



Señora

Edna Marcela Ramírez Orozco

Directora de Nuevas Creaciones

Superintendencia de Industria y Comercio

E. S. D.

Referencia: Solicitud de Patente de Invención PCT denominada “**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**”

Asunto: Respuesta al oficio No. 19504 de 30 de noviembre de 2023

Expediente No. NC2021/0000912

Juan Carlos Cuesta Quintero, mayor de edad, identificado como aparece al pie de mi firma, obrando en mi calidad de apoderado de **NOKIA SOLUTIONS AND NETWORKS OY** doy respuesta al Oficio No. 19504 de 30 de noviembre de 2023, bajo los siguientes términos:



1. De la solicitud de patente

1.1. Título

En la Acción de la Oficina, se objeta el Título de la presente solicitud por no reflejar el asunto de la descripción y las reivindicaciones. Concretamente, el Examinador sugiere el siguiente título: “NODO, FUNCIÓN DE RED Y EQUIPO DE USUARIO PARA MANEJAR FALLOS DE ASOCIACIÓN DE SEGURIDAD CON EL PLANO DE USUARIO”.

Sin embargo, nos parece más adecuado que el título sea:

“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 base al menos en esta modificación del Título de esta solicitud, el Solicitante solicita respetuosamente que el Examinador retire su objeción al Título de la solicitud conforme al Artículo 27(d) de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina.

1.2. Reivindicaciones

Para atender a la objeción en contra de la claridad del capítulo reivindicatorio, se han añadido los números de referencia.

Adicionalmente, para atender a las objeciones sustantivas se han modificado las reivindicaciones y se han añadido las nuevas reivindicaciones 17 a 21.

Las modificaciones hallan soporte literal en los párrafo [0011] a [0018] tal como se presentó.



2. Examen de Patentabilidad

2.1. Novedad y Nivel Inventivo

En el Examen, se alega que **D1** (*Technical Specification Group Services and System Aspects; Procedures for the 5G System; Stage 2 (Release 15)*) es el estado de la técnica más cercano y que las Reivindicaciones 14, 15, 19 y 20 carecen de novedad en vista de **D1**.

Se alega además que las Reivindicaciones 1-13 y 16-18 carecen de actividad inventiva a la vista de **D1** y **D2 (US2016127415)**.

Sin embargo, **D1** no describe ni sugiere el nodo de función de interfuncionamiento de la reivindicación 1 al menos porque **D1** no describe ni sugiere al menos:

Distinción 1: 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

Distinción 2: un mensaje de detención que finaliza la solicitud para establecer la conexión segura a la red central 5GCN a través de la red de acceso no confiable no 3GPP.

Con respecto a la Distinción 1, sostenemos respetuosamente que esta distinción proporciona un efecto técnico de gestión de fallos durante el establecimiento de una conexión segura para el acceso a una red central 5G a través de redes de acceso que no son 3GPP, y que el problema técnico objetivo como consecuencia de la Distinción 1 es gestionar 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.



Sostenemos respetuosamente que a un experto, partiendo de **D1**, y enfrentado a este problema técnico objetivo, no le habría resultado obvio generar un nuevo código de error que indique una notificación de error, como cuando al UE no se le permite utilizar un Acceso no 3GPP a EPC porque o bien:

I. el UE no tiene una suscripción para establecer una conexión segura con el 5GCN a través de una red de acceso no confiable no 3GPP; o

II. 5GCN no está configurado para permitir el establecimiento de una conexión segura a través de una red de acceso no confiable no 3GPP.

Patentabilidad de la reivindicación 1 modificada a la vista de D1 y D2

Sin embargo, aunque discrepemos de algunas caracterizaciones, objeciones o rechazos presentados en el Examen, hemos modificado las Reivindicaciones independientes 1, 9 (anterior reivindicación 10) y la Reivindicación independiente 12 (anteriormente Reivindicación 14) para aclarar la materia reivindicada.

Por ejemplo, la Reivindicación 1 independiente se ha modificado de modo que dice:

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 son 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).

Si bien **D1** puede describir, en general, un proceso mediante el cual se rechaza una solicitud de registro **particular**, **D1** no describe ni sugiere que un rechazo de registro, o también una



verificación de suscripción y autenticación entre N3IWF y AUSF, pueda incluir una indicación de que el 5GCN no permite el establecimiento de una conexión segura con 5GCN a través de **CUALQUIER** red de acceso que no sea de confianza y que no sea 3GPP, lo cual es una indicación de una configuración del lado 5GCN, en lugar de un rechazo anecdótico de una solicitud de registro anecdótica realizada por el UE.

El UE, al recibir un mensaje de rechazo de registro que incluye un valor de causa de 5GMM que indica que el 5GCN no permite el establecimiento de una conexión segura a través de **CUALQUIER** red de acceso no confiable no 3GPP, puede determinar que no debe volver a intentar el registro con el 5GCN a través de la misma o cualquier otra red de acceso no confiable no 3GPP basada en dicha información de configuración sobre el 5GCN.

Por el contrario, el UE en **D1** seguramente volverá a intentar registrarse con el 5GCN a través de la red de acceso no confiable que no es 3GPP como algo natural, según los requisitos de versiones anteriores del estándar 3GPP y tal como se describe en **D1**.

