicionales.

La figura 10B es un diagrama de bloques de un equipo de red, según otras realizaciones.

Descripción detallada

La figura 1 muestra un sistema de comunicación inalámbrica 10, según algunas realizaciones. El sistema 10 incluye una o varias redes de acceso por radio (Radio Access Network, RAN) 14 que conectan de manera inalámbrica dispositivos inalámbricos 12 a una o varias redes centrales (Core Network, CN) 16, por ejemplo, de una o varias redes móviles terrestres públicas (Public Land Mobile Network, PLMN). Las CN 16, a su vez, conectan los dispositivos inalámbricos 12 a una o varias redes de datos 18, por ejemplo, Internet, una red telefónica pública conmutada (Public Switched Telephone Network, PSTN), etc.

La una o varias CN 16 en algunas realizaciones tienen una arquitectura basada en servicios que aprovecha las interacciones basadas en servicios entre las funciones de red (Network Function, NF) de la CN, dos de las cuales se muestran como NF 20, 30. Cada NF 20, 30 puede implementarse mediante equipos de red, ya sea como un elemento de red en hardware específico, como una instancia de software que se ejecuta en un hardware específico, o como una función virtualizada instanciada en una plataforma adecuada, por ejemplo, en una infraestructura de la nube. Cuando el sistema 10 es un sistema 5G, por ejemplo, las NF en el plano de control pueden incluir una función de gestión del acceso y la movilidad (Access and Mobility Management Function, AMF), una función de gestión de sesión (Session Management Function, SMF), una función de control de políticas (Policy Control Function, PCF), una función de servidor de autenticación (AUthentication Server Function, AUSF), una función de gestión de datos unificados (Unified Data Management, UDM), etc.

Una NF puede proporcionar sus servicios a otras NF autorizadas que consumen esos servicios. Por lo tanto, una NF puede asumir una función de proveedor, como proveedor de un servicio (proveedor de servicios de NF) y/o una función de consumidor, como consumidor de un servicio (consumidor de servicios de NF). En un ejemplo, la NF 20 funciona como consumidor de servicios de NF para consumir servicios proporcionados por la NF 30, como proveedor de servicios de NF. Independientemente, como parte de, o para que un proveedor de servicios de NF proporcione sus servicios a un consumidor de servicios de NF, las NF 20, 30 intercambian comunicación en forma de mensajes. En algunas realizaciones, sin embargo, las NF 20, 30 están en diferentes PLMN. Por lo tanto, en estas y otras realizaciones, estos mensajes deben ser transmitidos entre diferentes dominios de la red central.

La figura 1 muestra que los servidores proxy 40, 50 facilitan el intercambio de mensajes entre dominios. Cada servidor proxy 40, 50 está configurado como un servidor proxy para un dominio respectivo de la red central. Donde las NF 20, 30 están en PLMN diferentes, por ejemplo, los servidores proxy 40, 50 pueden ser servidores proxy de borde (por ejemplo, en forma de servidores proxy de protección perimetral de seguridad, SEPP, Security Edge Protection Proxies) en el perímetro de una PLMN respectiva. Cada servidor proxy 40, 50 intercepta mensajes (por ejemplo, en una capa de aplicación) que entran y/o salen de ese dominio, por ejemplo, para inspeccionar y/o filtrar los mensajes (por ejemplo, en busca de malicia), para realizar el equilibrio de carga, o similares. Los servidores proxy 40, 50 en algunas realizaciones ocultan la topología de sus respectivos dominios de la red central. Los servidores proxy 40, 50 también protegen los mensajes transmitidos entre dominios de la red central.

Más particularmente a este respecto, la figura 1 muestra como ejemplo que NF 20 es la fuente de un mensaje 60 (por ejemplo, un mensaje de capa de aplicación) que se transmitirá a la NF 30 como el destino del mensaje 60. Con las NF 20, 30 en diferentes dominios de la red central, el servidor proxy 40 recibe (por ejemplo, intercepta) el mensaje 60 antes de que el mensaje 60 sea transmitido a través del límite del dominio de la red central. El servidor proxy 40 aplica protección de seguridad entre dominios 70 al mensaje 60. Cuando la protección 70 incluye protección de confidencialidad, por ejemplo, la aplicación de la protección 70 puede implicar cifrado. Alternativa o adicionalmente, cuando la protección 70 incluye protección de integridad, la aplicación de la protección 70 puede implicar la adición de una suma de comprobación, un código de autenticación de mensaje (Message Authentication Code, MAC), una firma u otra información para detectar la manipulación maliciosa de mensajes. En cualquier caso, a continuación, el servidor proxy 40 reenvía el mensaje 60, con la protección 70 aplicada, hacia la NF 30, como el destino 30 del mensaje. El servidor proxy 50 recibe (por ejemplo, intercepta) el mensaje 60 entrante al dominio de la NF 30 de la red central. El servidor proxy 50 elimina la protección de seguridad entre dominios 70 (por ejemplo, realizando descifrado y/o confirmación de suma de comprobación y eliminación). A continuación, el servidor proxy 50 reenvía el mensaje 60 hacia la NF 30 como destino 30 del mensaje.

Según algunas realizaciones, la protección de seguridad entre dominios 70 se aplica a una o varias porciones o partes del mensaje 60, por ejemplo, de tal manera que la protección se puede aplicar selectivamente solo a ciertas partes del mensaje 60, en lugar de tener que aplicarse al mensaje 60 en su totalidad. En realidad, en algunas realizaciones, la protección 70 se aplica a una o varias partes del contenido de un cierto campo 62 en el mensaje 60. El campo 62 a este respecto puede estar predefinido (por ejemplo, basándose en el protocolo según el cual se genera el mensaje 60) con contenido de cierto tipo y/o propósito. El campo 62 en algunas realizaciones también se puede denominar elemento o elemento de información. De esta manera, la protección se puede aplicar selectivamente a cierta parte o a ciertas partes del contenido de un campo determinado, en lugar de al contenido del campo en su totalidad.

La figura 2A muestra un ejemplo. Tal como se muestra en la figura 2A, el contenido del campo 62 tiene múltiples partes 62A, 62B y 62C. Estas partes pueden tener todas el mismo tipo y/o propósito, con el fin de formar juntos el contenido del campo. Pero la protección 70 se puede aplicar selectivamente a la parte 62B, con exclusión de las partes 62A y 62C. En algunas realizaciones, por ejemplo, el servidor proxy 50 extrae la parte 62B del campo 62 y aplica la protección 70 selectivamente a la parte extraída 62B (por ejemplo, cifrando selectivamente la parte 62B y/o generando una suma de comprobación selectivamente para la parte 62B). Las partes 62A y 62C pueden permanecer sin protección. El servidor proxy 60, tras la recepción del mensaje 60 puede, a su vez, extraer la parte 62B del campo 62 y eliminar la protección 70 de manera selectiva de la parte 62B extraída (por ejemplo, descifrando selectivamente la parte 62B y/o confirmando y eliminando la suma de comprobación de la parte 62B).

La figura 2B muestra un ejemplo específico del contenido del campo en algunas realizaciones, donde el mensaje 60 es un mensaje de protocolo de transferencia de hipertexto (HTTP) y el campo 62 es un campo HTTP (por ejemplo, un cuerpo o una parte del cuerpo del mensaje de HTTP, o un campo en una cabecera o pseudo cabecera HTTP). Tal como se muestra, el mensaje 60 es una solicitud de GET de HTTP y el campo 62 es un campo RUTA. El contenido del campo RUTA es un identificador uniforme de recursos (URI) de solicitud. Por lo tanto, en este caso, la protección 70 puede ser aplicada a una o varias partes del URI de solicitud en el campo RUTA. De hecho, el contenido del campo RUTA (es decir, el URI de la solicitud) en este ejemplo contiene múltiples partes 62A, 62B y 62C, con la protección 70 aplicada selectivamente solo a la parte 62B del URI de solicitud. La parte 62B en este ejemplo incluye un identificador de abonado en forma de un identificador de abonado móvil internacional (International Mobile Subscriber Identifier, IMSI). Otras partes 62A y 62C pueden permanecer desprotegidas.

La protección selectiva de seguridad entre dominios de ciertas partes del mensaje 60 (por ejemplo, una o varias partes del contenido del campo 62) según algunas realizaciones, puede salvaguardar ventajosamente esas ciertas partes contra la inspección y/o manipulación maliciosa no autorizada, mientras que al mismo tiempo permite que las entidades lean y/o modifiquen otras partes. Por ejemplo, un proveedor de intercambio de interconexión de redes que proporciona la conexión entre diferentes dominios de la red central puede leer y/o modificar partes desprotegidas según sea necesario para ofrecer servicios a los operadores de red. Por lo tanto, la granularidad de la protección se puede adaptar estrechamente a la granularidad del contenido (por ejemplo, sensible) que realmente necesita protección. Esto evita una protección demasiado amplia que ponga en peligro la utilización de otros contenidos por parte de otras entidades y/o que pueda aumentar innecesariamente los recursos de comunicación o la potencia de procesamiento.

En particular, algunas realizaciones en el presente documento aprovechan una política de protección 80 para realizar esta protección selectiva de seguridad entre dominios de ciertas partes del mensaje 60 (por ejemplo, una o varias partes del contenido del campo 62). La política de protección 80 incluye información que indica a cuál o cuáles de la una o varias partes del mensaje 60 se va a aplicar la protección de seguridad entre dominios 70 (por ejemplo, por parte del servidor de proxy 40) o eliminar (por ejemplo, por parte del servidor de proxy 50). Entonces, en algunas realizaciones, esta información indica a cuál o cuáles de la una o varias partes del contenido de un campo 62 se va a aplicar o eliminar la protección de seguridad entre dominios 70. Cabe señalar que la información puede indicar efectivamente a cuál o cuáles de la una o varias partes se debe aplicar/eliminar la protección 70, ya sea explícitamente indicando la parte o las partes a las que se va a aplicar/eliminar la protección 70, o implícitamente indicando la parte o las partes a las que no se va a aplicar/eliminar la protección 70. La política de protección 80 en una realización también indica, para cada una de la una o varias partes, un tipo de protección de seguridad entre dominios 70 que se aplicará o eliminará (por ejemplo, protección de confidencialidad y/o integridad).

Por ejemplo, en algunas realizaciones, la información en la política de protección 80 incluye una o varias expresiones regulares que indican una o varias partes. Una expresión regular en este sentido puede ser una secuencia de caracteres que define un patrón de búsqueda. El patrón de búsqueda, a su vez, puede ser utilizado por algoritmos de búsqueda para encontrar un cierto patrón de caracteres en el mensaje 60 (por ejemplo, en el contenido del campo).

Por ejemplo, una expresión regular que se puede utilizar para encontrar la parte 62B en la figura 2B (por ejemplo, IMSI) puede ser “^/udm-sdm/v1/([^/?#]+)/nssai$”. En este ejemplo, el carácter circunflejo (es decir, ^) y el carácter de signo de dólar (es decir, $) son anclas que no “consumen” ningún carácter, sino que vinculan el patrón al principio y al final de la cadena que se busca. Los caracteres ([^/?#]+) en la expresión regular capturan cualquier subpatrón o subgrupo que incluye una o varias apariciones de cualquier carácter excepto el carácter de barra inclinada (/), el carácter de signo de interrogación (?) y el carácter de almohadilla (#). Este subpatrón o subgrupo capturado sale del algoritmo de búsqueda. En consecuencia, explicar el contenido del campo mediante la expresión regular proporciona el subpatrón “imsi-214050123456789”. Por lo tanto, la protección 70 puede ser aplicada selectivamente solo a este subpatrón, con exclusión de otras partes 62A y 62C del contenido del campo.

Por supuesto, una expresión regular es solo una forma de indicar una parte tal como se utiliza en el presente documento. La política de protección 80 puede incluir cualquier tipo de expresión, patrón, sintaxis, idioma, delimitador, puntero, regla u otra información que indique una o varias partes. Por ejemplo, en unas realizaciones, la información puede ser cualquier información que indique un patrón, token o subcadena dentro de una cadena más amplia. En el ejemplo de la figura 2B, por ejemplo, la información puede indicar alternativamente la parte 62B como el tercer fragmento de ruta en el contenido del campo; es decir, el subpatrón o subgrupo de caracteres que se encuentran entre el tercer y cuarto tokens o delimitadores en forma de barra inclinada (/). En otras realizaciones adicionales, la información puede incluir uno o varios rangos de bytes dentro del campo 62, y/o uno o varios rangos de bits dentro del campo 62, que indican la una o varias partes.

