

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 34193

Ref. Expediente N° NC2021/0000912

Por la cual se otorga una Patente de Invención

LA SUPERINTENDENTE DE INDUSTRIA Y COMERCIO
en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 24 del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO

Que mediante escrito radicado en esta Superintendencia el 28 de enero de 2021 con el N° NC2021/0000912, por NOKIA SOLUTIONS AND NETWORKS OY, entró a fase nacional la solicitud de patente de invención titulada “MANEJO DE FALLOS DE ACCESO NO 3GPP A UNA 5GCN NO PERMITIDO”, que corresponde a la solicitud internacional PCT/US2019/039992 del 28 de junio de 2019.

Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 924 el 19 de abril de 2021, sin que se hubieran presentado oposiciones por parte de terceros.

Que realizado el examen de fondo mediante Oficio No. 19504 del 30 de noviembre de 2023, se requirió al solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

Que el solicitante mediante escrito radicado bajo el N° NC2021/0000912 el 21 de febrero de 2024, respondió oportunamente el requerimiento formulado y presentó las reivindicaciones 1 a 21 que reemplazan las originalmente presentadas. Adicionalmente y de manera simultánea, mediante escrito radicado bajo el N° NC2024/0001870 el 21 de febrero de 2024, el solicitante presentó las reivindicaciones 1 a 21 para que sean tenidas en cuenta al momento de realizar el examen definitivo de la solicitud. Se acepta este último capítulo reivindicatorio presentado, comoquiera que se ajusta a las prescripciones contenidas en el artículo 34 de la Decisión 486.

Que en virtud de lo dispuesto en el artículo 14 de la Decisión 486 expedida por la Comisión de la Comunidad Andina *“Los países miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial.”*

Que en el presente caso dichas reivindicaciones cumplen los requisitos indicados en el considerando anterior, toda vez que se refiere a un nodo de función de intertrabajo, una función de gestión de acceso y movilidad y un equipo de usuario para manejar fallas debido a que no se permite el acceso no 3GPP a 5GCN, que difiere de la información del estado de la técnica más cercano, el artículo *“Technical Specification Group Services and System Aspects; Procedures for the 5G System; Stage 2 (Release 15)”*¹, en que la invención incluye en una modalidad una indicación de que el establecimiento de conexiones seguras con la red central 5GCN sobre redes de acceso no confiables no 3GPP no está permitido por la red central 5GCN y la etapa de recibir desde el UE un mensaje de detención que finaliza la

¹ 3GPP. (2017). Group and System for the 5G System; Stage 2 (Release 15). 3GPP Draft. Recuperado desde: https://www.3gpp.org/ftp/Specs/archive/23_series/23.502/

Resolución N° 34193

Ref. Expediente N° NC2021/0000912

solicitud para establecer la conexión segura a la red central 5GCN a través de la red de acceso no confiable no 3GPP. Además, la invención incluye en otra modalidad la etapa de generar un mensaje de respuesta a la solicitud de autenticación y establecimiento de conexión segura recibida desde la función de interfuncionamiento N3IWF encapsulando en el mensaje de respuesta un valor de causa que indica que el acceso a la red central 5GCN no está permitido por la red central 5GCN que se establece a través de redes de acceso no confiables no 3GPP, donde dicho mensaje se genera en respuesta a que la verificación de autenticación y suscripción por parte de la función de autenticación y suscripción AUSF ha fallado.

Adicionalmente, estas diferencias no se encuentran sugeridas en el estado de la técnica y, como consecuencia de ello, se evidencia el efecto técnico de gestionar de manera adecuada fallos durante el establecimiento de la conexión segura para el acceso a una red central 5G a través de redes de acceso que no son 3GPP, disminuyendo así los riesgos de seguridad al momento de acceder a dicha red.

En consecuencia, las reivindicaciones 1 a 21 cumplen los requisitos de novedad, nivel inventivo y aplicación industrial establecidos en la normatividad citada en precedencia y esta Oficina encuentra procedente conceder para las mismas la patente solicitada.