Asimismo, el N3IWF en la presente solicitud está configurado para indicar información de configuración de 5GCN al UE mediante la generación de un mensaje de rechazo de registro que indica que el 5GCN no permite el establecimiento de conexión segura con el 5GCN a través de **CUALQUIER** red de acceso no confiable no 3GPP, que indica una configuración 5GCN.

Por el contrario, cualquier indicación de error previamente existente, como cualquiera divulgado en **D1** o en cualquier versión anterior del estándar 3GPP, simplemente indica que **la solicitud de registro específica** recibida del UE es rechazada, pero no proporciona ninguna información al UE sobre capacidades o información de configuración con respecto al 5GCN, como que el 5GCN no permite que se inicie o lleve a cabo el establecimiento



seguro de conexión/sesión con el 5GCN a través de cualquier red de acceso no confiable no 3GPP.

Otra distinción sobre **D1** es que el UE del solicitante envía (y el N3IWF del solicitante recibe del UE del solicitante) un mensaje de detención en respuesta a que el UE del solicitante recibe la indicación de causa 5GMM en el mensaje de rechazo de registro del N3IWF del solicitante, lo que hace que el UE del solicitante termine inmediatamente la solicitud de registro, envíe el mensaje de detención y preferentemente agregue un identificador para el 5GCN a una lista (almacenada en el UE) de PLMN para las cuales el establecimiento de conexión/sesión segura no se puede iniciar/realizar a través de una red de acceso no confiable no 3GPP.

Por el contrario, el UE en **D1** volvería a intentar la solicitud de registro para establecer la conexión segura con el 5GCN a través de la misma red de acceso hasta que expire un temporizador de nuevo intento de registro.

Además, **D1** no dice nada sobre las causas o factores desencadenantes del rechazo de una solicitud de registro o de establecimiento de sesión. Como tal, **D1** guarda completo silencio con respecto a al menos “describir”, “proporcionar, desde el N3IWF, al UE, un mensaje de respuesta que comprenda un valor de causa de gestión de movilidad 5G (5GMM) que indique que el 5GCN no permite el acceso a el 5GCN a través de cualquier red de acceso no confiable no 3GPP” 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)”, tal como se indica ahora en la Reivindicación 1 modificada.



Además, **D1** no describe ni sugiere el nodo de función de interfuncionamiento de la reivindicación 1 al menos porque **D1** no describe ni sugiere "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)".

Como se señaló anteriormente, si bien **D1** puede describir, en general, un proceso mediante el cual se rechaza una solicitud de registro particular, **D1** no describe ni sugiere que un rechazo de registro, o una verificación de suscripción y autenticación entre N3IWF y AUSF, pueda incluir una indicación de que el 5GCN no permite el establecimiento de una conexión segura con el 5GCN a través de CUALQUIER red de acceso no confiable no 3GPP, lo cual es una indicación de una configuración del lado del 5GCN, en lugar de un rechazo anecdótico de una solicitud de registro anecdótica realizada por el UE. El UE, al recibir un mensaje de rechazo de registro que incluye una indicación del lado 5GMM que indica que el 5GCN no permite el establecimiento de una conexión segura a través de CUALQUIER red de acceso no confiable no 3GPP, puede determinar que no debe volver a intentar el registro con el 5GCN a través de la misma o cualquier otra red de acceso no confiable no



3GPP basada en dicha información de configuración sobre el 5GCN. Por el contrario, el UE en **D1** seguramente volverá a intentar registrarse con el 5GCN a través de la red de acceso no confiable que no es 3GPP como algo natural, según los requisitos de las versiones anteriores del estándar 3GPP, tanto como se describe en **D1** o en otras secciones del estándar 3GPP tal como existía antes de la fecha de presentación más temprana de la presente solicitud. Asimismo, el N3IWF en la presente solicitud está configurado para indicar información de configuración de 5GCN al UE mediante la generación de un mensaje de rechazo de registro que incluye la indicación 5GMM que indica que el 5GCN no permite el establecimiento de conexión segura con el 5GCN a través de **CUALQUIER** red de acceso no confiable no 3GPP, que indica una configuración 5GCN, mientras que cualquier indicación previamente existente, como cualquiera divulgada en **D1**, simplemente indica que la solicitud de registro específica recibida del UE es rechazada, pero no proporciona dicha información de configuración a la UE.

Otra distinción con respecto a **D1** es que el UE envía (y el N3IWF recibe) un mensaje de detención del UE en respuesta a recibir la indicación 5GMM en el mensaje de rechazo de registro, que finaliza inmediatamente la solicitud de registro. En **D1**, el UE volvería a intentar la solicitud de registro para establecer la conexión segura con el 5GCN a través de la misma red de acceso hasta que expire un temporizador de nuevo intento de registro. Además, en **D1**, las únicas causas/desencadenantes del rechazo de una solicitud de registro que se divulgan son “si falla el procedimiento de autenticación/seguridad” (ver **D1**, en la página 11), si la red no puede cumplir con una solicitud de servicio (ver **D1**, en la parte superior de la página 15 y en la parte superior de la página 16), si la AMF no puede manejar una solicitud de servicio (ver **D1**, en la página 18), si la AMF recibe un mensaje N11 de la SMF que reemplaza el procedimiento de registro debido a un cambio de AMF (ver **D1**, en las páginas 19-21), si una entidad de red asignada para una Solicitud de notificación de accesibilidad del UE no está autorizada para el suscriptor asociado con el UE (ver **D1**, en la página 23), o si la SMF determina que una solicitud de UE particular no cumple con la suscripción del



usuario o las políticas locales (ver **D1** en la página 27). Sin embargo, **D1** guarda completo silencio con respecto a al menos *“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)”, “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)” red de acceso”, como se indica ahora en la Reivindicación 1 enmendada.*