En otras realizaciones adicionales, la información en la política de protección 80 incluye uno o varios punteros de notación de objeto JavaScript, JSON, que indican una o varias partes. Un puntero de JSON (por ejemplo, tal como se define en RFC 6901) es una sintaxis de cadena para identificar un valor específico dentro de un documento de JSON. Un puntero de JSON puede expresarse en valores de cadena de JSON y/o identificadores de fragmentos de URI. Un puntero de JSON, en particular, es una cadena Unicode que contiene una secuencia de cero o más tokens de referencia. Cada token está precedido por un carácter de barra inclinada ‘/’. Por lo tanto, en estas y otras realizaciones, la política de protección 80 como ejemplo puede indicar una o varias partes de contenido en el cuerpo o carga útil de un mensaje de HTML, donde ese cuerpo o carga útil incluye un documento de JSON.

Con independencia de la naturaleza particular de la información en la política de protección 80, estos ejemplos muestran que la política de protección 80 en algunas realizaciones indica la parte o las partes (a las que se va a aplicar o eliminar la protección 70) con información que es agnóstica, independiente y/o genéricamente aplicable a cualquiera de los contenidos del mensaje/campo subyacente o el protocolo de transmisión del mensaje. La política de protección 80 puede ser capaz, por ejemplo, de indicar cualquier parte de contenido en un campo 62 con el mismo tipo de información general (por ejemplo, una expresión regular), independientemente del tipo, estructura o formato del contenido del campo. Es decir, en un caso, la información se puede formar (por ejemplo, como una expresión regular particular) para indicar una cierta parte del contenido en el campo 62 basándose en el contenido que tiene un cierto tipo o formato (por ejemplo, un IMSI), pero, en otro caso, la información puede estar formada (por ejemplo, como una expresión regular diferente) para indicar una parte diferente del contenido en el campo 62 basándose en el contenido

que tiene un tipo o formato diferente (por ejemplo, un identificador de celda). Pero la información en ambos casos tiene el mismo carácter general (por ejemplo, ambas son expresiones regulares), con el fin de permitir universalmente que los servidores proxy 40, 50 identifiquen cualquier parte o partes independientemente de si el tipo, la estructura o el formato del contenido subyacente evoluciona o de cómo lo hace. En consecuencia, la configuración de los servidores proxy 40, 50 para comprender o procesar de manera genérica expresiones regulares u otra información en la política de protección 80 equipa suficientemente a los servidores proxy 40, 50 para aplicar o eliminar selectivamente la protección 70 a cualquier parte de contenido en el mensaje 60 o el campo 62, incluso sin que los servidores proxy 40, 50 están configurados para comprender más específicamente ese contenido. Por lo tanto, en el ejemplo de la figura 2B, un proxy simplemente necesita comprender cómo procesar una expresión regular para proteger la parte 62B, sin tener que comprender más específicamente cómo identificar un IMSI. Esto significa que los servidores proxy 40, 50 pueden permanecer ignorantes de cómo cambia o evoluciona el contenido subyacente (por ejemplo, en términos de su forma o estructura), tal como en respuesta a la introducción de nuevas entidades (por ejemplo, funciones de red) y/o servicios (por ejemplo, representados por sus URI de HTTP) al sistema 10. En algunas realizaciones, por lo tanto, es la información en la política de protección 80 (por ejemplo, las expresiones regulares) la que cambia o evoluciona dinámicamente para dar cuenta de los cambios o la evolución del contenido subyacente del mensaje 60 (por ejemplo, en términos de su estructura o formato), en lugar de la configuración general de los servidores proxy para identificar la parte o las partes utilizando ese tipo de información.

Alternativa o adicionalmente a las realizaciones anteriores, el servidor proxy 40 o 50 puede recibir y/o actualizar dinámicamente una política de protección 80 para la protección de seguridad entre dominios 70 de un mensaje 60. La recuperación dinámica y/o la actualización de la política 80 puede tener en cuenta los cambios o evolución en el contenido del mensaje 60. De esta manera, la configuración del propio servidor proxy 40 o 50 no necesita ser actualizada (manualmente) para tener en cuenta dicho cambio o evolución. Según algunas realizaciones, esto puede proporcionar, ventajosamente, una protección flexible que evoluciona junto con los cambios de formateo del mensaje (por ejemplo, atribuibles a la evolución de las funciones de red o servicio en la red central), aun minimizando o al menos reduciendo la sobrecarga administrativa y/u operativa que de otro modo se requeriría para dicha flexibilidad.

La figura 3, por ejemplo, muestra algunas realizaciones en las que el servidor proxy 40 y/o 50 descubre dinámicamente la política de protección 80 de una o varias funciones de depósito de red (NRF) 90, por ejemplo, en respuesta a la recepción del mensaje 60. Tal como se muestra, la NF 20, como origen del mensaje 60, transmite el mensaje 60, que es interceptado o recibido de otro modo por el servidor proxy 40 (etapa 1). En respuesta a la recepción del mensaje 60, el servidor proxy 40 transmite una solicitud de descubrimiento 92 a un servicio de descubrimiento (en su dominio de la red central) solicitando el descubrimiento de la política de protección 80 para proteger el mensaje 60 (etapa 2). El servicio de descubrimiento se muestra en este caso como siendo implementado por una función de depósito de red, NRF, 90A pero, en otras realizaciones, puede ser implementado mediante una función independiente coubicada con la NRF, o mediante otros equipos o funciones de red. Independientemente de esto, el servidor proxy 40 recibe la política de protección 80 en respuesta a la solicitud de descubrimiento (etapa 3). El servidor proxy 40 aplica protección a una o varias partes del mensaje 60 (por ejemplo, una o varias partes del contenido del campo 62) determinadas según la política de protección 80, y transmite el mensaje protegido 60 a través del límite del dominio de la red central al servidor proxy 50 (etapa 4). En respuesta a la recepción del mensaje 60, el servidor proxy 50 transmite, a su vez, una solicitud de descubrimiento 94, a un servicio de descubrimiento (en su dominio de la red central), que se muestra implementado mediante la NRF 90B (etapa 5). En respuesta a la solicitud de descubrimiento, el servidor proxy 50 recibe la política de protección 80 del servicio de descubrimiento (etapa 6). El servidor proxy 50 elimina la protección de la una o varias partes del mensaje 60 (por ejemplo, una o varias partes del contenido del campo 62) determinadas según la política de protección 80, y transmite el mensaje 60 (sin protección) hacia la NF 30 como destino del mensaje (etapa 7).

Aunque no se muestra, en algunas realizaciones, el origen y/o el destino del mensaje proporciona la política de protección 80 aplicable para el mensaje 60 al servicio de descubrimiento en uno o varios de los dominios de la red central, por ejemplo, para el descubrimiento posterior de esa política 80, tal como se muestra en la figura 3. Por ejemplo, donde la NF 30 es un proveedor de NF que proporciona un servicio a la NF 20 como un consumidor de NF, y el mensaje 60 es un mensaje que la NF 20 envía a la NF 30 para consumir ese servicio, la NF 30 como proveedor de NF en algunas realizaciones proporciona su perfil de servicio a la NRF 90B (por ejemplo, como parte del registro inicial o de la actualización de registro), incluida la política de protección 80 aplicable para uno o varios mensajes utilizados para consumir un servicio proporcionado por la NF 30. La NRF 90B puede, a su vez, distribuir o proporcionar de otro modo el perfil de servicio o al menos la política de protección 80, a la NRF 90A, para su descubrimiento posterior por parte de las NF de potenciales consumidores.

Sin embargo, en otras realizaciones más, el servidor proxy 40 y/o 50 puede suscribirse para recibir proactivamente políticas de protección nuevas o actualizadas desde la NRF 90A y/o 90B. En estas y otras realizaciones, el servidor proxy 40 y/o 50 puede almacenar (por ejemplo, en la memoria caché) las políticas de protección recibidas en previsión de una utilización posterior para proteger los mensajes transmitidos entre los dominios de la red central.

La figura 4, por el contrario, muestra otras realizaciones donde el servidor proxy 40 y/o 50 recibe la política de protección 80 de las funciones o equipos de la red en una ruta que el mensaje 60 toma desde el origen hasta el destino del mensaje 60. En particular, la figura 4 muestra que la NF 20, como origen del mensaje, transmite el mensaje 60 con la política de protección 80 incorporada o incluida de otro modo en el propio mensaje 60 (por ejemplo, en la cabecera

del mensaje) (etapa 1). De esta manera, el servidor proxy 40 recibe la política de protección 80 desde el origen del mensaje 60. E continuación, el servidor proxy 40 transmite el mensaje 60 protegido a través del límite del dominio de la red central, de nuevo con la política de protección 80 incluida en el mensaje 80 (etapa 2). En consecuencia, el servidor proxy 50 recibe la política de protección 80 del servidor proxy 40 en un dominio diferente de la red central. A continuación, el servidor proxy 50 puede eliminar la protección del mensaje 60 y reenviarlo hacia la NF 30 como destino (etapa 3).

A la vista de las variaciones y modificaciones anteriores, el equipo de red en algunas realizaciones realiza, en general, el procedimiento 100 que se muestra en la figura 5. El equipo de red puede ser configurado como un servidor proxy para uno de múltiples dominios diferentes de la red central de un sistema de comunicación inalámbrica 10. Por ejemplo, el procedimiento 100 puede ser realizado por el equipo de red configurado como servidor proxy 40 o servidor proxy 50. El procedimiento 100, tal como se muestra, incluye recibir un mensaje 60 que ha sido, o será, transmitido entre los diferentes dominios de la red central (bloque 110). El procedimiento 100 también puede incluir recibir una política de protección 80 que incluye información que indica a cuál o cuáles de la una o varias partes del mensaje 60 (por ejemplo, una o varias partes del contenido de un campo 62 en el mensaje 60) se va a aplicar o eliminar la protección de seguridad entre dominios 70 (bloque 120). El procedimiento 100 puede incluir, además, la aplicación de protección de seguridad entre dominios o la eliminación de la protección de seguridad entre dominios de la una o varias partes, según la política de protección 80 (bloque 130). El procedimiento 100 en algunas realizaciones también puede incluir el reenvío del mensaje 60, con protección de seguridad entre dominios aplicada o eliminada a la una o varias partes, hacia un destino del mensaje 60 (bloque 140).

En algunas realizaciones, el procedimiento comprende, además, en respuesta a la recepción del mensaje 60, transmitir una solicitud de descubrimiento a una función de depósito de red, NRF, solicitar el descubrimiento de la política de protección 80 para proteger el mensaje 60, y recibir la política de protección en respuesta a la solicitud de descubrimiento. Alternativamente, el procedimiento puede comprender recibir la política de protección 80 del equipo de red en una ruta que toma el mensaje desde el origen del mensaje hasta el destino del mensaje.

Asimismo, a la vista de las variaciones y modificaciones anteriores, el equipo de red en otras realizaciones realiza, en general, el procedimiento 200 que se muestra en la figura 6 para facilitar la protección de un mensaje 60 transmitido entre diferentes dominios de la red central de un sistema de comunicación inalámbrica 10. El procedimiento 200 puede ser realizado, por ejemplo, por equipos de red que implementan NF 20, servidores proxy 40, servidores proxy 50, NF 30 o una o varias NRF 90. El procedimiento 200, tal como se muestra a este respecto, incluye la obtención de una política de protección 80 que incluye información que indica a cuál o cuáles de la una o varias partes del mensaje 60 (por ejemplo, una o varias partes del contenido de un campo 62 en el mensaje 60) se va a aplicar o eliminar la protección de seguridad entre dominios 70 (bloque 210). El procedimiento 200 también puede incluir la transmisión de la política de protección 80 (bloque 220).

Por ejemplo, en algunas realizaciones, la transmisión de la política de protección comprende transmitir la política de protección al equipo de red configurado como un servidor proxy de uno de los diferentes dominios de la red central, para aplicar la protección de seguridad entre dominios a la una o varias partes o eliminar la protección de seguridad entre dominios de la una o varias partes, según la política de protección.

Alternativa o adicionalmente, el procedimiento puede ser realizado por un equipo de red que implementa una función de depósito de red, NRF, y puede comprender, además, recibir una solicitud de descubrimiento que solicita el descubrimiento de la política de protección para proteger el mensaje, y transmitir la política de protección en respuesta a la solicitud de descubrimiento.