Que de acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC2024/0001870 el 21 de febrero de 2024 y teniendo en cuenta el objeto concedido, se modifica el título de la invención el cual quedará de la siguiente manera: “NODO DE FUNCIÓN DE INTERTRABAJO, FUNCIÓN DE GESTIÓN DE ACCESO Y MOVILIDAD, Y EQUIPO DE USUARIO PARA MANEJAR FALLAS DEBIDO A QUE NO SE PERMITE EL ACCESO NO 3GPP A 5GCN”.

Con fundamento en las anteriores consideraciones, la Superintendente de Industria y Comercio,

RESUELVE

ARTÍCULO 1: Otorgar patente de invención a la solicitud que entró en fase nacional en virtud del Tratado de Cooperación en Materia de Patentes (PCT), para la creación titulada:

“NODO DE FUNCIÓN DE INTERTRABAJO, FUNCIÓN DE GESTIÓN DE ACCESO Y MOVILIDAD, Y EQUIPO DE USUARIO PARA MANEJAR FALLAS DEBIDO A QUE NO SE PERMITE EL ACCESO NO 3GPP A 5GCN”

Clasificación IPC: H04L 29/06, H04W 12/06, H04W 60/00, H04W 84/04, H04W 84/12.

Reivindicación(es): 1 a 21 incluidas en el radicado bajo el N° NC2024/0001870 el 21 de febrero de 2024, de acuerdo con el Anexo No. 1.

Titular(es): NOKIA SOLUTIONS AND NETWORKS OY.

Dirección(es): KARAKAARI 7, 02610 ESPOO, FINLANDIA.

Inventor(es): Jennifer LIU.

Prioridad(es) N°: 30/06/2018, US (ESTADOS UNIDOS DE AMÉRICA), 62/692,722.

Solicitud internacional N°: PCT/US2019/039992

Fecha: 28 de junio de 2019.

Resolución N° 34193

Ref. Expediente N° NC2021/0000912

Vigente desde: 28 de junio de 2019

Hasta: 28 de junio de 2039.

ARTÍCULO 2: El titular tendrá los derechos y las obligaciones establecidos en la Decisión 486 de la Comisión de la Comunidad Andina y en las demás disposiciones legales vigentes sobre propiedad industrial, precisando que para mantener vigente la patente se deberá cancelar la tasa anual de mantenimiento, conforme lo dispone el artículo 80 de la referida norma comunitaria.

ARTÍCULO 3: Notificar el contenido de la presente resolución a NOKIA SOLUTIONS AND NETWORKS OY, advirtiéndole que contra ella procede el recurso de reposición, ante la Superintendente de Industria y Comercio, el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 27 de junio de 2024

LA SUPERINTENDENTE DE INDUSTRIA Y COMERCIO,



Firmado digitalmente
por: CIELO ELAINNE
RUSINQUE URREGO
Fecha: 2024.06.27
17:01:17 COT
Razón: Validez jurídica.
Ubicación: Bogotá,
Colombia.

Resolución N° 34193

Ref. Expediente N° NC2021/0000912

ANEXO No. 1

REIVINDICACIONES CONCEDIDAS

1. Un nodo de función de interfuncionamiento (N3IWF) (204) para manejar una conexión de red a través de una red de acceso no confiable (110) a una red central (100), en el que la red central (100) es una red 5GCN y la red de acceso no confiable (110) es una red de acceso no 3GPP, que comprende:

una primera interfaz de red configurada para comunicarse con el equipo de usuario (UE) (200) a través de la red de acceso no confiable no 3GPP (110),

una segunda interfaz de red configurada para comunicarse con una función de gestión de acceso y movilidad (AMF) (202) de la red central 5GCN (100), y

un dispositivo de procesamiento (1800) configurado para al menos:

procesar una solicitud del UE (200) de establecimiento de una conexión con la red central 5GCN (100) a través de la red de acceso no confiable no 3GPP (110) y generar una solicitud a la función de gestión de acceso y movilidad (AMF) (202) de la red central 5GCN (100),