Por ejemplo, la Figura 4.12.2-1 de **D1**, que se reproduce a continuación para facilitar la referencia, describe en cambio:

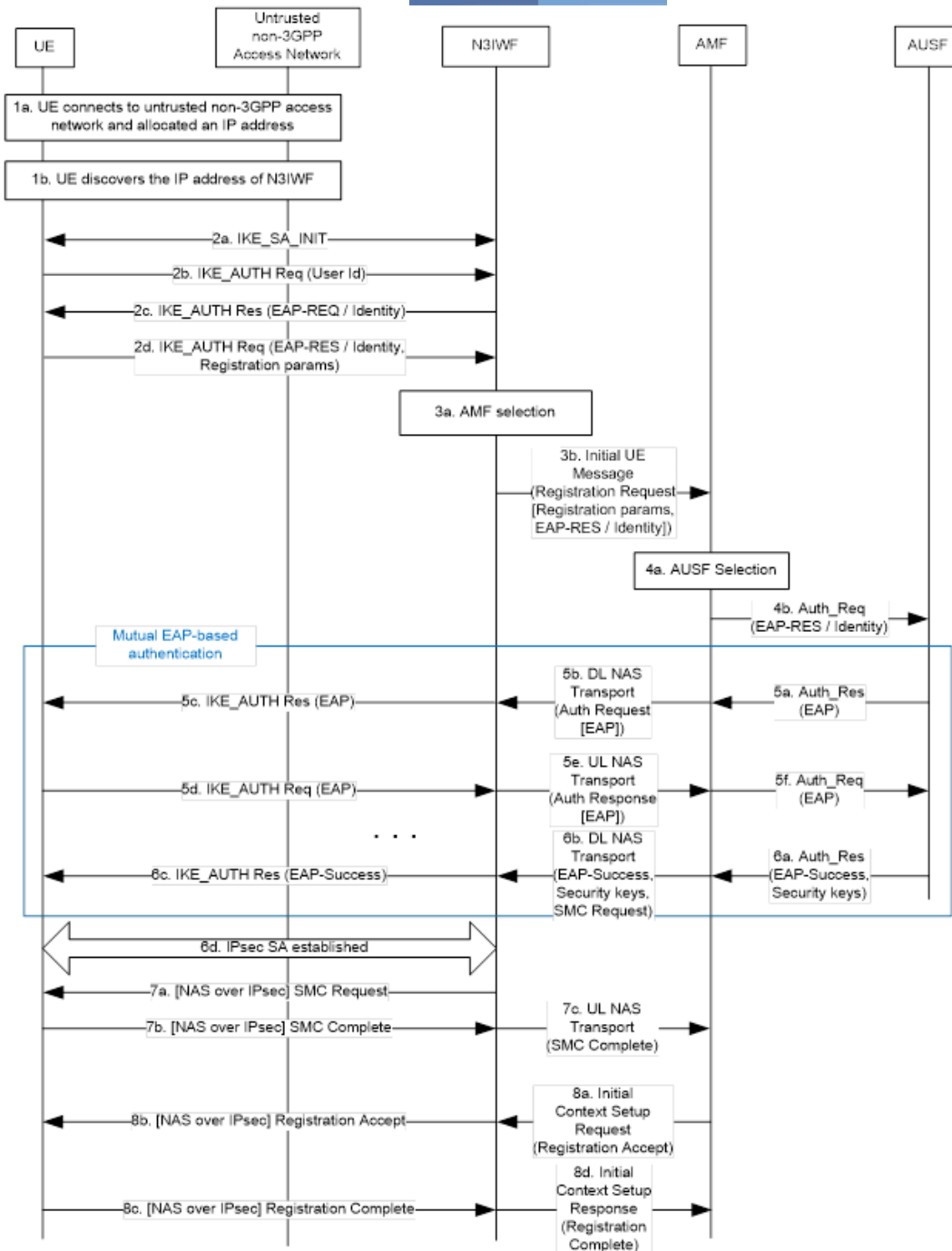


FIGURA 4.12.2-1 Registro mediante acceso no confiable no 3GPP



Sería inadecuado interpretar el paso 6b de la Figura 4.12.2-1 de **D1** como supuestamente "recibir, desde uno o más nodos en la red central, en respuesta a la solicitud de autenticación y establecimiento de conexión segura, una indicación de que el establecimiento de conexiones seguras a la red central a través de redes de acceso no confiables no está permitido por la red central" o "proporcionar, al UE, un mensaje de respuesta que incluya una indicación de que la solicitud para establecer la conexión segura no está aprobada porque el establecimiento de una conexión segura a la red central porque la red central no permite la conexión a través de redes de acceso que no son de confianza".