Alternativamente, el procedimiento puede ser realizado por un equipo de red en una ruta que toma el mensaje desde el origen del mensaje hasta el destino del mensaje (por ejemplo, por una NF 20, servidores proxy 40, servidores proxy 50 o una NF 30).

A continuación, se explicarán algunas realizaciones con particular relevancia para ellas aplicables en ocasiones a 5G.

3GPP funciona en 5G y su red central asociada (5GC), que proporciona servicios a los usuarios que se conectan, desde la autenticación hasta la asignación de direcciones IP y el enrutamiento de paquetes. Sin embargo, la red central 5G es significativamente diferente de las generaciones anteriores.

Uno de los cambios en la arquitectura 5G es implementar una llamada arquitectura basada en servicios (Service-Based Architecture, SBA). En esta nueva arquitectura, varias de las interfaces dentro de la red central (incluidas las interfaces de itinerancia) se cambian del estilo de telecomunicaciones heredado a modernas interfaces de programación de aplicaciones (Application Programming Interfaces, API) basadas en la web. Los detalles de estas API se están trabajando actualmente en el grupo SA2 del 3GPP, en los documentos 23.501 y 23.502 de arquitectura de la red central del 5G, así como en los grupos CT del 3GPP.

Existen varias alternativas para desarrollar e implementar una arquitectura basada en servicios. De entre las diversas posibilidades, el grupo CT4 del 3GPP seleccionó una arquitectura basada en el modelo arquitectónico transferencia de estado representacional (Representational State Transfer, REST). En este modelo, las diferentes entidades (servicios, funciones de red, etc.) en el sistema 5G interactúan entre sí invocando acciones en un llamado “recurso”,

que se identifica en HTTP mediante el Identificador Uniforme de Recursos (URI). Por lo tanto, las diferentes acciones a invocar en las diferentes entidades del sistema están definidas por los diferentes comandos estándar de HTTP (por ejemplo, GET, POST, PUT, DELETE, etc.), mientras que los mensajes de HTTP transmiten representaciones de los recursos afectados en la carga útil de HTTP. Estas representaciones se pueden formatear en diferentes lenguajes de codificación de datos (por ejemplo, JSON).

La red central 5G puede seguir estos requisitos: protocolo principal: HTTP/2; protocolo de transporte: TCP; estilo de diseño de API RESTful; formato de serialización de datos: JSON; Interacciones iniciadas por el servidor: "*Web-hook*"; y lenguaje de definición de interfaz: OpenAPI 3.0.0 (anteriormente conocido como "Swagger").

Las diferentes funciones de red en la red central 5G exponen sus servicios a través de una interfaz de programación de aplicaciones (API). Esta API define los recursos de HTTP (Universal Resource Identifiers, URI), las operaciones permitidas (GET, POST, PUT,...) y el formato del datos transportados en la carga útil del mensaje (cuerpo del mensaje).

A menos que la información sobre los proveedores de servicios de NF esté configurada localmente en los consumidores de servicios de NF correspondientes (este puede ser el caso si el servicio de NF esperado o la NF están en la misma PLMN que la NF solicitante), los consumidores de servicios de NF descubren y seleccionan dinámicamente productores de servicios de NF utilizando una función de depósito de red, NRF. La NRF es la función lógica que se utiliza para mantener el perfil de NF de las instancias disponibles de los productores de servicios de NF y sus servicios soportados, recibir solicitudes de descubrimiento de servicios de NF de los consumidores de servicios de NF y proporcionar la información de las instancias disponibles de los productores de servicios de NF correspondientes, al consumidor de servicios de NF solicitante.

Con el fin de permitir el acceso a un tipo de NF o servicio de NF solicitado, la NF solicitante inicia el descubrimiento de la NF o el servicio de NF proporcionando a la NRF el tipo de NF o el servicio específico que está intentando descubrir (por ejemplo, la función de gestión de sesión, SMF, la función de políticas de tarificación, PCF (Policy Control Function), el equipo de usuario, UE (User Equipment), informes de ubicación) y otros parámetros del servicio (por ejemplo, información relacionada con la segmentación). Dependiendo del modelo de enrutamiento de mensajes elegido, la NRF puede proporcionar a la NF solicitante la dirección IP o el nombre completamente definido del dominio (Fully Qualified Domain Name, FQDN) o el identificador de los servicios y/o la o las instancias relevantes de la NF. Con base en esa información, la NF solicitante puede seleccionar una instancia de NF específica o una instancia de NF que pueda proporcionar un servicio de NF en particular (por ejemplo, una instancia de PCF que pueda proporcionar autorización de política).

En los casos de itinerancia (es decir, cuando el usuario está accediendo a una red distinta de su red doméstica, donde el usuario tiene su suscripción), la comunicación puede estar protegida (por ejemplo, criptográficamente) entre la red visitada y la red doméstica, para garantizar que la información enviada a través de las redes interconectadas no sea inspeccionada o modificada por terceros no autorizados. Esta tarea la realiza un elemento de red llamado SEPP (Security Edge Protection Proxy, Servidor proxy de protección de borde de seguridad). Puede haber un vSEPP (el SEPP en la red visitada) y un hSEPP (el SEPP en la red doméstica) que se comunican a través de una interfaz N32.

La protección de la comunicación entre los SEPP puede estar en la capa de aplicaciones. En algunas realizaciones, la protección de integridad se aplica a todos los atributos transferidos a través de la interfaz N32. Alternativa o adicionalmente, uno o varios de los siguientes atributos pueden tener protección de confidencialidad cuando son enviados a través de la interfaz N32: vectores de autenticación; material criptográfico; datos de ubicación, por ejemplo, ID de celda e ID de celda física; o identificador permanente de abonado (Subscriber Permanent Identifier, SUPI) tal como el identificador de abonado móvil internacional (IMSI).

Como parte de las funciones del SEPP, una de ellas es proteger la información enviada en los diferentes campos que componen los mensajes de HTTP. Estos campos de HTTP pueden ser, por ejemplo, el URI de solicitud de HTTP, las cabeceras de HTTP y diferentes partes del cuerpo (o carga útil) de HTTP.

La conexión entre dos PLMN se realiza, en general, a través de los llamados proveedores de IPX. Además de la conexión real, los proveedores de IPX también suelen ofrecer servicios adicionales a los operadores. Algunos de estos servicios se basan en la lectura y/o cambio de campos en los mensajes enviados entre varias PLMN. Por lo tanto, es deseable que ciertas partes o campos del mensaje no estén protegidos criptográficamente cuando se envían a través de la interfaz N32 entre el vSEPP y el hSEPP.

Resumiendo, el SEPP debe proteger (cifrar y/o proteger la integridad) algunos de los campos de información o partes en los mensajes enviados en la N32, y algunas otras partes de los mensajes que el SEPP debe dejar sin protección, por ejemplo, para realizar servicios adicionales proporcionados por proveedores de IPX.

Sin embargo, si se envía un nuevo tipo de mensaje a través de la N32, que no se definió en la implementación o en la última actualización del SEPP, las partes del mensaje que deben ser protegidas no son conocidas explícitamente por el SEPP. Sin embargo, es deseable que el SEPP pueda proporcionar sus servicios sin requerir una actualización de software como resultado de la evolución funcional habitual de las diferentes funciones de red en la red central.

Algunas realizaciones en el presente documento proporcionan una política que define qué partes de un mensaje necesitan ser protegidas, y de qué manera deben ser protegidas (confidencialidad, integridad). En una o varias realizaciones, esta política se expresa en un idioma o "máscara" que es aplicable (coincidencia de patrones) para nuevos tipos de mensajes. De esta manera, la política se puede expresar de manera dinámica y no es necesario conocerla en el momento de la implementación o última actualización del SEPP. Por lo tanto, las realizaciones en el presente documento también incluyen flujos para informar al SEPP de la política aplicable para un mensaje específico. Por lo tanto, las realizaciones proporcionan un modo dinámico y flexible de proteger selectivamente partes de los mensajes enviados en la N32, de tal manera que las entidades que realizan dicha protección (cifrado y/o protección de integridad) no dependen de la configuración estática y no necesitan ser cambiadas cuando aparecen nuevas entidades (funciones de red) y se agregan nuevos servicios (representados por sus URI de HTTP) al sistema.

Algunas realizaciones permiten la aplicación de un mecanismo de seguridad sin afectar al diseño (API) de los servicios entre las PLMN doméstica y visitada. Adicional o alternativamente, algunas realizaciones permiten la protección (cifrado y/o protección de integridad) de elementos de información confidenciales (tal como identidades de usuario, tal como IMSI) que se encuentran en mensajes de HTTP en el tráfico de 5G transportado entre operadores de red de manera flexible, no vinculada a la actual definición de las API de servicio, y preparada para la introducción de nuevas funciones de red, servicios y API en una posterior evolución de la red central de 5G.

A continuación, se explican dos variantes como ejemplos de flujos de señalización para informar al SEPP de la política para un mensaje específico. La figura 7 muestra un contexto de ejemplo para explicar las variantes 1 y 2.

En la variante 1, el SEPP consulta a la NRF para obtener información sobre la política de protección aplicable. Tal como se muestra, la función de red NF1 en una PLMN1 pretende enviar un mensaje a una función de red NF2 en una PLMN2. El mensaje se enruta a través de SEPP1 y SEPP2 en la PLMN1 y la PLMN2. Cuando el SEPP1 recibe el mensaje, comprueba si tiene almacenada una política de protección para este tipo de mensajes, que aún no haya caducado. Si no se dispone de dicha política de protección, el SEPP1 consulta a la NRF en la PLMN1 (denominada NRF1).

Si la NRF1 fue consultada por el SEPP1 sobre las políticas de protección aplicables al mensaje, la NRF1 envía las políticas de protección disponibles al SEPP1. La NRF1 puede necesitar consultar a la NRF2, la NRF en la PLMN2. Es posible que la NRF1 haya recibido las políticas de protección de la NF1 en el momento del registro. Es posible que la NRF2 haya recibido las políticas de protección de la NF2 en el momento del registro.

Antes de reenviar el mensaje al SEPP2, el SEPP1 realiza la protección (por ejemplo, protección criptográfica) del mensaje según la política recibida de la NRF1 y/o la NRF2. El SEPP1 puede incluir la política de protección en el mensaje que reenvía. Cabe señalar que el SEPP que "realiza el reenvío" puede modificar el mensaje o incluso encapsularlo dentro de otro mensaje.

Cuando recibe el mensaje del SEPP1, el SEPP2 descifra las partes cifradas de del mensaje y comprueba la integridad de las partes protegidas en integridad del mensaje. El SEPP2 puede utilizar la política de protección recibida del SEPP1 o consultar la NRF1 y/o la NRF2 según sea necesario para obtener la información de la política de protección.

El SEPP2 reenvía el mensaje a la NF2.

En la variante 2, por el contrario, la NF que envía el mensaje (NF1) incluye la política de protección en el mensaje. La NF puede haber recibido la política durante el descubrimiento del servicio (si es el consumidor del servicio) o durante el registro del servicio (si es el productor del servicio).

Más particularmente en este sentido, una función de red NF1 realiza el descubrimiento del servicio o el registro del servicio en la NRF1, la NRF en su PLMN. Como parte del descubrimiento o registro anterior, la NRF1 puede incluir políticas de protección de tipos de mensajes que la NF1 puede enviar mientras consume o produce el servicio. Para el caso de descubrimiento, la NRF1 puede haber recibido la política de protección de la NRF2.

Mientras consume o produce el servicio, la NF1 pretende enviar un mensaje a la NF2. El mensaje se enruta a través del SEPP1 y el SEPP2. En el mensaje, la NF1 incluye la política de protección que es aplicable para este mensaje. La NF1 puede haber recibido la política de la NRF1 o la NRF2, pero la política puede estar originada, alternativamente, en la propia NF1.

Antes de reenviar el mensaje al SEPP2, el SEPP1 realiza la protección del mensaje según la política recibida de la NF1. Para garantizar que el SEPP2 pueda recuperar el mensaje original, el SEPP1 puede incluir información que le permita al SEPP2 saber qué partes estaban protegidas. Esto lo puede solucionar, por ejemplo, el SEPP1 incluyendo la política de protección en el mensaje que reenvía. De nuevo, cabe señalar que el SEPP que "realiza el reenvío" podría modificar el mensaje o incluso encapsularlo dentro de otro mensaje.