proporcionar a la función de gestión de acceso y movilidad (AMF) (202) de la red central 5GCN (100), a través de la segunda interfaz de red, una solicitud de autenticación y conexión segura;

recibir, desde la función de gestión de acceso y movilidad (AMF) en el 5GCN (100), en respuesta a la solicitud de autenticación y establecimiento de conexión segura, una indicación de que el establecimiento de conexiones seguras con la red central 5GCN (100) sobre redes de acceso no confiables no 3GPP (110) no está permitido por la red central 5GCN (100);

proporcionar, al UE (200), un mensaje de respuesta que comprende una indicación de que la solicitud para establecer la conexión segura con la red central 5GCN (100) a través de la red de acceso no confiable no 3GPP (110) no está aprobada porque el establecimiento de conexión segura a la red central 5GCN (100) a través de redes de acceso no confiables no 3GPP (110) no está permitido por la red central 5GCN (100); y

recibir, desde el UE (200), después de proporcionar el mensaje de respuesta al UE (200), un mensaje de detención que finaliza la solicitud para establecer la conexión segura a la red central 5GCN (100) a través de la red de acceso no confiable no 3GPP (110).

2. El nodo de función de interfuncionamiento (204) de la reivindicación 1, en el que el dispositivo de procesamiento (1800) está configurado para:

recibir en la primera interfaz de red, de la UE (200), una solicitud de autenticación y establecimiento de conexión segura del UE con la red central 5GCN (100) a través de la red de acceso no confiable no 3GPP (110),

generar una solicitud de verificación de suscripción y autenticación y transmitir la solicitud de verificación de suscripción y autenticación a través de la segunda interfaz de red a la función de gestión de acceso y movilidad (AMF) (202) de la red central 5GCN (100),

recibir, desde la función de gestión de acceso y movilidad (AMF) (202), sobre la segunda interfaz de red, una respuesta a la verificación de suscripción y autenticación de la AMF, y

generar un mensaje de respuesta de intercambio de claves de Internet (IKE) para el UE (200) con una carga útil de NAS que incluya el error, que indique que la red central 5GCN (100) no permite el establecimiento de la conexión con la red central 5GCN (100) a través de la red de acceso no confiable no 3GPP (110).

3. El nodo de función de interfuncionamiento (204) de la reivindicación 2, en el que el

Resolución N° 34193

Ref. Expediente N° NC2021/0000912

dispositivo de procesamiento (1800) está configurado además para:

recibir una respuesta de la función de gestión de acceso y movilidad (202) que encapsule un mensaje de rechazo del registro, que incluya un valor de causa de 5GMM que indique que no se permite el acceso no 3GPP a la 5GCN (100); y

generar el mensaje de respuesta de IKE con una carga útil que incluya un tipo de mensaje que indique que la red central 5GCN (100) no acepta el establecimiento de la conexión a redes de acceso no confiables no 3GPP (110).

4. El nodo de función de interfuncionamiento (204) de la reivindicación 2, en el que el dispositivo de procesamiento (1800) está configurado además para generar el mensaje de respuesta de IKE mediante:

generación del mensaje de respuesta de IKE con una carga útil de notificación que incluya un tipo de mensaje de notificación privado que indique un motivo del fallo.

5. El nodo de función de interfuncionamiento (204) de la reivindicación 2, en el que el dispositivo de procesamiento (1800) está configurado además para generar el mensaje de respuesta de IKE mediante:

generación del mensaje de respuesta de IKE con una carga útil de notificación que incluya un tipo de mensaje de notificación privado que indique que la red central (5GCN) (100) no permite el establecimiento de conexión o acceso seguro a la red central (5GCN) (100) a través de redes de acceso no-3GPP no confiables no 3GPP (110).

6. El nodo de función de interfuncionamiento (204) de la reivindicación 1, en el que el dispositivo de procesamiento (1800) está configurado además para:

tras recibir un mensaje de detención del UE (200);

generar un mensaje de fallo para el UE y;

transmitirle el mensaje de fallo al UE (200).