En cambio, el paso 6b de la Figura 4.12.2-1 de **D1** simplemente ilustra la AMF transmitiendo al N3IWF un mensaje de Transporte DL NAS que indica que el AUSF seleccionado por la AMF ha autenticado al UE para acceder a la red central. En particular, la página 46 de **D1** describe claramente que *"puede usarse [c]ualquier método de autenticación que no sea 3GPP"*. **D1** también describe en la página 46 que la AMF, al recibir el mensaje de UE inicial en el paso 3b de la N3IWF, *"la AMF puede solicitar el contexto SUPI y MM del UE de otra AMF"*. **D1** también describe en la página 46 que *"[l]a AMF seleccionará un AUSF de acuerdo con el procedimiento de selección especificado en TS 23.501 [2] cláusula TBD, y solicitará a AUSF autenticar el UE enviando un Auth_Req (EAP-RES/ Identidad) a AUSF"* y que *"[e]l AUSF operará como un servidor EAP y elegirá un método EAP para autenticar el UE, p.e. basado en la información de suscripción de UE y la información incluida en la NAI de UE. La AUSF puede recuperar información de suscripción de UE de la UDM"*. Dicho de otro modo, **D1** describe que, al recibir un mensaje de UE inicial (por ejemplo, solicitud de registro de UE) de la N3IWF, la AMF "deberá" comunicarse con "otra AMF" para solicitar cualquier información de UE o de abonado faltante, y la AMF "deberá" "seleccionar un AUSF que "deberá" autenticar el UE "recuperando la información del suscriptor del UDM".



D1 guarda completo silencio sobre cualquier situación en la que la AMF pueda incluso decidir o determinar que la red central no acepta solicitudes de conexión a través de redes de acceso que no son de confianza. Como tal, si bien **D1** puede describir que la AMF puede aceptar una solicitud de conexión a través de redes de acceso que no son de confianza (por ejemplo, no 3GPP), **D1** no dice nada acerca de que la AMF determine que la red central no aceptará solicitudes de conexión a través de redes de acceso que no son de confianza, y de hecho, proporciona una solución alternativa para procesar solicitudes de conexión a través de redes de acceso no confiables desde el UE. En particular, **D1** describe que la N3IWF selecciona particularmente una AMF y una red central basándose en los parámetros y requisitos de registro particulares del UE y la red central, lo que significa que la N3IWF de **D1** simplemente selecciona una AMF de una red central que la N3IWF sabe que acepta dicha solicitud de conexión del UE a través de una red de acceso no confiable. **D1** también describe que la AMF recibe la solicitud de conexión de la N3IWF en nombre del UE y, si falta el contexto SUPI o MM, puede recuperarlos de "otra AMF". **D1** también describe que, si la AMF recibe una solicitud de conexión y le falta información del abonado, la AMF puede recuperar la información del abonado del UDM. Sin embargo, **D1** también describe que "cómo y cuándo la AMF obtiene datos de suscriptores de UE" es "FFS", es decir, "queda en estudio".

Incluso suponiendo *arguyendo* que **D1** describe que la N3IWF y la AMF facilitan el establecimiento de una conexión entre el UE y la red central en respuesta a la recepción de una solicitud de conexión del UE en la red de acceso no confiable, **D1** no proporciona ninguna orientación sobre lo que debería hacer la AMF si la red central no aceptara el establecimiento de conexión en la red de acceso no confiable, ni **D1** proporciona ninguna guía sobre cómo la AMF comunicaría dicha no aceptación del establecimiento de conexión a la N3IWF o desde la N3IWF al UE.



En cambio, el paso 6b de la Figura 4.12.2-1 de **D1** en realidad describe exactamente lo contrario, que es que el N3IWF determina que el establecimiento de la conexión **es aceptado** por la red central porque el N3IWF recibe, desde el AMF, un mensaje de transporte DL NAS que incluye el Mensaje de éxito EAP, claves de seguridad y solicitud de SMC. ¿Cómo puede una persona con conocimientos habituales en la técnica inferir del paso 6b de la Figura 4.12.2-1 de **D1**, los mensajes específicos y distintos que se requerirían entre la AMF y la N3IWF, y entre la N3IWF y el UE, en la situación exactamente opuesta en la que la red central rechaza la solicitud de restablecimiento de la conexión cuando esa situación opuesta ni siquiera se discute o se insinúa en **D1**? El solicitante sostiene respetuosamente que no se podría haber esperado razonablemente que la persona con conocimientos habituales en la técnica hubiera interpretado o inferido que la N3IWF determinaría que el establecimiento de la conexión **no es aceptado** por la red central basándose en cualquier divulgación o sugerencia de **D1**.