Cuando recibe el mensaje del SEPP1, el SEPP2 descifra las partes cifradas del mensaje y comprueba la integridad de las partes del mensaje protegidas en integridad. Por ejemplo, el SEPP2 puede utilizar una política de protección recibida del SEPP1.

El SEPP2 reenvía el mensaje a la NF2.

Una política de protección, tal como se explica en estos ejemplos, describe qué elementos de un mensaje se deben cifrar y qué elementos se deben proteger en integridad. La política puede describir explícitamente qué elementos deben ser protegidos (cifrados y/o protegidos en integridad), o puede describir explícitamente qué elementos no deben ser protegidos (no cifrados y/o no protegidos en integridad).

Una de las realizaciones potenciales de una política de protección se describe a continuación. Se puede definir una política de protección para todos los mensajes enviados y recibidos por una NF. Los mensajes pueden ser solicitudes de HTTP o respuestas de HTTP.

Una política de protección, en algunas realizaciones, comprende una o varias reglas de protección. Cada regla de protección consta de: (1) un tipo de mensaje al que se le puede aplicar la regla, que incluye, por ejemplo, una solicitud de HTTP, una respuesta de HTTP o ambas; (2) una entidad de mensaje a la que se le puede aplicar la regla, que puede ser, por ejemplo, el URI de solicitud, una pseudo cabecera de HTTP, una cabecera de HTTP o el cuerpo de HTTP; y (3) una operación de coincidencia y reemplazo. Dependiendo de la entidad del mensaje, la operación puede estar representada por una expresión regular, un puntero de JSON (RFC 6901) a un elemento en una estructura de JSON y su reemplazo, o cualquier otra expresión.

En algunas realizaciones, existirá una regla de protección dentro de la política de protección para cada iteración de cada mensaje que requiere ser protegido.

En una comunicación entre dos NF, se puede utilizar una sola política de protección en algunas realizaciones. Esta política de protección puede ser definida por la NF que proporciona el servicio (es decir, la NF llamada). La política de protección podrá ser aplicable a los mensajes enviados y recibidos por la NF. La política de protección de una NF puede ser almacenada en la NRF ubicada en la PLMN de la NF que proporciona el servicio.

Se puede utilizar una política de protección para la comunicación de NF con varias PLMN pero, también es posible definir políticas de protección individualmente para cada PLMN con la que interactúa la NF.

La política de protección para las NF en una PLMN determinada puede ser común a todos los consumidores de servicios de NF con los que interactúa la NF que proporciona el servicio.

Un SEPP, al cifrar un mensaje enviado a una NF, debe realizar iteraciones sobre las reglas de protección de la política de protección para esa NF. Para cada regla de política, si el tipo de mensaje de la regla coincide con el tipo de mensaje del mensaje, se aplicará la correspondiente operación de coincidencia y reemplazo sobre la entidad del mensaje determinado por la regla.

Un SEPP, cuando descifra un mensaje enviado a una NF, debe realizar iteraciones sobre las reglas de protección de la política de protección para esa NF. Para cada regla de política, si el tipo de mensaje de la regla coincide con el tipo de mensaje del mensaje, se aplicará la correspondiente operación de coincidencia y reemplazo sobre la entidad del mensaje determinada por la regla.

El proceso de cifrado y descifrado finaliza cuando todas las reglas de protección de la política de protección han sido evaluadas.

Dependiendo de la variante aplicable, la política de protección aplicable puede ser proporcionada al SEPP (por la FN o el SEPP en la otra PLMN) o consultada por la SEPP en la NRF.

En algunas realizaciones, la política de protección puede ser proporcionada localmente a la NF y en la NRF. Para este último caso, se podrá registrar una política de protección en la NRF para cada NF. Esto puede hacerlo la NF como parte de su proceso de registro en la NRF, o mediante un mecanismo diferente, tal como el aprovisionamiento de operación y mantenimiento (Operation & Maintenance, O&M). En ambos casos, el objetivo es evitar que el SEPP requiera una actualización cuando se implementan nuevas NF o cambios en la política de protección de las NF existentes.

En la figura 8 se muestra un ejemplo concreto para la variante 2. En este ejemplo, una función de red en la PLMN visitada (por ejemplo, una función de acceso y movilidad, AMF) necesita enviar una solicitud de HTTP a una función de red en la PLMN doméstica (por ejemplo, una función de gestión de datos unificados, UDM), para recuperar los datos de abonado de un usuario en particular. Los datos del abonado pueden ser una pequeña parte del perfil del abonado, tal como los datos necesarios para seleccionar un “fragmento” concreto de la red central 5G.

Con el fin de averiguar el URI de la UDM (que se encuentra en la PLMN de origen), la AMF consulta a la NRF local emitiendo un mensaje de solicitud de descubrimiento. El mensaje de solicitud de descubrimiento incluye criterios de búsqueda tales como el tipo de función de red requerida (UDM en este caso), o el servicio específico (“nudm-sdm”, en este caso). La NRF en la vPLMN, a su vez, reenvía la solicitud de descubrimiento a la NRF en la hPLMN y, como resultado, se devuelve a la vAMF una lista de funciones de red de UDM disponibles (puntos finales de URI) en la hPLMN.

Como parte de los perfiles devueltos de las instancias de UDM disponibles, la información del perfil incluye parámetros que indican las diferentes URI disponibles en cada servicio. La información del perfil también incluye una política de protección 80 que incluye información sobre dónde en estos URI hay información confidencial que necesita ser protegida. Considérese un ejemplo:

Vaya a http://www.homeoperator.com/nudm-sdm/v1/{SUPI}/nssai

En este caso, una AMF puede utilizar este URI cuando necesita recuperar la información de asistencia a la selección de fragmentos de la red (Network Slice Selection Assistance Information, NSSAI) de un usuario determinado almacenada en la UDM en su red doméstica. En la sintaxis anterior, el componente {SUPI} representa una variable a sustituir por la identidad real del usuario, tal como, por ejemplo:

Vaya a http://www.homeoperator.com/nudm-sdm/v1/imsi-214050123456789/nssai

La solicitud de HTTP se enruta desde la AMF al SEPP en la red visitada (vSEPP), y la AMF incluye la política de protección 80 en una cabecera de HTTP específica, incluida la información recibida de la NRF sobre las partes del URI que deben ser protegidas, debido a que contienen información confidencial.

El vSEPP recibe el mensaje de HTTP. El vSEPP determina el SEPP en la hPLMN (hSEPP) a donde se debe enviar esta información, y comprueba el acuerdo de itinerancia correspondiente para averiguar las claves de cifrado adecuadas que se utilizarán para proteger los mensajes entre los SEPP. El vSEPP también extrae la cabecera de HTTP específica enviada por la AMF y procesa el URI en consecuencia, por lo que las partes confidenciales del URI se pueden cifrar utilizando las claves encontradas. La cabecera de HTTP puede indicar, por ejemplo, la siguiente expresión regular (del ejemplo de URL anterior): “^/udm-sdm/v1/([^/?#]+)/nssai$”. Esto permite encontrar una coincidencia completa, donde el primer grupo interno: “([^/?#]+)” es el conjunto de caracteres donde se espera encontrar el valor del {supi}.

El hSEPP recibe el mensaje de HTTP y realiza la operación inversa. Determina la PLMN que está enviando el mensaje, para comprobar los acuerdos de itinerancia aplicables y determinar las claves de cifrado correctas. A continuación, comprueba la cabecera de HTTP específica y determina las partes del URI que están sujetas a protección (cifradas), y las descifra, y loas reemplaza por la versión sin cifrar. El hSEPP también elimina la cabecera de HTTP que indicaba las partes del URI que fueron cifradas.

A continuación, el hSEPP reenvía el mensaje de HTTP a la instancia de UDM en la HPLMN. Este mensaje es idéntico al mensaje originado por la vAMF y, por lo tanto, el cifrado/descifrado realizado entre varios SEPP, de ciertos componentes de URI es transparente para la comunicación vAMF -> hUDM.

Aunque las realizaciones se han ejemplificado en un contexto para transmitir un mensaje 60 entre dominios de red central que toman la forma de redes centrales en diferentes PLMN, las realizaciones en el presente documento son extensibles a cualquier tipo de dominios de red central. En realidad, en algunas realizaciones, los dominios de la red central son dominios diferentes dentro de la misma red central.

Cabe señalar, además, que las realizaciones del presente documento pueden utilizar cualquiera de uno o varios protocolos de comunicación conocidos en la técnica o que pueden ser desarrollados, como IEEE 802.xx, Acceso múltiple por división de código (Code Division Multiple Access, CDMA), CDMA de banda ancha (Wideband CDMA, WCDMA), sistema global para telecomunicaciones móviles (Global System for Mobile telecommunications, GSM), evolución a largo plazo (Long Term Evolution, LTE), WiMax, nueva radio (New Radio, NR) o similares. En consecuencia, aunque a veces se describen en el presente documento en el contexto de 5G, los principios y conceptos explicados en el presente documento son aplicables a sistemas 4G y otros.

Un dispositivo inalámbrico tal como el utilizado en el presente documento es cualquier tipo de dispositivo capaz de comunicarse con otro nodo de radio de manera inalámbrica por medio de señales de radio. Por lo tanto, un dispositivo inalámbrico puede referirse a un equipo de usuario (UE), una estación móvil, un ordenador portátil, un teléfono inteligente, un dispositivo de máquina a máquina (Machine to Machine, M2M), un dispositivo de comunicaciones de tipo máquina (Machine Type Communications, MTC), un dispositivo de internet de las cosas (IoT) de banda estrecha, etc. Es decir, aunque el dispositivo inalámbrico se puede denominar UE, se debe tener en cuenta que el dispositivo inalámbrico no tiene necesariamente un “usuario” en el sentido de una persona individual que posee y/u opera el dispositivo. Un dispositivo inalámbrico también se puede denominar dispositivo de comunicación inalámbrica, dispositivo de radio, dispositivo de comunicación por radio, terminal inalámbrico o simplemente terminal - a menos que el contexto indique otra cosa, la utilización de cualquiera de estos términos tiene la intención de incluir los UE o dispositivos de dispositivo a dispositivo, dispositivos de tipo máquina o dispositivos con capacidad de comunicación de máquina a máquina, sensores equipados con un dispositivo inalámbrico, ordenadores de sobremesa habilitados para conexión inalámbrica, terminales móviles, teléfonos inteligentes, equipos integrados en ordenadores portátiles (Laptop - Embedded Equipment, LEE), equipos montados en ordenadores portátiles (Laptop - Mounted Equipment, LME), dongles de USB, dispositivos inalámbricos en las instalaciones del cliente (Customer - Premises Equipment, CPE), etc. En la explicación del presente documento, también se pueden utilizar los términos dispositivo de máquina a máquina (M2M), dispositivo de comunicación de tipo máquina (MTC), sensor inalámbrico y sensor. Se debe comprender que estos dispositivos pueden ser los UE pero, en general, pueden ser configurados para transmitir y/o

recibir datos sin interacción humana directa.

En un planteamiento de IoT, un dispositivo inalámbrico tal como el descrito en el presente documento puede estar, o estar comprendido en una máquina o dispositivo que realiza monitorización o mediciones, y transmite los resultados de dichas mediciones de monitorización a otro dispositivo o a una red. Ejemplos particulares de dichas máquinas son medidores de potencia, maquinaria industrial o electrodomésticos para el hogar o electrodomésticos personales, por ejemplo, refrigeradores, televisores, accesorios ponibles personales, tales como relojes, etc. En otros planteamientos, un dispositivo de comunicación inalámbrica tal como el descrito en el presente documento puede estar comprendido en un vehículo y puede monitorizar y/o informar sobre el estado operativo del vehículo u otras funciones asociadas con el vehículo.

Tal como se utiliza en el presente documento, “equipo de red” se refiere a un equipo con capacidad, configurado, dispuesto y/u operable para comunicarse directa o indirectamente con un dispositivo inalámbrico y/o con otro equipo en la red de comunicación inalámbrica que permite y/o proporciona acceso inalámbrico al dispositivo inalámbrico. Ejemplos de equipos de red incluyen, pero no están limitados a, equipos de red central en una red central (por ejemplo, equipos que implementan una AMF o SMF).