7. El nodo de función de interfuncionamiento (204) de la reivindicación 6, en el que el dispositivo de procesamiento (1800) está configurado además para:

procesar el mensaje de detención del UE (200), en el que el mensaje de detención incluye un formato de mensaje de detención de 5G que tiene un campo de identificador de mensaje y en el que el campo de identificador de mensaje incluye un identificador de detención de 5G.

8. El nodo de función de interfuncionamiento (204) de la reivindicación 1, en el que la solicitud de establecimiento de la conexión del UE (200) en la red de acceso no confiable no 3GPP (110) incluye un mensaje de solicitud de IKE para iniciar una asociación de seguridad (SA) IPsec con la red central 5GCN (100).

9. Una función de gestión de acceso y movilidad (AMF) (202) para manejar una solicitud de conexión de red con una red central 5GCN (100) asociada a un UE (200) y recibido de un nodo de función de interfuncionamiento (N3IWF) (204), que comprende:

una interfaz de red configurada para comunicarse con el nodo de función de interfuncionamiento (N3IWF) (204) y una función de autenticación y suscripción (AUSF) (210) en una red central 5GCN (100) y

un dispositivo de procesamiento (1700) configurado para al menos:

recibir, desde la función de interfuncionamiento N3IWF (204), a través de la interfaz de red, una solicitud de autenticación y establecimiento de conexión segura, estando asociada la solicitud de autenticación y establecimiento de conexión segura con una solicitud de establecimiento de conexión segura con la red central 5GCN (100) recibida por la función de interfuncionamiento N3IWF (204) desde el UE (200) a través de una red de acceso no confiable no 3GPP (110);

en respuesta a recibir la solicitud de autenticación y establecimiento de

Resolución N° 34193

Ref. Expediente N° NC2021/0000912

conexión segura, proporcionar una solicitud de autenticación y verificación de suscripción a la función de autenticación y suscripción AUSF (210) de la red central 5GCN (100);

en respuesta a determinar que la verificación de autenticación y suscripción por parte de la función de autenticación y suscripción AUSF (210) ha fallado, generar un mensaje de respuesta a la solicitud de autenticación y establecimiento de conexión segura recibida desde la función de interfuncionamiento N3IWF (204) encapsulando en el mensaje de respuesta un valor de causa que indica que el acceso a la red central 5GCN (100) no está permitido por la red central 5GCN (100) que se establece a través de redes de acceso no confiables no 3GPP (110); y

proporcionar el mensaje de respuesta a la función de interfuncionamiento N3IWF (204) a través de la interfaz de red.

10. La función de gestión de acceso y movilidad AMF (202) de la reivindicación 9, en la que el dispositivo de procesamiento (1700) está configurado para:

encapsular en el mensaje de respuesta un mensaje de rechazo del registro que incluya el valor de la causa, en el que el valor de la causa incluye un valor de causa de 5GMM que indica que no se permite el acceso no 3GPP a la 5GCN (100).

11. La función de gestión de acceso y movilidad AMF (202) de la reivindicación 10, en la que el dispositivo de procesamiento (1700) está configurado para:

generar una indicación de fallo del protocolo de autenticación extensible (EAP) en el mensaje de respuesta.

12. Equipo de usuario (UE) (200) que comprende:

una interfaz de red configurada para comunicarse con un nodo de función de interfuncionamiento N3IWF (204) de una red central 5GCN (100) a través de una red de acceso no confiable no 3GPP (110),

un dispositivo de procesamiento (1600) configurado para al menos:

generar una solicitud de registro para el establecimiento de una sesión segura con una red central 5GCN (100),

enviar, a través de la red de acceso no confiable no 3GPP (110), a la función de interfuncionamiento N3IWF (204) de la red central 5GCN (100), la solicitud de registro;

recibir, en respuesta a la solicitud de registro, desde la función de interfuncionamiento N3IWF (204) de la red central 5GCN (100), un mensaje de respuesta, comprendiendo el mensaje de respuesta una indicación de si el establecimiento de conexión segura a la red central 5GCN (100) sobre redes de acceso no confiables no 3GPP (110) está permitido por la red central 5GCN (100);