Como tal, **D1** no puede proporcionar ninguna guía para el elemento de la reivindicación 1 de "proporcionar, al equipo del usuario, un mensaje de respuesta que comprende una indicación de que la solicitud para establecer la conexión segura no está aprobada porque el establecimiento de la conexión segura a la red central a través de La red central no permite redes de acceso que no sean de confianza". Una persona con conocimientos habituales en la técnica, basándose en la divulgación de **D1**, entendería únicamente que el N3IWF puede generar y transmitir al UE un mensaje de "EAP-Éxito", como se ilustra en el paso 6c de la Figura 4.12.2-1 de **D1**. Como tal, incluso si la AMF de **D1** determinara que el establecimiento de la conexión no es aceptado por la red central porque la conexión se realizaría a través de una red de acceso no confiable, la persona con conocimientos habituales en la técnica no encontraría ninguna orientación en **D1**. sobre cómo la AMF debería indicar a la N3IWF que la red central no aceptará la solicitud de establecimiento de conexión, ni cómo la N3IWF debería comunicar lo mismo al UE.



Dado que **D1** no enseña o sugiere al menos “recibir, desde uno o más nodos en la red central, en respuesta a la solicitud de autenticación y establecimiento de conexión segura, una indicación de que el establecimiento de conexiones seguras a la red central a través de redes de acceso no confiables no está permitido por la red central” y “proporcionar, al UE, un mensaje de respuesta que comprende una indicación de que la solicitud para establecer la conexión segura no está aprobada porque la red central no permite el establecimiento de una conexión segura a la red central a través de redes de acceso no confiables”, se deduce lógicamente que la Reivindicación 1 es novedosa y representa una actividad inventiva en vista de **D1**.

Además, como se señaló anteriormente, **D1** no dice nada con respecto a que el UE envía al N3IWF un mensaje de detención en respuesta a que el UE recibe una indicación de que la red central no permite el establecimiento de una conexión segura a la red central a través de redes de acceso no confiables.

Incluso suponiendo que el uso de un mensaje de detención para finalizar una solicitud de registro se considera parte del conocimiento común para una persona con conocimientos habituales en la técnica, no habría sido obvio enviar un mensaje de detención en respuesta al mensaje de rechazo de rechazo recibido de la N3IWF al menos porque el enfoque estándar bajo 3GPP antes del momento de la presentación de la presente solicitud era iterar un contador de intentos de registro y/o verificar un temporizador de intentos de registro (por ejemplo, el temporizador T3510) y luego volver a intentar solicitud de registro a través de la misma red de acceso. Por ejemplo, la N3IWF podría haber utilizado un valor de causa 5GMM de “11” en **D1** para indicar al UE que el acceso a la PLMN no está permitido según los términos/políticas de suscripción o la prohibición del operador de la PLMN. Este es una indicación 5GMM que indica que no se permite ningún acceso por parte del UE a la PLMN a través de cualquier red de acceso porque, por ejemplo, el UE está asociado con un abonado que no es un abonado de la PLMN y para el cual no existe ningún acuerdo de



itinerancia entre la HPLMN del UE y la PLMN (por ejemplo, VPLMN) a la que el UE está intentando acceder. Sin embargo, muchas veces el problema con la solicitud de registro/solicitud de sesión inicial/original es que el UE incluyó información de suscripción incorrecta o desactualizada, o similar. Por lo tanto, el UE normalmente volverá a intentar la solicitud de registro después de un rechazo por parte de la PLMN y, a menudo, incluirá información de suscripción actualizada, información actualizada sobre la red de acceso, información actualizada del acuerdo de itinerancia y/o similares.

Por el contrario, en la presente solicitud, el Solicitante divulga una indicación 5GMM nueva y distinta que se comunica entre nodos de una red central y/o con el UE para indicar que un 5GCN no permite que se establezca ninguna conexión segura al 5GCN a través de cualquier red de acceso que no sea de confianza. Al transmitir dicha información de configuración al UE, el UE reconocerá inmediatamente que volver a intentar la solicitud de registro a través de la misma red de acceso no confiable, ya sea que se proporcione o no información de abonado nueva/actualizada, nunca logrará la aceptación de la solicitud de registro porque el 5GCN simplemente no permite que se establezcan conexiones seguras a través de redes de acceso que no sean de confianza. Después de presentar la presente solicitud, el Solicitante también presentó un documento de contribución de estándares al 3GPP, lo que llevó a la creación de un nuevo valor de causa 5GMM en el estándar 3GPP, a saber, "*Cause #73 – Serving network not authorized*", lo que hace que el UE inmediatamente (sin volver a intentar el registro ni siquiera una vez) envíe un mensaje de detención, reinicie el contador de intentos de registro, almacene la identidad de PLMN en la "lista de PLMN prohibida" en el UE e ingrese al estado 5GMM-DEREGISTRED, PLMN-SEARCH. Ver, por ejemplo, las páginas 147, 148, 160, 182, 206 y 440 de 3GPP TS 24.501, versión 15.5.0, de fecha 24 de septiembre de 2019.

Incluso suponiendo que el uso de un mensaje de detención para finalizar una solicitud de registro se considera parte del conocimiento común para una persona con conocimientos



habituales en la técnica, no habría sido obvio que el UE de **D1** envíe un mensaje de detención para finalizar una solicitud de registro/sesión en respuesta a un mensaje inicial o único de Rechazo de Registro o similar. El UE en **D1** no sólo no tendría ningún motivo para no volver a solicitar el registro con la red central a través de la misma red de acceso no confiable no 3GPP, o una red de acceso diferente no confiable no 3GPP, en respuesta a que el UE reciba una única/inicial mensaje de Rechazo de Registro, pero además el UE en **D1** no tendría ninguna razón para generar un Mensaje de Detención en particular, ni para transmitir ese mensaje particular al N3IWF de **D1** porque el UE de **D1** simplemente interpretaría un fallo de la solicitud de registro, por ejemplo, como siendo un fracaso de un intento de registro particular y discreto, y no indicativo de ninguna limitación de 5GCN, requisito de registro o acción deseada por parte del UE con respecto a solicitudes de registro posteriores, que el UE de **D1** gestionaría de forma completamente independiente de cualquier intento de registro anterior.