Cabe señalar que el equipo de red tal como se ha descrito anteriormente puede realizar cualquiera de los procesamientos del presente documento implementando cualquier medio o unidad funcional. En una realización, por ejemplo, el equipo de red comprende circuitos respectivos o circuitería configurada para realizar las etapas que se muestran en la figura 5. Los circuitos o la circuitería, a este respecto pueden comprender circuitos específicos para realizar cierto procesamiento funcional y/o uno o varios microprocesadores junto con la memoria. En realizaciones que emplean memoria, que puede comprender uno o varios tipos de memoria, tal como una memoria de solo lectura (Read Only Memory, ROM), una memoria de acceso aleatorio, una memoria caché, dispositivos de memoria flash, dispositivos de almacenamiento óptico, etc., la memoria almacena código de programa que, cuando es ejecutado por uno o varios procesadores, lleva a cabo las técnicas descritas en el presente documento.

La figura 9A muestra el equipo de red 300, según una o varias realizaciones. Tal como se muestra, el equipo de red 300 incluye circuitería de procesamiento 310 y circuitería de comunicación 320. La circuitería de comunicación 320 está configurada para transmitir y/o recibir información hacia y/o desde uno o varios nodos, por ejemplo, por medio de cualquier tecnología de comunicación. La circuitería de procesamiento 310 está configurada para realizar el procesamiento descrito anteriormente, por ejemplo, en la figura 5, tal como ejecutar instrucciones almacenadas en la memoria 330. La circuitería de procesamiento 310, en este sentido, puede implementar ciertos medios, unidades o módulos funcionales.

La figura 9B muestra el equipo de red 400 según una o varias de otras realizaciones. Tal como se muestra, el equipo de red 400 implementa diversos medios, unidades o módulos funcionales, por ejemplo, mediante la circuitería de procesamiento 410 en la figura 9A y/o mediante código de software. Estos medios, unidades o módulos funcionales, por ejemplo, para implementar el procedimiento de la figura 5, incluyen, por ejemplo, una unidad o módulo de recepción 410, para recibir un mensaje 60 que ha sido, o será, transmitido entre los diferentes dominios de la red central, y para recibir una política de protección 80 que incluye información que indica a cuál o cuáles de la una o varias partes del mensaje 60 (por ejemplo, una o varias partes del contenido de un campo 62 en el mensaje 60) se va a aplicar o eliminar la protección de seguridad entre dominios 70. También se puede incluir una unidad de protección o módulo 420 para aplicar protección de seguridad entre dominios o eliminar la protección de seguridad entre dominios de la una o varias partes, según la política de protección 80. Además, una unidad o módulo de reenvío 430 puede estar incluida en algunas realizaciones, para reenviar el mensaje 60, con protección de seguridad entre dominios aplicada o eliminada a la una o varias partes, hacia un destino del mensaje 60.

Cabe señalar, asimismo que el otro equipo de red tal como el descrito anteriormente puede realizar cualquiera de los procesamientos descritos en el presente documento mediante la implementación de cualquier medio o unidad funcional. En una realización, por ejemplo, el equipo de red comprende circuitos respectivos o circuitería configurados para realizar las etapas que se muestran en la figura 6. Los circuitos o circuitería a este respecto pueden comprender circuitos específicos para realizar cierto procesamiento funcional y/o uno o varios microprocesadores junto con la memoria. En realizaciones que emplean una memoria, que puede comprender uno o varios tipos de memoria, tal 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 varios procesadores, lleva a cabo las técnicas descritas en el presente documento.

La figura 10A muestra el equipo de red 500, según una o varias realizaciones. Tal como se muestra, el equipo de red 500 incluye circuitería de procesamiento 510 y circuitería de comunicación 520. La circuitería de comunicación 520 está configurada para transmitir y/o recibir información hacia y/o desde uno o varios nodos, por ejemplo, a través de cualquier tecnología de comunicación. La circuitería de procesamiento 510 está configurada para realizar el procesamiento descrito anteriormente, por ejemplo, en la figura 6, tal como por ejemplo mediante la ejecución de instrucciones almacenadas en la memoria 530. La circuitería de procesamiento 510 en este sentido puede implementar ciertos medios, unidades o módulos funcionales.

La figura 10B muestra el equipo de red 600, según una o varias realizaciones. Tal como se muestra, el equipo de red 600 implementa diversos medios funcionales, unidades o módulos, por ejemplo, mediante la circuitería de procesamiento 610 en la figura 10A y/o mediante código de software. Estos medios, unidades o módulos funcionales, por ejemplo, para implementar el procedimiento de la figura 6, incluyen, por ejemplo, una unidad o módulo de obtención 410, para obtener una política de protección 80 que incluye información que indica a cuál o cuáles de la una o varias partes del mensaje 60 (por ejemplo, una o varias partes del contenido de un campo 62 en el mensaje 60) se va a aplicar o eliminar la protección de seguridad entre dominios 70. Además puede estar incluida una unidad o módulo de transmisión 420 para transmitir la política de protección 80.

Los expertos en la materia también apreciarán que las realizaciones en este documento incluyen, además, programas informáticos correspondientes.

Un programa informático comprende instrucciones que, cuando son ejecutadas en al menos un procesador de un equipo de red, hacen que el equipo de red realice cualquiera de los procesamientos respectivos descritos anteriormente. En este sentido, un programa informático puede comprender uno o varios módulos de código correspondientes a los medios o unidades descritos anteriormente.

Las realizaciones incluyen, además, una portadora que contiene dicho programa informático. Esta portadora comprender una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por un ordenador.

A este respecto, las realizaciones en el presente documento también incluyen un medio de almacenamiento (almacenamiento o grabación) no transitorio legible por un ordenador que tiene almacenadas en el mismo instrucciones que, cuando son ejecutadas por un procesador de un equipo de red, hacen que el equipo de red funcione tal como se ha descrito anteriormente.

REIVINDICACIONES

1. Un procedimiento realizado por el equipo de red (300, 400) en uno de los múltiples dominios diferentes de la red central de un sistema de comunicación inalámbrica (10), comprendiendo el procedimiento:

recibir (110) un mensaje (60) que ha sido, o será, transmitido entre los diferentes dominios de la red central;

aplicar (130) la protección de seguridad entre dominios o eliminar la protección de seguridad entre dominios de una o varias partes de un contenido de un campo en el mensaje (60), según una política de protección (80) que incluye información que indica a cuál o cuáles de la una o varias partes del contenido del campo se va a aplicar o eliminar la protección de seguridad entre dominios,

en donde la información incluye uno o varios punteros de notación de objetos de JavaScript, JSON, que indican la una o varias partes del contenido del campo al que se aplicará o eliminará la protección de seguridad entre dominios; y

reenviar (140) el mensaje (60), con protección de seguridad entre dominios aplicada o eliminada a la una o varias partes, hacia un destino del mensaje (60).

2. El procedimiento de la reivindicación 1, en el que el mensaje (60) es un mensaje del protocolo de transferencia de hipertexto (HTTP) y el campo es un campo de HTTP.

3. El procedimiento de la reivindicación 2, en el que el mensaje HTTP (60) es un mensaje de solicitud de HTTP y el campo es un campo de ruta, y en el que el contenido del campo de ruta es una solicitud de identificador uniforme de recursos, URI.

4. El procedimiento de cualquiera de las reivindicaciones 1 a 3, en el que la información incluye una o varias expresiones regulares que indican la una o varias partes.

5. El procedimiento de cualquiera de las reivindicaciones 1 a 4, en el que la política de protección (80) indica, además, para cada una de la una o varias partes, un tipo de protección de seguridad entre dominios que se aplicará o eliminará, y en el que, para cada una de la una o varias partes, el tipo de protección de seguridad entre dominios que se aplicará o eliminará comprende protección de confidencialidad y/o protección de integridad.

6. El procedimiento de cualquiera de las reivindicaciones 1 a 5, que comprende, además, en respuesta a la recepción del mensaje (60), transmitir una solicitud de descubrimiento a una función de depósito de red, NRF, solicitando el descubrimiento de la política de protección (80) para proteger el mensaje (60), y recibir la política de protección (80) en respuesta a la solicitud de descubrimiento.

7. El procedimiento de cualquiera de las reivindicaciones 1 a 6, en el que el procedimiento está realizado por un servidor proxy de protección de borde de seguridad, SEPP.

8. El procedimiento de la reivindicación 7, en el que SEPP comprende el SEPP en una red visitada, vSEPP, y el SEPP en una red doméstica, hSEPP.

9. Un equipo de red (300, 400), configurado para ser utilizado en uno de múltiples dominios diferentes de la red central de un sistema de comunicación inalámbrica (10), en el que el equipo de red (300, 400) comprende:

circuitería de comunicación (320); y

circuitería de procesamiento (310), configuradas para:

recibir, a través de la circuitería de comunicación (320), un mensaje (60) que se ha transmitido o se transmitirá entre los diferentes dominios de la red central;

aplicar protección de seguridad entre dominios o eliminar la protección de seguridad entre dominios de una o varias partes de un contenido de un campo en el mensaje (60), según una política de protección (80) que incluye información que indica a cuál o cuáles de la una o varias partes del contenido del campo se va a aplicar o eliminar la protección de seguridad entre dominios, en donde la información incluye uno o varios punteros de notación de objetos de JavaScript, JSON, que indican la una o varias partes del contenido a las que se aplicará o eliminará la protección de seguridad entre dominios; y

reenviar el mensaje (60), con protección de seguridad entre dominios aplicada o eliminada a la una o varias partes, hacia un destino del mensaje (60) por medio de la circuitería de comunicación (320).

10. El equipo de red de la reivindicación 9, en el que el mensaje (60) es un mensaje de protocolo de transferencia de hipertexto (HTTP) y el campo es un campo de HTTP.

11. El equipo de red de la reivindicación 10, en el que el mensaje de HTTP (60) es un mensaje de solicitud de HTTP y el campo es un campo de ruta, y en el que el contenido del campo de ruta es una solicitud de identificador uniforme de recursos, URI.

12. El equipo de red de cualquiera de las reivindicaciones 9 a 11, en el que la información incluye una o varias expresiones regulares que indican la una o más partes.

13. El equipo de red de cualquiera de las reivindicaciones 9 a 12, en el que la política de protección (80) indica, además, para cada una de la una o varias partes, un tipo de protección de seguridad entre dominios que se aplicará o eliminará, y en el que, para cada una de la una o varias partes, el tipo de protección de seguridad entre dominios a aplicar o eliminar comprende protección de confidencialidad y/o protección de integridad.

14. El equipo de red de cualquiera de las reivindicaciones 9 a 13, en el que la circuitería de procesamiento (310) está configurada además para, en respuesta a recibir el mensaje (60), transmitir una solicitud de descubrimiento a una función de depósito de red, NRF, solicitar el descubrimiento de la política de protección (80) para proteger el mensaje (60) y recibir la política de protección (80) en respuesta a la solicitud de descubrimiento.

15. El equipo de red según cualquiera de las reivindicaciones 9 a 14, en el que el equipo de red está configurado como un servidor proxy de protección de borde de seguridad, SEPP.

16. El equipo de red de la reivindicación 15, en el que SEPP comprende SEPP en una red visitada, vSEPP, y SEPP en una red doméstica, hSEPP.

17. Un programa informático, que comprende instrucciones que, cuando son ejecutadas por al menos un procesador del equipo de red (300, 400) en uno de múltiples dominios diferentes de la red central de un sistema de comunicación inalámbrica, hacen que el equipo de red (300, 400) realice el procedimiento de cualquiera de las reivindicaciones 1 a 8.

18. Una portadora, que contiene el programa informático de la reivindicación 17, en donde la portadora es una de una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por un ordenador.