determinar, basándose en el mensaje de respuesta, si la red central 5GCN (100) permite el establecimiento de una conexión segura a la red central 5GCN (100) a través de redes de acceso no confiables no 3GPP (110);

determinar, con base en el mensaje de respuesta, que la solicitud de registro para el establecimiento de sesión segura a la red central 5GCN (100) es rechazada; y

en un caso en el que la red central 5GCN (100) no permite el establecimiento de una conexión segura a la red central 5GCN (100) a través de redes de acceso no confiables no 3GPP (110), proporcionando a la función de interfuncionamiento N3IWF (204) de la red central 5GCN (100), un mensaje de detención para finalizar la solicitud de registro para el establecimiento de sesión segura a la red central 5GCN (100).

13. El equipo de usuario UE (200) de la reivindicación 12, en el que el dispositivo de procesamiento (1600) está configurado además para:

Resolución N° 34193

Ref. Expediente N° NC2021/0000912

generar el mensaje de detención como un mensaje formateado de respuesta al EAP que incluya un campo de identificador de mensaje establecido como detención de 5G.

14. El equipo de usuario UE (200) de la reivindicación 13, en el que el dispositivo de procesamiento (1600) está configurado además para:

procesar un mensaje de fallo del EAP del nodo de función de interfuncionamiento N3IWF (204) y

realizar un procedimiento de eliminación de la asociación de seguridad.

15. El equipo de usuario UE (200) de la reivindicación 12, en el que el dispositivo de procesamiento (1600) está configurado además para:

reintentar el registro con la red central 5GCN (100) mediante la generación de una segunda solicitud de registro para el establecimiento de una sesión segura con la red central 5GCN (100);

transmitir, a través de la red de acceso no confiable no 3GPP (110), hacia la red central 5GCN (100), la segunda solicitud de registro para el establecimiento de sesión segura a la red central 5GCN (100);

recibir, desde la función de interfuncionamiento N3IWF (204) de la red central 5GCN (100), un segundo mensaje de respuesta; y

determinar, a partir de un segundo mensaje de respuesta recibido en el equipo de usuario UE (200) desde la función de interfuncionamiento N3IWF (204) de la red central 5GCN (100), el éxito de la segunda solicitud de registro para el establecimiento de sesión segura a la red central 5GCN (100) a través de la red de acceso no confiable no 3GPP (110).

16. El equipo de usuario UE (200) de la reivindicación 15, en el que el dispositivo de procesamiento (1600) está configurado además para:

generar la segunda solicitud de registro para el establecimiento de una sesión segura con la 5GCN (100), con parámetros actualizados.

17. Un nodo de función de interfuncionamiento (N3IWF) (204) para gestionar una conexión de red a través de una red de acceso (110) no confiable no 3GPP (110) a una red central de quinta generación (5GCN) (100), comprendiendo el nodo de función de interfuncionamiento N3IWF (204):

una primera interfaz de red configurada para comunicarse con el equipo de usuario (200) a través de la red de acceso no confiable no 3GPP (110);

una segunda interfaz de red configurada para comunicarse con un nodo (202) de función de gestión de acceso y movilidad (AMF) en la red central 5GCN (100); y

un dispositivo de procesamiento (1800) configurado para realizar al menos:

procesar una solicitud de registro para un establecimiento de conexión segura a la red central 5GCN (100) desde el UE (200) a través de la red de acceso no confiable no 3GPP (110);

proporcionar, al nodo AMF (202) en la red central 5GCN (100), a través de la segunda interfaz de red, una solicitud de autenticación y establecimiento de conexión segura;

determinar, basándose en una respuesta recibida del nodo AMF (202) en el 5GCN (100) en respuesta a la solicitud de autenticación y establecimiento de conexión segura, que ese establecimiento de conexiones seguras con la red central 5GCN (100) sobre cualquier red de acceso no confiable no 3GPP (110) no está permitido por la red central 5GCN (100); y

proporcionar, al UE (200), un mensaje de respuesta que comprende una indicación de que la solicitud de registro para establecer la conexión segura con la red central 5GCN (100) no está aprobada porque el establecimiento de conexión segura con

Resolución N° 34193

Ref. Expediente N° NC2021/0000912

la red central 5GCN (100) a través de cualquier acceso no confiable no 3GPP (110) no está permitida por la red central 5GCN (100).