Además, en versiones anteriores del estándar 3GPP, los valores de causa 5GMM de “11”, por ejemplo, son utilizados por una N3IWF para indicar a un UE que el acceso a una PLMN particular no está permitido según los términos/políticas de suscripción o la prohibición del operador de la PLMN. Este es un valor de causa de 5GMM que indica que cualquier acceso del UE a la PLMN a través de cualquier red de acceso (ya sea confiable o no confiable, ya sea 3GPP o no 3GPP) no está permitido porque, por ejemplo, el UE está asociado con un abonado que es no es un abonado de la PLMN y para el cual no se ha establecido ningún acuerdo de itinerancia entre la HPLMN del UE y la PLMN (por ejemplo, VPLMN) a la que el UE está intentando acceder. Sin embargo, muchas veces el problema con la solicitud de registro/solicitud de sesión inicial/original es que el UE incluyó información de suscripción incorrecta o desactualizada, o similar. Por lo tanto, el UE normalmente volverá a intentar la solicitud de registro después de un rechazo por parte de la PLMN y, a menudo, incluirá información de suscripción actualizada, información actualizada sobre la red de acceso, información actualizada del acuerdo de itinerancia y/o similares. Como tal, incluso pariendo



de **D1**, y en vista de versiones anteriores de partes relevantes del estándar 3GPP, una persona con conocimientos habituales en la técnica habría configurado el UE de **D1** para volver a intentar el registro en la red central sin tener en cuenta el tipo de red de acceso, habría configurado el N3IWF de **D1** para indicar a un UE simplemente que el intento de registro discreto particular ha fallado, y habría configurado el AMF de **D1** para indicar simplemente al N3IWF que el intento de registro discreto particular ha fallado, por ejemplo, debido a un problema de autenticación/términos/políticas del suscriptor.

Por el contrario, en la presente solicitud, el Solicitante divulga un valor de causa 5GMM nuevo y distinto que se comunica entre nodos de una red central y/o con el UE para indicar que un 5GCN no permite que se establezca ninguna conexión/sesión segura al 5GCN a través de cualquier red de acceso que no sea de confianza, como una red de acceso que no sea de confianza y que no sea 3GPP. Al transmitir dicha información de configuración del 5GCN (información sobre las limitaciones del 5GCN) al UE, el UE reconocerá inmediatamente que volver a intentar el registro con el 5GCN a través de la misma red de acceso no confiable que no es 3GPP u otra red de acceso no confiable que no es 3GPP, ya sea Se proporciona o no información nueva/actualizada del suscriptor, nunca logrará la aceptación de la solicitud de registro porque el 5GCN simplemente no permite que se establezcan conexiones seguras a través de ninguna red de acceso no confiable que no sea 3GPP.

Basado al menos en las deficiencias con respecto a **D1** descritas anteriormente, el Solicitante sostiene respetuosamente que el rechazo de la Reivindicación 1 es inadecuado y debe retirarse.

Además, en la Acción de la Oficina, el Examinador alega que **D2** soluciona al menos algunas de estas deficiencias de **D1**. Discrepamos respetuosamente, según nuestra opinión, D2 no logra superar al menos estas deficiencias de **D1**.



Al contrario, **D2** puede describir, en general, el uso de tipos de error IKE cuando un UE intenta conectarse con una red a través de una interfaz SWm mediante una puerta de enlace de datos en paquetes evolucionada. Sin embargo, la indicación del tipo de error IKEv2 es específica de la aplicación ePDG abordada en **D2**, que se refiere a fallas de autenticación. En la presente solicitud, como queda claro en las reivindicaciones modificadas, la autenticación del UE tiene éxito, pero el registro/establecimiento de sesión aún no está permitido porque el UE está intentando establecer el registro/sesión con el 5GCN a través de un acceso no confiable que no es 3GPP. La red y el 5GCN no permiten ningún registro/establecimiento de sesión con el 5GCN a través de redes de acceso no confiables que no sean 3GPP. Como tal, **D2** no describe ni sugiere al menos "recibir, desde uno o más nodos en la red central, en respuesta a la solicitud de autenticación y establecimiento de conexión segura, una indicación de que el establecimiento de conexiones seguras a la red central a través de accesos no confiables no está permitido por la red central " y "proporcionar, al UE, un mensaje de respuesta que comprende una indicación de que la solicitud para establecer la conexión segura no está aprobada porque el establecimiento de una conexión segura a la red central a través de redes de acceso no confiables no está permitido por la red central". Dado que **D1** y **D2** no describen ni sugieren al menos estos mismos elementos de la Reivindicación independiente 1 modificada, se deduce lógicamente que la Reivindicación independiente 1 modificada es novedosa y representa una actividad inventiva con respecto a **D1**, en vista de **D2**.