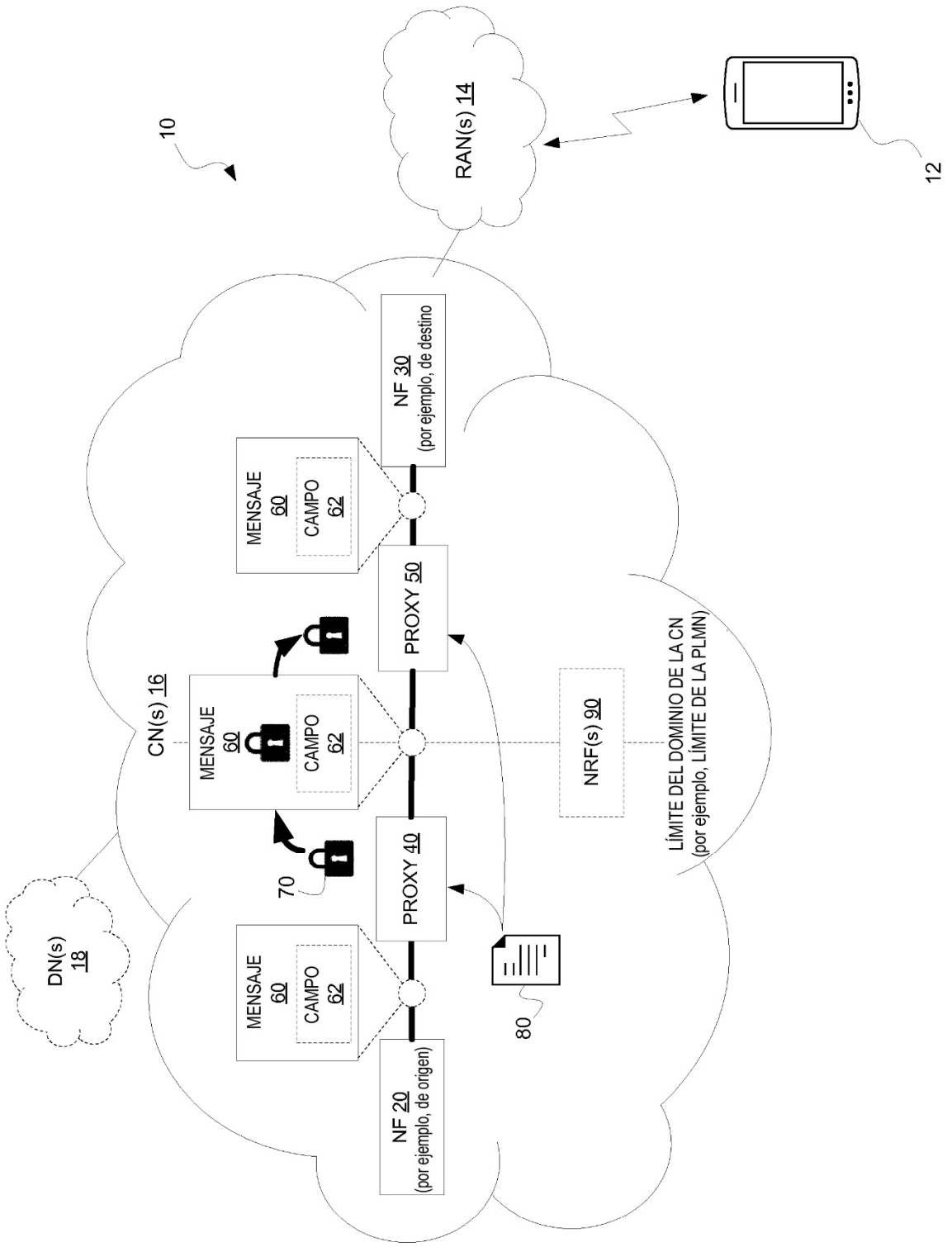
10
RAN(s) 14
12
NF 30
(por ejemplo, de destino
MENSAJE 60
CAMPO 62
PROXY 50
CN(s) 16
MENSAJE 60
CAMPO 62
NRF(s) 90
LÍMITE DEL DOMINIO DE LA CN
(por ejemplo, LÍMITE DE LA PLMN)
70
DN(s) 18
MENSAJE 60
CAMPO 62
PROXY 40
80
NF 20
(por ejemplo, de origen)

FIG. 1

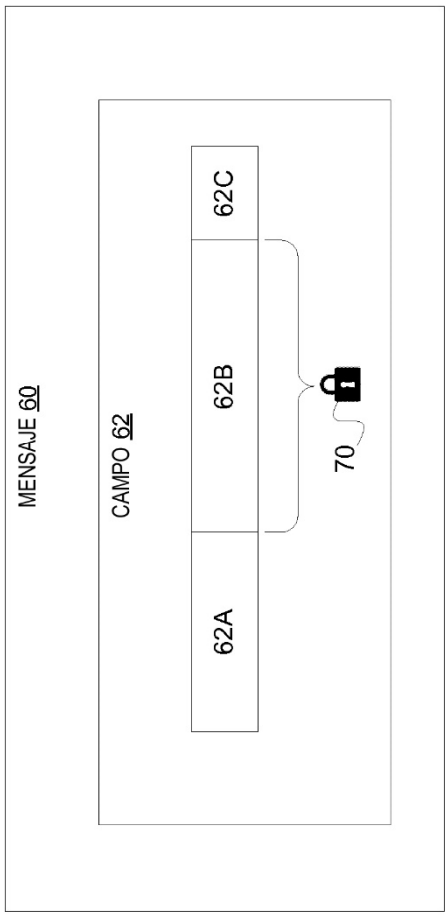
MENSAJE 60
CAMPO 62
62A
62B
62C
70

FIG. 2A

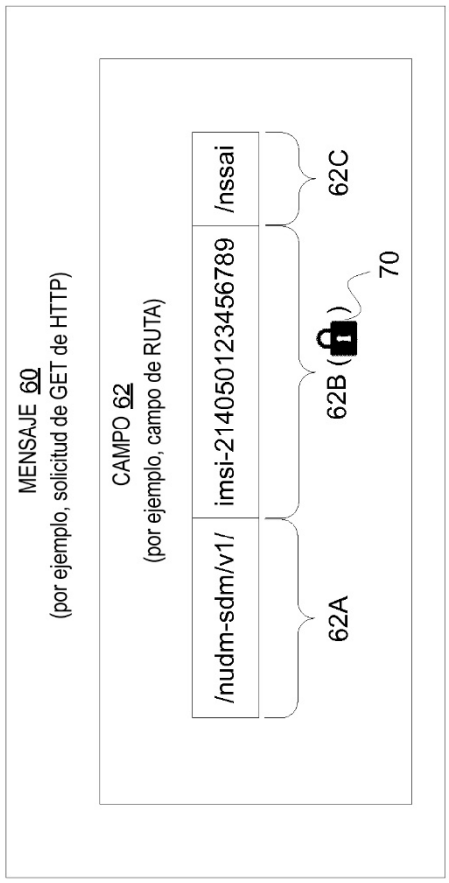
MENSAJE 60
(por ejemplo, solicitud de GET de HTTP)
CAMPO 62
(por ejemplo, campo de RUTA)
/nudm-sdm/v1/
imsi-214050123456789
/nssai
62A
62B
62C
70

FIG. 2B

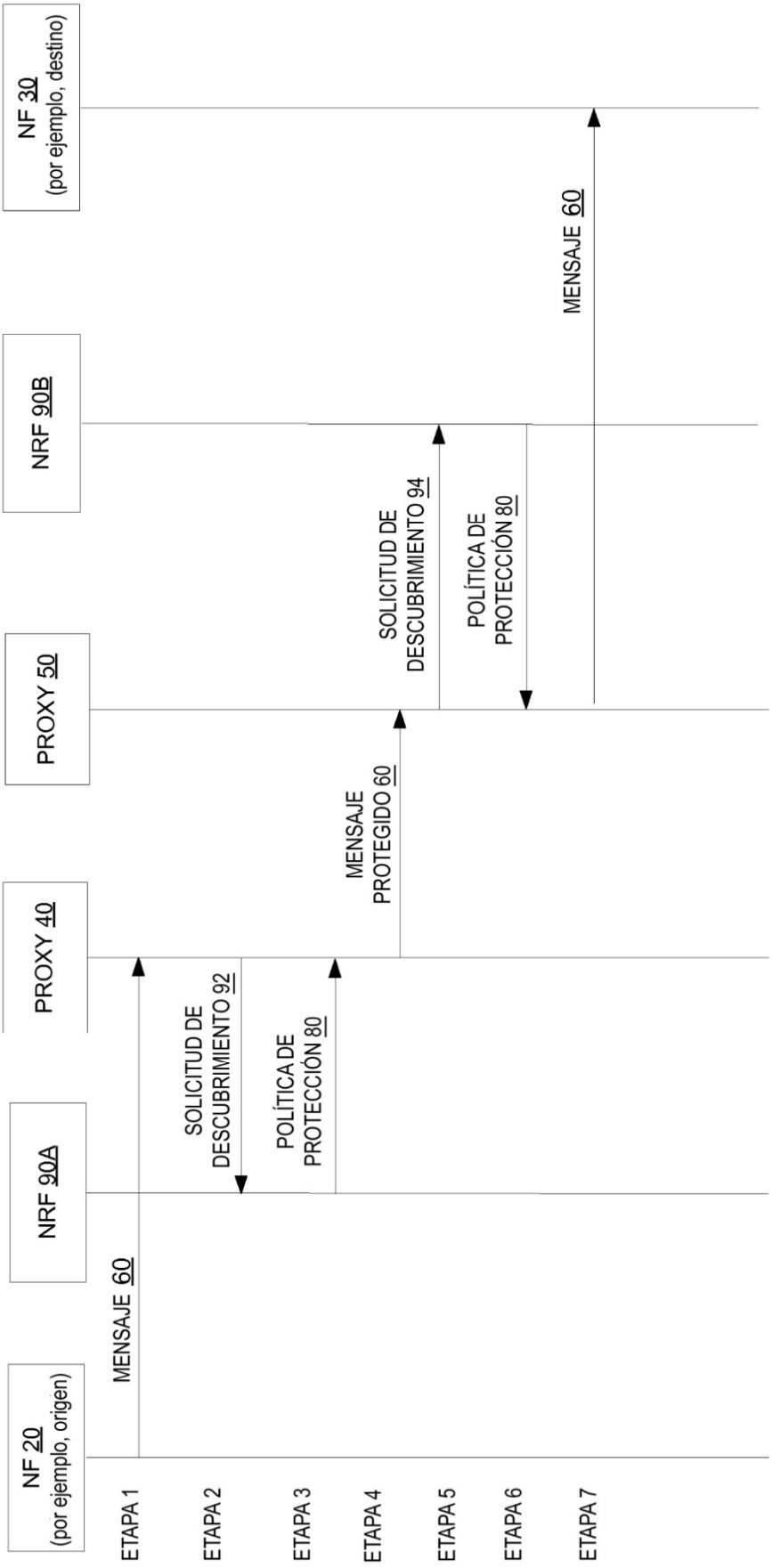
NF 20
(por ejemplo, origen)
NRF 90A
PROXY 40
PROXY 50
NRF 90B
NF 30
(por ejemplo, destino)
MENSAJE 60
SOLICITUD DE DESCUBRIMIENTO 92
POLÍTICA DE PROTECCIÓN 80
MENSAJE PROTEGIDO 60
SOLICITUD DE DESCUBRIMIENTO 94
POLÍTICA DE PROTECCIÓN 80
MENSAJE 60
ETAPA 1
ETAPA 2
ETAPA 3
ETAPA 4
ETAPA 5
ETAPA 6
ETAPA 7