18. Un dispositivo (204) configurado para funcionar como un nodo de función de gestión de acceso y movilidad (AMF) en una red central de quinta generación (5GCN) (100) para manejar solicitudes de conexión de red recibidas desde un nodo de función de interfuncionamiento (N3IWF) (202), el dispositivo (204) comprende:

- una interfaz de red configurada para comunicarse con el nodo de función de interfuncionamiento N3IWF (202) y una función de autenticación y suscripción (AUSF) (210) en la red central 5GCN (100); y

- un dispositivo de procesamiento (1700) configurado para realizar al menos:

- procesar una solicitud de registro para el establecimiento de una conexión segura para un UE (200), siendo proporcionada la solicitud de registro por el UE (200) a través de una red de acceso (110) no confiable no 3GPP (110);

- generar una solicitud de verificación de autenticación y suscripción para transmitirla hacia la AUSF (210);

- determinar, basándose en una respuesta de autenticación a la verificación de autenticación y suscripción recibida del AUSF (210), si la respuesta de autenticación indica un éxito de autenticación o un fracaso de autenticación;

- generar, en respuesta a la solicitud de registro para el establecimiento de conexión segura sobre la red de acceso no confiable no 3GPP (110), un mensaje de respuesta de registro; y

- en un caso en el que la respuesta de autenticación indica un error de autenticación, encapsular en el mensaje de respuesta de registro un valor de causa que indica que la red central 5GCN no permite el establecimiento de una conexión segura con la red central 5GCN (100) a través de cualquier red de acceso no confiable no 3GPP (110).

19. Un equipo de usuario (200) que comprende:

- una interfaz de red configurada para comunicarse con un nodo de función de interfuncionamiento (N3IWF) (204) de una red central (100) a través de una red de acceso (110) no confiable no 3GPP (110); y

- un dispositivo de procesamiento (1600) configurado para realizar al menos:

- generar una solicitud de registro para el establecimiento de una conexión segura para enviarla hacia la red central (100);

- enviar, a través de la red de acceso no confiable (110) no 3GPP (110), al nodo de función de interfuncionamiento N3IWF (204) de la red central (100), la solicitud de registro;

- recibir, en respuesta a la solicitud de registro, desde el nodo de función de interfuncionamiento N3IWF (204) de la red central (100), un mensaje de respuesta, comprendiendo el mensaje de respuesta una indicación de si se permite la solicitud de establecimiento de conexión segura a la red central (100) a través de redes de acceso no confiables no 3GPP (110);

- determinar, a partir del mensaje de respuesta, que la red central (100) no permite el establecimiento de conexión segura con la red central (100) a través de cualquier red de acceso no confiable no 3GPP (110);

- determinar finalizar la solicitud de registro para el establecimiento de conexión segura con la red central (100) a través de la red de acceso no confiable no 3GPP (110);

- generar un mensaje de detención que comprende un campo de identificador de mensaje que incluye un identificador de detención en el campo de identificador de mensaje, indicando el identificador de detención que el UE (200) tiene la intención de finalizar la solicitud de registro para el establecimiento de conexión segura con la red central (100) a través de la red no confiable no 3GPP (110); y

- transmitir el mensaje de detención hacia el nodo de función de interfuncionamiento N3IWF (204) de la red central (100) para finalizar la solicitud de registro para el establecimiento de conexión segura con la red central (100) a través de la

Resolución N° 34193

Ref. Expediente N° NC2021/0000912

red de acceso no confiable no 3GPP (110).