Basado al menos en las carencias descritas anteriormente de **D1** y **D2**, considerados aislados o en combinación, y dado que el objeto de la Reivindicación 1 independiente modificada es novedoso e implica una actividad inventiva sobre la técnica citada, sostenemos respetuosamente que la Reivindicación 1 supera las objeciones sustantivas.



Las Reivindicaciones independientes 9 y 12 reenumeradas fueron modificadas de manera similar, mutatis mutandis, de modo que se apliquen a cada una de estas reivindicaciones argumentos iguales o similares a los discutidos anteriormente con respecto a la Reivindicación independiente 1 modificada. Como tal, las Reivindicaciones 9 y 12 también son novedosas y representan una actividad inventiva.

Las reivindicaciones dependientes 2-8, 10, 11 y 13-16 (renumeradas) también son novedosas y representan una actividad inventiva sobre **D1**, incluso en vista de **D2**, considerados aislados o en combinación, al menos porque dependen de una de las Reivindicaciones independientes modificadas 1, 9 o 12.

Las nuevas reivindicaciones 17 a 21 también presentan novedad e implican actividad inventiva por al menos razones similares a las analizadas anteriormente con respecto a las reivindicaciones independientes modificadas 1, 9 y 12.

Conclusiones

Con base a las reivindicaciones modificadas y los argumentos anteriores, el Solicitante sostiene respetuosamente que la presente solicitud está en condiciones de ser admitida y solicita respetuosamente la reconsideración de la admisión de la presente solicitud a su debido tiempo.

En consecuencia y luego de haber presentado los argumentos necesarios y haber realizado las modificaciones pertinentes en el capítulo reivindicatorio de la presente invención, queda evidenciado que la invención cumple con los requisitos de patentabilidad definidos en la



Decisión 486 de 2000.

Cordialmente,

Juan Carlos Cuesta Quintero

C.C. 79.339.809 de Bogotá

T.P. 43.273 del C.S. de la J.

Anexos: Comprobante de pago por modificación de la solicitud.
Capítulo reivindicatorio modificado con control de cambios.
Capítulo reivindicatorio modificado en limpio.

REIVINDICACIONES

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~~ una función de gestión de acceso y movilidad (AMF) (202) de la red central 5GCN (100) ~~o más nodos en la red central,~~ 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) ~~en 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) ~~para la red central,~~

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 ~~son~~ 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 ~~ella~~ red central 5GCN (100) a través de la red de acceso no confiable ~~no~~ 3GPP (110) ~~no~~ 3GPP no está aprobada porque el establecimiento de conexión segura a la red central 5GCN (100) a través de redes de acceso no confiables ~~que no son~~ 3GPP

(110) no está permitido por e-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 que no es 3GPP (110) determinar que la red central no acepta el establecimiento de la conexión, y

generar un mensaje de respuesta para el UE, en el que el mensaje de respuesta incluye un error que indica que la red central no permite el establecimiento de la conexión 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 ~~de-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), ~~de-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 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
 5 conexión a redes de acceso 3GPP-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:

10 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
 15 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 5G (5GCN) -(100) no permite el establecimiento de conexión o acceso seguro a la red central 5G-(5GCN) (100) no se permite el acceso a través de redes de acceso no-no-3GPP no confiables no 3GPP (110)a la red central 5G-(5GCN).
 20

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

transmitirle el mensaje de respuesta al UE, en el que el mensaje de respuesta indica que la red central no acepta el establecimiento de la conexión;
 25 tras recibir un mensaje de detención del UE (200); y
 generar un mensaje de fallo para el UE y;
transmitirle el mensaje de fallo al UE (200).

30 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.

5

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 \(100\)](#).

10

~~9. El nodo de función de interfuncionamiento de la reivindicación 1, en el que la red central es una 5GCN y la red de acceso no confiable es una red de acceso no 3GPP.~~

15

~~109.~~ 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

20

un dispositivo de procesamiento [\(1700\)](#) configurado para [al menos:](#)

25

[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 \(110\);](#)

30

[en respuesta a recibir la solicitud de autenticación y establecimiento de 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 del 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 ella red central 5GCN (100) que se establece a través de redes de acceso no confiables que no son 3GPP (110); y

proporcionar el mensaje de respuesta a la función de interfuncionamiento N3IWF (204) a través de la interfaz de red. procesar una solicitud de autenticación y establecimiento de conexión segura para un UE a través de una red de acceso no confiable;

generar una solicitud de verificación de suscripción y autenticación para una función de servidor de autenticación (AUSF);

determinar que una respuesta a la verificación de suscripción y autenticación indica un fallo de autenticación; y

generar un mensaje de respuesta a la autenticación y el establecimiento de una conexión segura encapsulando en el mensaje de respuesta un valor de causa que indique que no se permite el acceso a la red central a través de la red de acceso no confiable.

11. — La AMF de la reivindicación 10, en la que la red de acceso no confiable es una red de acceso no 3GPP y la red central es una red central 5G (5GCN).

1210. La función de gestión de acceso y movilidad AMF (202) de la reivindicación 119, 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).

1311. La función de gestión de acceso y movilidad AMF (202) de la reivindicación

1210, 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.