FIG. 3

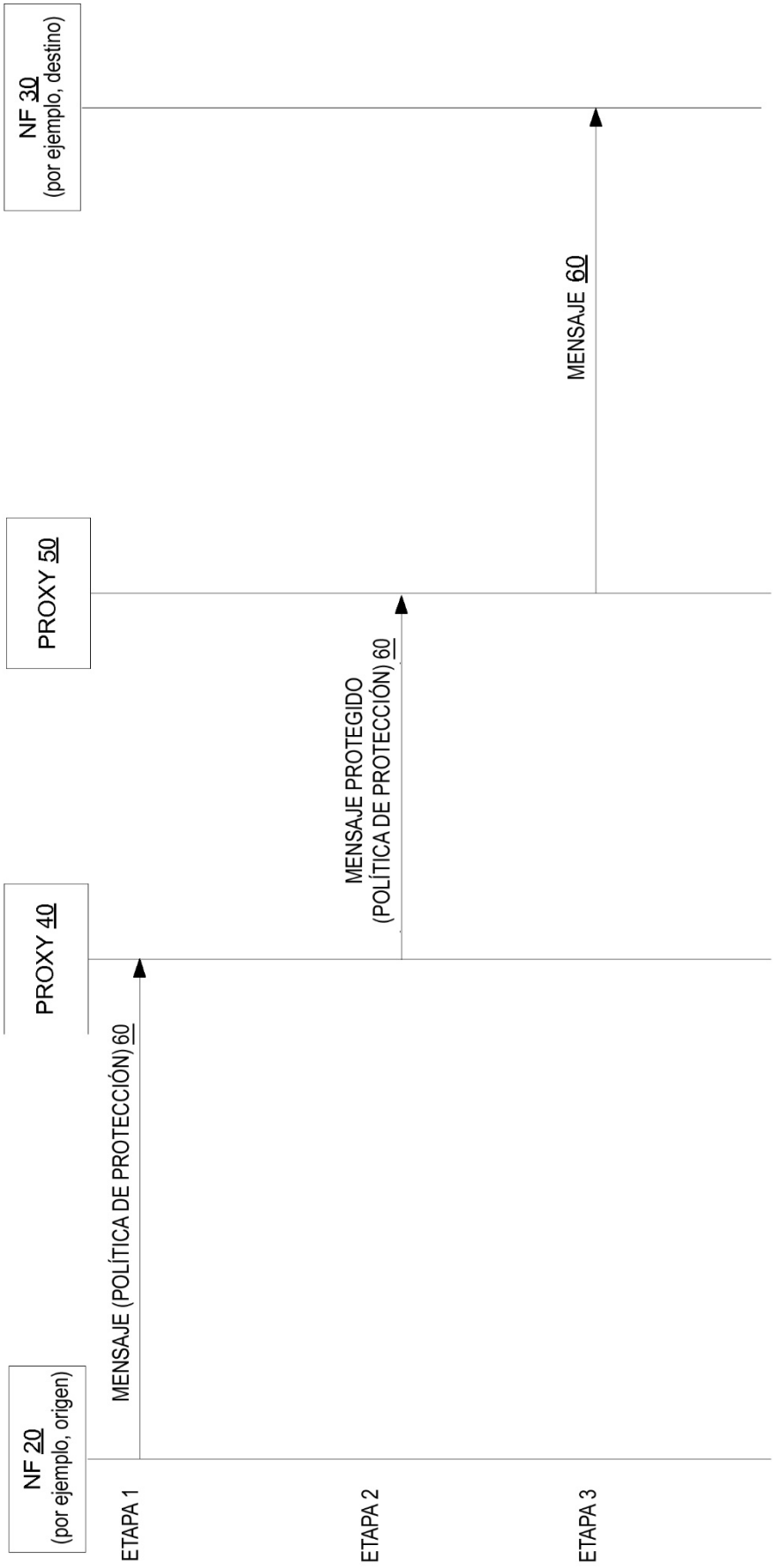
NF 20
(por ejemplo, origen)
PROXY 40
PROXY 50
NF 30
(por ejemplo, destino)
MENSAJE (POLÍTICA DE PROTECCIÓN) 60
MENSAJE PROTEGIDO
(POLÍTICA DE PROTECCIÓN) 60
MENSAJE 60
ETAPA 1
ETAPA 2
ETAPA 3

FIG. 4

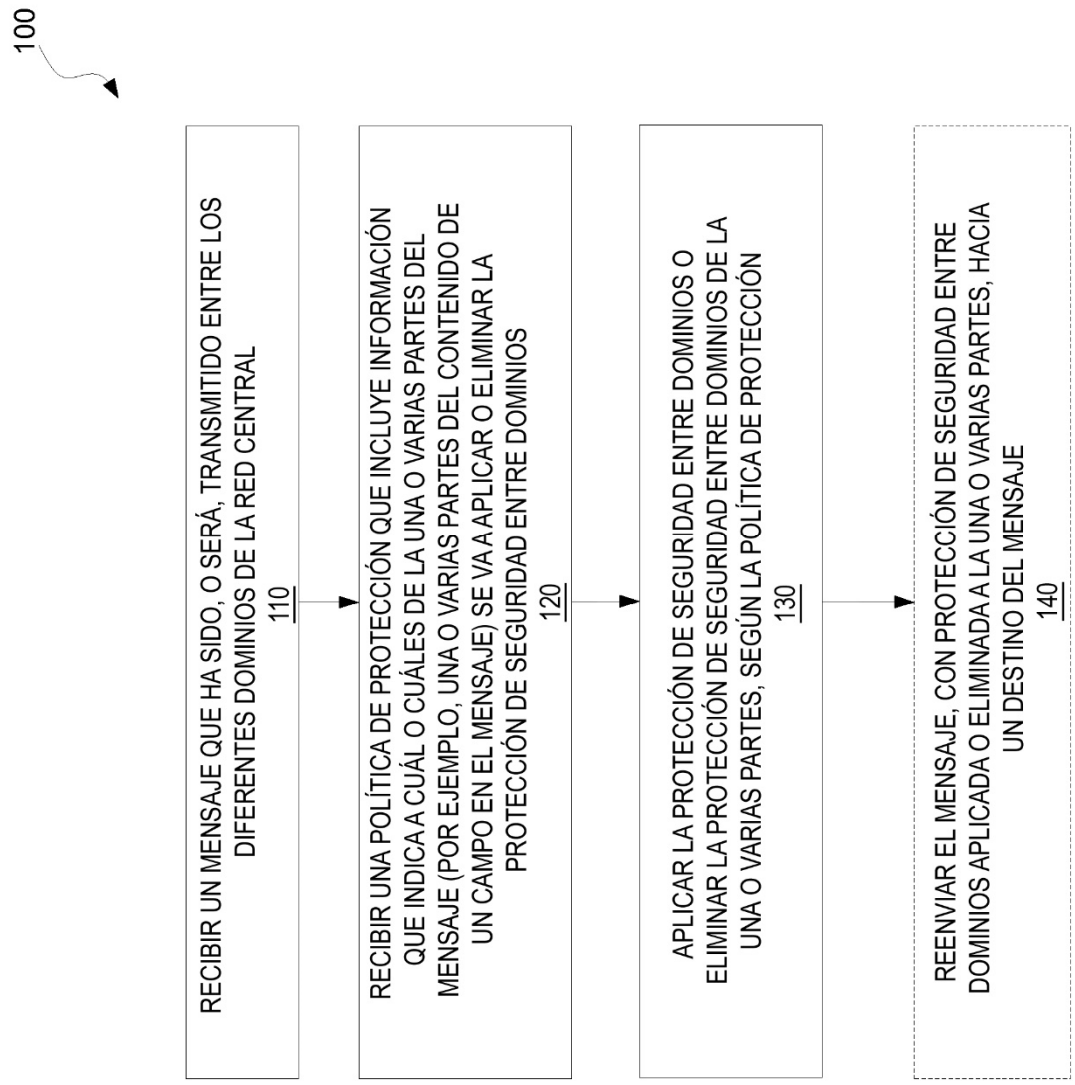
100
RECIBIR UN MENSAJE QUE HA SIDO, O SERÁ, TRANSMITIDO ENTRE LOS DIFERENTES DOMINIOS DE LA RED CENTRAL
110
RECIBIR UNA POLÍTICA DE PROTECCIÓN QUE INCLUYE INFORMACIÓN QUE INDICA A CUÁL O CUÁLES DE LA UNA O VARIAS PARTES DEL MENSAJE (POR EJEMPLO, UNA O VARIAS PARTES DEL CONTENIDO DE UN CAMPO EN EL MENSAJE) SE VA A APLICAR O ELIMINAR LA PROTECCIÓN DE SEGURIDAD ENTRE DOMINIOS
120
APLICAR LA PROTECCIÓN DE SEGURIDAD ENTRE DOMINIOS O ELIMINAR LA PROTECCIÓN DE SEGURIDAD ENTRE DOMINIOS DE LA UNA O VARIAS PARTES, SEGÚN LA POLÍTICA DE PROTECCIÓN
130
REENVIAR EL MENSAJE, CON PROTECCIÓN DE SEGURIDAD ENTRE DOMINIOS APLICADA O ELIMINADA A LA UNA O VARIAS PARTES, HACIA UN DESTINO DEL MENSAJE
140

FIG. 5

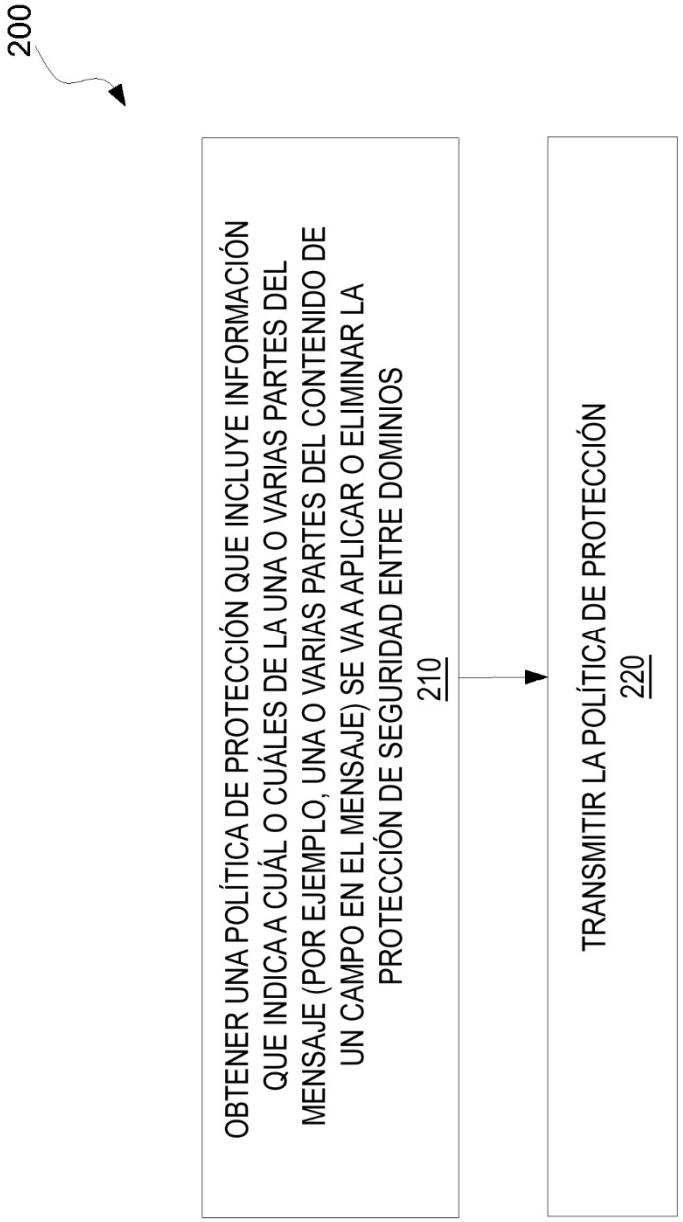
200
OBTENER UNA POLÍTICA DE PROTECCIÓN QUE INCLUYE INFORMACIÓN QUE INDICA A CUÁL O CUÁLES DE LA UNA O VARIAS PARTES DEL MENSAJE (POR EJEMPLO, UNA O VARIAS PARTES DEL CONTENIDO DE UN CAMPO EN EL MENSAJE) SE VA A APLICAR O ELIMINAR LA PROTECCIÓN DE SEGURIDAD ENTRE DOMINIOS
210
TRANSMITIR LA POLÍTICA DE PROTECCIÓN
220