20. Un equipo de usuario (UE) (200) que comprende:

una interfaz de red configurada para comunicarse con un nodo de función de interfuncionamiento (N3IWF) (204), de una red central de quinta generación (5GCN) (100), a través de una red de acceso no confiable (110); y

un dispositivo de procesamiento (1600) configurado para realizar al menos: generar una solicitud de registro para el establecimiento de conexión segura con la red central 5GCN (100);

enviar, a través de la red de acceso no confiable (110), al nodo de función de interfuncionamiento N3IWF (204) de la red central 5GCN (100), un mensaje que comprende la solicitud de establecimiento de conexión segura con la red central 5GCN (100);

recibir, en respuesta a la solicitud, desde el nodo de función de interfuncionamiento N3IWF (204) de la red central 5GCN (100), un mensaje de respuesta, comprendiendo el mensaje de respuesta un valor de causa de gestión de movilidad 5G (5GMM) que indica que la red central 5GCN (100) no permite establecimiento de una conexión segura con la red central 5GCN (100) sobre cualquier red de acceso no confiable (110);

determinar, a partir del valor de causa de la red central 5GMM en el mensaje de respuesta recibido del nodo de función de interfuncionamiento N3IWF (204), que la red central 5GCN (100) no permite que se establezca el establecimiento de una conexión segura con la red central 5GCN (100) a través de cualquier red de acceso no confiable (110);

en un caso en el que la red central 5GCN (100) no permite el establecimiento de una conexión segura con la red central 5GCN (100) a través de cualquier red de acceso no confiable (110), generar un mensaje de detención que comprende un campo de identificador de mensaje, incluyendo el campo de identificador de mensaje un identificador de detención de 5G ;

establecer el identificador de detención 5G en el campo de identificador de mensaje del mensaje de detención en 5G; y

transmitir el mensaje de detención hacia el nodo de función de interfuncionamiento N3IWF (204) de la red central 5GCN (100) para finalizar la solicitud de registro para el establecimiento de conexión segura con la red central 5GCN (100) a través de la red de acceso no confiable (110).

21. Un equipo de usuario (200) que comprende:

una interfaz de red configurada para comunicarse con un nodo de función de interfuncionamiento (N3IWF) (204) de una red central de quinta generación (5GCN) (100), a través de una red de acceso (110) no confiable no 3GPP (110); y

un dispositivo de procesamiento (1600) configurado para realizar al menos: generar una solicitud de registro para el establecimiento de conexión segura con la red central 5GCN (100);

enviar, a través de la red de acceso no confiable (110) no 3GPP, al nodo de función de interfuncionamiento N3IWF (204) de la red central 5GCN (100), un mensaje que comprende la solicitud de establecimiento de conexión segura con la red central 5GCN (100);

recibir, en respuesta a la solicitud, desde el nodo de función de interfuncionamiento N3IWF de la red central 5GCN (100), un mensaje de respuesta, comprendiendo el mensaje de respuesta un valor de causa de gestión de movilidad 5G (5GMM) que indica que la red central 5GCN (100) no permite el establecimiento de conexión segura con la red central 5GCN (100) sobre cualquier red de acceso no confiable no 3GPP (110);

determinar, a partir del mensaje de respuesta, que la red central 5GCN (100) no permite el establecimiento de una conexión segura con la red central 5GCN (100) a

Resolución N° 34193

Ref. Expediente N° NC2021/0000912

través de cualquier red de acceso no confiable no 3GPP (110);

en un caso en el que la red central 5GCN (100) no permite el establecimiento de una conexión segura con la red central 5GCN (100) a través de cualquier red de acceso no confiable (110) no 3GPP (110), generar un mensaje de detención que comprende un campo de identificador de mensaje, incluyendo el campo de identificador de mensaje un Identificador de detención 5G;

establecer el identificador de detención 5G en el campo de identificador de mensaje del mensaje de detención en 5G-; y

transmitir el mensaje de detención hacia el nodo de función de interfuncionamiento N3IWF (204) de la red central 5GCN (100) para finalizar la solicitud de registro para el establecimiento de conexión segura con la red central 5GCN (100) a través de la red de acceso no confiable no 3GPP (110).