5 1412. 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:

10 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;

15 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);

20 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);

25 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

30 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).

~~procesar un mensaje de respuesta del nodo de función de interfuncionamiento, y
— determinar, a partir del mensaje de respuesta, que la red central no permite el
establecimiento de una sesión segura a través de la red de acceso no confiable.~~

5 ~~15.— El equipo de usuario de la reivindicación 14, en el que la red de acceso no
confiable es una red de acceso no 3GPP y la red central es una red central 5G (5GCN).~~

~~1613. El equipo de usuario UE (200) de la reivindicación 1512, en el que el dispositivo
de procesamiento (1600) está configurado además para:~~

10 ~~generar un mensaje de detención que indique el fin de la solicitud de registro
para el establecimiento de una sesión segura con la 5GCN y~~

~~transmitirle el mensaje de detención al nodo de función de interfuncionamiento, a
través de la red de acceso no 3GPP.~~

15 ~~1713.~~ El equipo de usuario UE (200) de la reivindicación ~~1612~~, en el que el dispositivo
de procesamiento (1600) está configurado además para:

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.

20

~~1814.~~ El equipo de usuario UE (200) de la reivindicación ~~1713~~, 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

25

realizar un procedimiento de eliminación de la asociación de seguridad.

~~1915.~~ El equipo de usuario UE (200) de la reivindicación ~~1512~~, en el que el dispositivo
de procesamiento (1600) está configurado además para:

30

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); y

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), del nodo de función de interfuncionamiento, el éxito de la segunda solicitud de registro para el establecimiento de sesión segura a la red central 5GCN (100);
establecimiento de la conexión a través de la red de acceso no confiable no 3GPP (110).

2016. El equipo de usuario UE (200) de la reivindicación 1915, 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 ella 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 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 ~~la se permite el acceso a~~ 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 ~~terminar~~ 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 ~~parada~~ detención que comprende un campo de identificador de mensaje que incluye un identificador de ~~parada~~ detención en el campo de identificador de mensaje, indicando el identificador de ~~parada~~ detención que el UE (200) tiene la intención de ~~terminar~~ 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 ~~terminar~~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).

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 ~~establecimiento~~ 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), generando un mensaje de parada de detención que comprende un campo de identificador de mensaje, incluyendo el campo de identificador de mensaje un identificador de parada de detención de 5G ;

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

transmitir el mensaje de detención hacia el nodo de función de interfuncionamiento N3IWF (204) de la red central 5GCN (100) para terminar/ 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 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 parada detención 5G;

5 establecer el identificador de parada detención 5G en el campo de identificador de mensaje del mensaje de parada detención en 5G-Parada; 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)

10 a través de la red de acceso no confiable no 3GPP (110).

REIVINDICACIONES

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 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 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
10 (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).

- 15 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).

- 20 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
25 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
30 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:

5 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:

10 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);

15 en respuesta a recibir la solicitud de autenticación y establecimiento de 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);

20 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

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

30 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).

5

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.

10

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),

15

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;

20

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);

25

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

30

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:

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).

- 5 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.
- 10 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
 - 15 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
 - 20 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;
 - 25 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
 - 30 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 la red central 5GCN (100) a través de cualquier acceso no confiable no 3GPP (110) no está permitida por la red central 5GCN (100).

- 5 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).
- 30 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

5 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;

10 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);

15 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);

20 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

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

30 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:

5 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);

10 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
15 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
20 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
25 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
30 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)

5 (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);

10 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);

15 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);

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

25 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

30 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).



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT: 800.176.089-2

COMPROBANTE DE RECAUDO SISTEMA SIPI

Radicado: NC2021/0000912

Recibo: 21-7306

Fecha: 28/01/2021

TOBOS ABOGADOS SAS

NI: 900.367.556

Pago PSE No: 489881

CUS: 874550513

Patente PCT

MANEJO DE FALLOS DE ACCESO NO 3GPP A UNA 5GCN NO PERMITIDO

Detalle del pago

Id.	Rentístico	Concepto y Servicio	Cant.	Val. Unit.	Subtotal
1	50005-01-01	TRAMITES DE SOL. DE PATENTE DE INVENCION PCT (DESCUENTO INTERNET)	1	\$ 86,000	\$ 86,000
2	50005-01-02	Pago unitario reivindicacion adicional patente de invencion (A partir de de undí½cima reivindicacion) (DESCUENTO INTERNET)	10	\$ 43,500	\$ 435,000
TOTAL					\$ 521,000



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT: 800.176.089-2

COMPROBANTE DE RECAUDO SISTEMA SIPI

Radicado: NC2024/0001870
Recibo: 24-11879
Fecha: 21/02/2024

JUAN CARLOS CUESTA QUINTERO
CC: 79.339.809
Pago PSE No: 932685
CUS: 468611252

NC Modificación a las reivindicaciones
Request on Patente PCT NC2021/0000912

Detalle del pago

Id.	Rentístico	Concepto y Servicio	Cant.	Val. Unit.	Subtotal
1	50005-01-03	Modificaciones / Correcciones al registro Patente PCT (DESCUENTO INTERNET)	1	\$ 215,000	\$ 215,000
TOTAL					\$ 215,000