FIG. 6

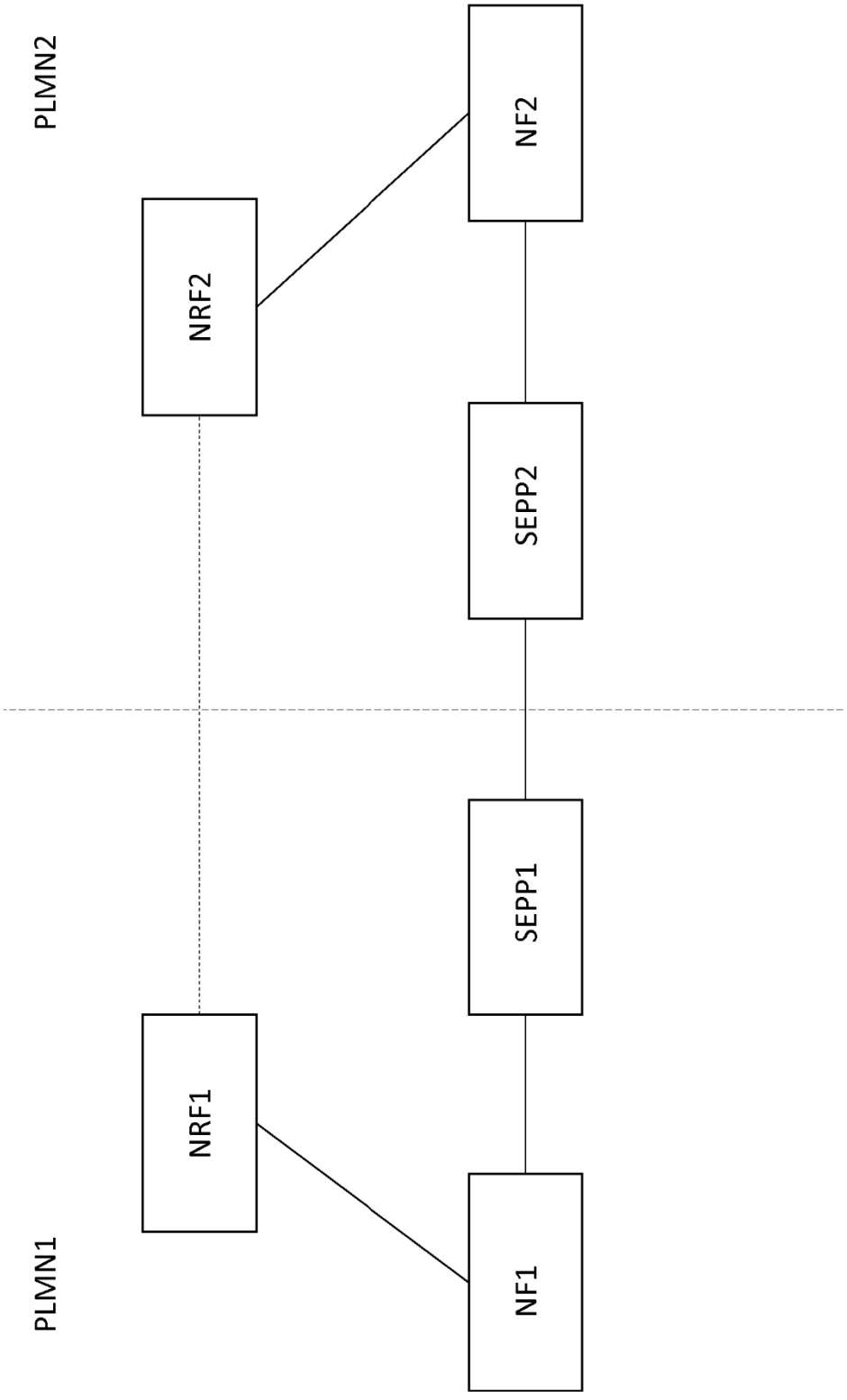

FIG. 7

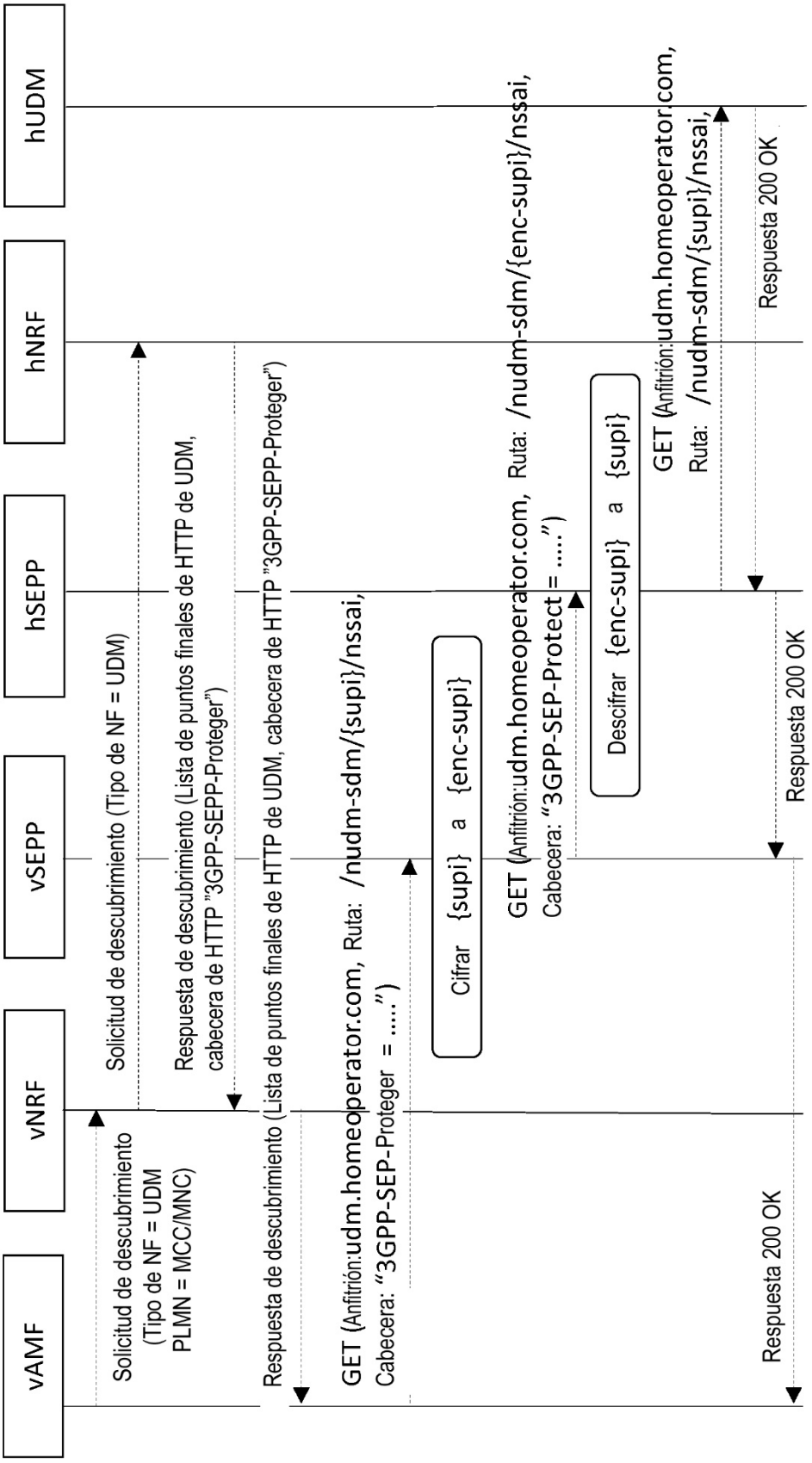
vAMF
vNRF
vSEPP
hSEPP
hNRF
hUDM
Solicitud de descubrimiento (Tipo de NF = UDM)
Solicitud de descubrimiento (Tipo de NF = UDM PLMN = MCC/MNC)
Respuesta de descubrimiento (Lista de puntos finales de HTTP de UDM, cabecera de HTTP "3GPP-SEPP-Proteger")
Respuesta de descubrimiento (Lista de puntos finales de HTTP de UDM, cabecera de HTTP "3GPP-SEPP-Proteger")
GET (Anfitrión:udm.homeoperator.com, Ruta: /nudm-sdm/{supi}/nssai, Cabecera: "3GPP-SEP-Proteger = ...")
Cifrar {supi} a {enc-supi}
GET (Anfitrión:udm.homeoperator.com, Ruta: /nudm-sdm/{enc-supi}/nssai, Cabecera: "3GPP-SEP-Protect = ...")
Descifrar {enc-supi} a {supi}
GET (Anfitrión:udm.homeoperator.com, Ruta: /nudm-sdm/{supi}/nssai,
Respuesta 200 OK
Respuesta 200 OK
Respuesta 200 OK

FIG. 8

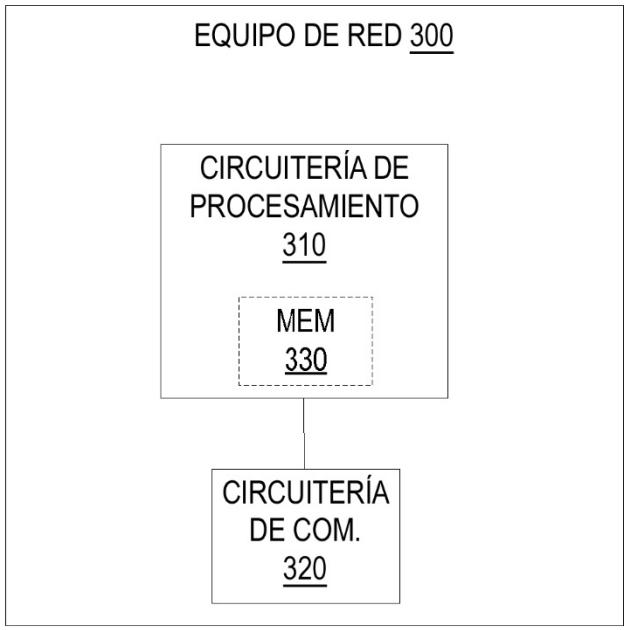

FIGURA 9A

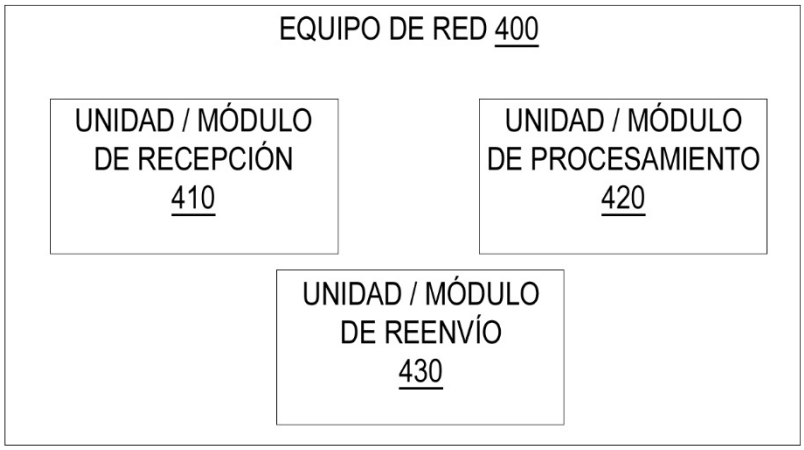

FIGURA 9B

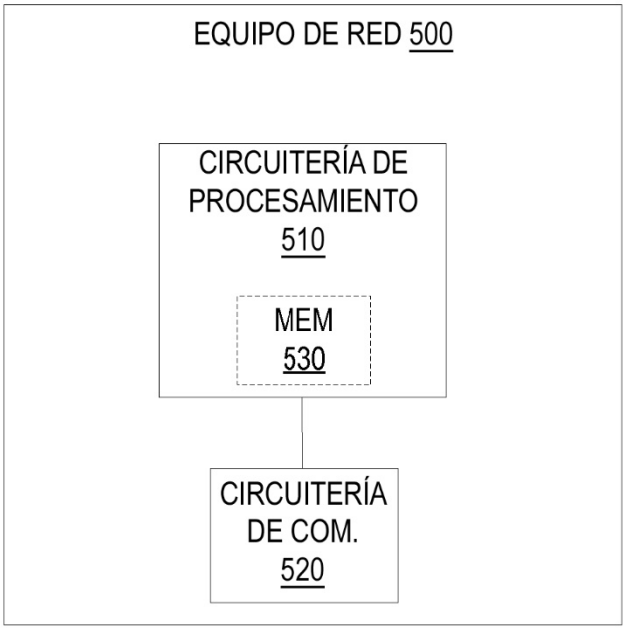

FIGURA 10A

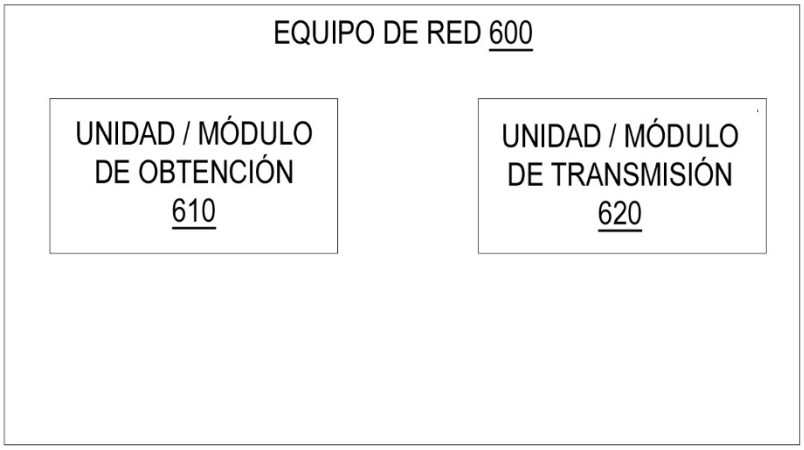

FIGURA 10B