

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

Señores
TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)

TÍTULO DE LA SOLICITUD: “MANEJO CONTROLADO DE CN DE LA POLÍTICA DE SEGURIDAD PARA LA PROTECCIÓN DEL PLANO DE USUARIO EN LOS SISTEMAS 5G”

NUMERO DE SOLICITUD INTERNACIONAL: PCT/EP2019/058623

FECHA DE PRESENTACIÓN INTERNACIONAL: 5 de abril de 2019.

PRIORIDAD: US (ESTADOS UNIDOS DE AMÉRICA), 62/654,611, 9 de abril de 2018.

Del carácter público de la invención (Art. 40 Decisión 486 de la Comunidad Andina).

Esta Oficina considera importante poner de presente que todas las solicitudes de patentes, así como, los documentos que las conforman tienen el carácter de documento públicos y en consecuencia sobre aquellas no se puede realizar ningún tipo de reserva o guardar confidencialidad, siempre que hayan sucedido alguno de los dos supuestos establecidos por el artículo 40 de la Decisión 486 de 2000 a saber: i) Haber transcurrido dieciocho meses contados a partir de la fecha de presentación de prioridad válidamente invocada, o, ii) Haberse efectuado la publicación de la solicitud de patente, una vez se haya superado el examen de forma de la solicitud.

Siendo así, se tiene que su solicitud fue publicada en la Gaceta de Propiedad Industrial N° 912 del 10 de diciembre de 2020, así como, el hecho de que su solicitud fue presentada a trámite el día 9 de septiembre de 2020, por lo que los supuestos establecidos por el artículo 40 de la Decisión 486 de 2000 se cumple cabalmente y en consecuencia no es dable predicar reserva o confidencialidad alguna sobre la solicitud de patente de invención por Ustedes presentada.

En consecuencia, es imposible mantener el carácter confidencial de los documentos allegados a trámite, dada la marca de agua existente en cada uno de estos que menciona “Confidencial”. Por lo tanto, se le requiere que allegue un nuevo capítulo descriptivo y reivindicatorio sin la inclusión de dicha marca de agua.

Requerimiento por no patentabilidad con fundamento en el artículo 45 de la Decisión 486 de la Comunidad Andina

De otra parte: Como resultado del examen de patentabilidad realizado a la solicitud indicada en la referencia, atendiendo a lo consagrado en el artículo 45 de la Decisión 486 de 2000, se le comunica que esta Dirección ha encontrado que la materia objeto de solicitud no cumple con algunos requisitos establecidos en la Decisión, con fundamento en los siguientes aspectos:

1. Modificaciones presentadas

Revisada la modificación a la solicitud objeto de estudio, la cual fue radicada el 5 de octubre de 2020 bajo el número NC2020/0011164, y teniendo en cuenta lo señalado en el artículo 34 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, esta oficina acepta las modificaciones presentadas por ajustarse a los requisitos legales.

Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

2. Objeto de la invención

El problema planteado consiste en la necesidad de diseñar e implementar una Función de Administración del Acceso y la Movilidad (AMF), una función de administración de sesión (SMF) y métodos asociados en sistemas de comunicaciones.

Para resolver dicho problema técnico, la solicitud en estudio plantea y proporciona un método para operar una Función de administración del acceso y la movilidad (AMF) de un sistema de comunicaciones que comprende un nodo de acceso (AN) configurado para comunicarse a través de una interfaz de aire inalámbrica con equipos de usuario (UE) y que comprende una Función de administración de sesión (SMF). El método incluye la recepción (910) de una indicación de Protección Máxima de la Integridad del Portador de Radio de Datos, DRB-IP, una tasa que indica una capacidad máxima computacional del UE para procesar los DRB que tienen una protección de integridad durante las sesiones de la Unidad de Datos en Paquetes (PDU). Se recibe un mensaje NAS de solicitud de establecimiento de sesión de PDU (920) del UE para establecer una sesión de PDU. Un mensaje de creación de sesión de PDU se comunica (930) hacia la SMF. Se recibe un mensaje de SMF (940) que contiene una indicación de una tasa DRB-IP asignada para los DRB que deben ser protegidos en cuanto a su integridad para una sesión de PDU que se está estableciendo.

3. Reivindicaciones estudiadas

El presente estudio se basa en el capítulo reivindicatorio presentado el 5 de octubre de 2020.

4. De la solicitud de patente

4.1. Título

De conformidad con el literal d) del artículo 27 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, el nombre de la invención de que se trata deberá reflejar el objeto y el campo industrial con el cual se relaciona la misma y ser concordante con la materia descrita y las reivindicaciones de la solicitud. El nombre no podrá referirse a nombres personales, marcas de productos o nombres de fantasía.

El título de la solicitud no refleja el objeto divulgado en la descripción y las reivindicaciones, por lo cual se sugiere el siguiente título: “FUNCIÓN DE ADMINISTRACIÓN DEL ACCESO Y LA MOVILIDAD, FUNCIÓN DE ADMINISTRACIÓN DE SESIÓN Y MÉTODOS ASOCIADO PARA EL MANEJO CONTROLADO DE CN DE LA POLÍTICA DE SEGURIDAD PARA LA PROTECCIÓN DEL PLANO DE USUARIO EN LOS SISTEMAS 5G”.

5. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 9 de abril de 2018, que corresponde a la fecha de presentación de la solicitud de prioridad.

Consultadas las fuentes de información con que se cuenta, se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de publicación
------	-----------	--------	----------------------

Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

D1	ZTE	“Guarantee the UE Max Data Rate for Integrity Protection”	5 de abril de 2018
D2	ZTE Corporation, Sanechips	“Framework for DRB integrity protection”	15 de febrero de 2018

D1¹ divulga la protección de integridad UP para que sea compatible con DRB, NR PDCP para SA y MR-DC@5GC (...) acuerdos relacionados con la tasa de datos de protección de integridad: - Se deja a la red garantizar que no se supere la velocidad de datos admitida por el UE para la protección de la integridad. El UE no especifica el comportamiento cuando la velocidad de datos excede la velocidad admitida. - Señale la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la seguridad del UE capacidad. Esto debe confirmarse con SA3/CT1/RAN3. - El valor más bajo posible para la velocidad de datos es 64 kbps (...) (Introducción).

D2² divulga el marco arquitectónico general aplicable a DRB IP y sugiere capturar el dataRateDRB-IP como una capacidad de seguridad (...) (Introducción, Párr. 4).

6. Examen de Patentabilidad

De acuerdo con lo establecido en el artículo 14 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, en el cual se establecen los requisitos de patentabilidad objeto de la solicitud en estudio, esta Oficina presenta a continuación el análisis de los requisitos de patentabilidad.

6.1. Nivel Inventivo

Teniendo en cuenta lo señalado en el artículo 18 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 1 (NC2020/0011164 del 5 de octubre de 2020) refiere a: *“Una Función de administración del acceso y la movilidad, AMF, de un sistema de comunicaciones que comprende un nodo de acceso (AN) configurado para comunicarse a través de una interfaz de aire inalámbrica con equipos de usuario, UE, y que comprende una Función de administración de sesión, SMF; la AMF comprende: (...)”*. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

Tabla 1.

CARACTERÍSTICAS ESENCIALES	D1	D2
Una Función de administración del acceso y la movilidad, AMF, de un sistema de comunicaciones que comprende.	(...) mensaje recibido en la AMF (...). (Pág. 5).	(...) función que admitirán los UE (...) La política de seguridad del plano de usuario y el perfil de QoS están determinados por SMF (junto con PCF) como se muestra en la Figura 1 (...). (Pág. 1, Párr. 5).
Un nodo de acceso (AN) configurado para comunicarse a través de una interfaz de aire inalámbrica con equipos de usuario, UE.	(...) El nodo fuente NG-RAN estimó la continuidad del servicio para el UE (...). (Pág. 5).	(...) apoyado por la UE. En base a esto (junto con otra información relacionada con los requisitos de velocidad de datos para la

¹ZTE (2018). “Guarantee the UE Max Data Rate for Integrity Protection”. 3GPP Draft; R3-181691 Guarantee the UE Max Data Rate for Integrity Protection v2, 20180405 3rd Generation Partnership Project (3GPP), Mobile Competence Centre; 650, route des Lucioles; F-06921 Sophia-Antipolis Cedex; France. Source info:Vol: RAN WG3, Nr: Sanya, China; 20180416 – 20180420. Recuperado desde: https://www.3gpp.org/ftp/TSG_RAN/WG3_lu/TSGR3_99bis/Docs/R3-181691.zip (Última vez consultado el 15 de agosto de 2023).

²ZTE Corporation, Sanechips (2018). “Framework for DRB integrity protection”. 3GPP Draft; R2-1802049_R2-1800466_upIntegrityCheck, 20180215 3rd Generation Partnership Project (3GPP), Mobile Competence Centre; 650, route des Lucioles; F-06921 Sophia-Antipolis Cedex; France. Source info:Vol: RAN WG2, Nr: Athens, Greece; 20180226 - 20180302. Recuperado desde: https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_101/Docs/R2-1802049.zip (Última vez consultado el 15 de agosto de 2023).



Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

		sesión, etc.), la SMF decidirá si habilitar o no la protección de integridad UP e indicará esta decisión al gNB (...). (Pág. 1, Párr. 5).
Y que comprende una Función de administración de sesión, SMF.	No menciona.	(...) la SMF debe tener el conocimiento necesario sobre la velocidad de datos hasta la cual la protección de integridad es compatible con la UE (...). (Pág. 1, Párr. 5).
La AMF comprende.	(...) mensaje recibido en la AMF (...). (Pág. 5).	No menciona.
Por lo menos un procesador configurado para realizar operaciones que comprenden.	(...) la capacidad del UE de tasa de datos de protección de integridad es un hardware (...). (Pág. 1, Párr. 10). Adicionalmente, por conocimiento del técnico medianamente versado en la materia, un UE cuenta con procesadores.	(...) el UE (...). (Pág. 1, Párr. 1). Adicionalmente, para un técnico medianamente versado en la materia es evidente que los dispositivos de equipo de usuario UE tienen un procesador.
La recepción (910) de una indicación de Protección Máxima de la Integridad del Portador de Radio de Datos, DRB-IP, una tasa que indica una capacidad máxima computacional del UE para procesar los DRB que tienen una protección de integridad durante las sesiones de la unidad de datos en paquetes, PDU, sesiones.	(...) la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la capacidad de seguridad del UE (...). (Pág. 1, Párr. 3). (...) Se ha acordado que la protección de integridad UP sea compatible con DRB (...). (Pág. 1, Párr. 1). (...) En caso de que se establezcan múltiples sesiones de PDU que pertenecen a diferentes segmentos de red para un UE determinado, la política de seguridad UP (es decir, qué sesión de PDU será necesaria para activar la protección de integridad) (...) la tasa de datos habilitada para la integridad a fin de garantizar que no se exceda la capacidad del UE (...). (Pág. 1, Párr. 7).	No menciona.
La recepción (920) de una unidad de datos en paquetes, PDU, estrato de acceso a la red de solicitud de sesión, NAS, mensaje del UE para establecer una sesión de PDU.	(...) conjunto de valores objetivo-recibidos (...). (Pág. 2, Párr. 6). (...) Señalar la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la capacidad de seguridad del UE (...). (Pág. 1, Párr. 3). (...) múltiples sesiones de PDU que pertenecen a diferentes segmentos de red para un UE determinado (...). (Pág. 1, Párr. 7).	No menciona.
La comunicación (930) de un mensaje de creación de sesión de PDU.	(...) el mensaje de AMF contenía sesiones de PDU (...). (Pág. 5).	No menciona.



Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

Hacia la SMF; y.	No menciona.	(...) la SMF debe tener el conocimiento necesario sobre la velocidad de datos hasta la cual la protección de integridad es compatible con la UE (...). (Pág. 1, Párr. 5).
La recepción (940) de un mensaje de SMF.	No menciona.	(...) la SMF debe tener el conocimiento necesario sobre la velocidad de datos hasta la cual la protección de integridad es compatible con la UE (...). (Pág. 1, Párr. 5).
Que contiene una indicación de una tasa DRB-IP asignada para los DRB que deben ser protegidos en cuanto a su integridad para una sesión de PDU que se está estableciendo.	(...) conjunto de valores objetivo-recibidos (...). (Pág. 2, Párr. 6). (...) Señalar la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la capacidad de seguridad del UE (...). (Pág. 1, Párr. 3). (...) Qué sesión de PDU se requerirá para activar la protección de integridad (...). (Pág. 1, Párr. 7).	No menciona.

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 1, ya que divulga la protección de integridad UP para que sea compatible con DRB, NR PDCP para SA y MR-DC@5GC (...) acuerdos relacionados con la tasa de datos de protección de integridad: - Se deja a la red garantizar que no se supere la velocidad de datos admitida por el UE para la protección de la integridad. El UE no especifica el comportamiento cuando la velocidad de datos excede la velocidad admitida. - Señale la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la seguridad del UE capacidad. Esto debe confirmarse con SA3/CT1/RAN3. - El valor más bajo posible para la velocidad de datos es 64 kbps (...) (Introducción).

La diferencia entre la invención definida entre la reivindicación 1 y la función de administración del acceso y la movilidad divulgado en D1, consiste en una función de administración de sesión.

El efecto que se logra al incluir específicamente una función de administración de sesión es asegurar que la tasa asignada no exceda la tasa disponible proporcionada por la AMF en la operación y proporcionar una indicación de la tasa DRB-IP que se asigna a la sesión de PDU.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar la función de administración del acceso y la movilidad divulgada en D1 para asegurar que la tasa asignada no exceda la tasa disponible proporcionada por la AMF en la operación y proporcionar una indicación de la tasa DRB-IP que se asigna a la sesión de PDU?

Sin embargo, el incluir una función de administración de sesión para asegurar que la tasa asignada no exceda la tasa disponible proporcionada por la AMF en la operación y proporcionar una indicación de la tasa DRB-IP que se asigna a la sesión de PDU, ya está divulgado en D2 que se refiere a una función que admitirá los UE (...) La política de seguridad del plano de usuario y el perfil de QoS están determinados por SMF (junto con PCF) como se muestra en la Figura 1 (...) la SMF debe tener el conocimiento necesario



Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

sobre la velocidad de datos hasta la cual la protección de integridad es compatible con la UE (...) (Pág. 1, Párr. 5).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir una función de administración de sesión del D2 en la función de administración de sesión de D1, para así llegar al objeto de la reivindicación 1. Por lo cual se considera obvia.

Teniendo en cuenta lo señalado en el artículo 18 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 16 (NC2020/0011164 del 5 de octubre de 2020) refiere a: “Un método mediante una Función de administración del acceso y la movilidad, AMF, de un sistema de comunicaciones que comprende un nodo de acceso, AN, configurado para comunicarse a través de una interfaz de aire inalámbrica con equipos de usuario, UE, y que comprende una Función de administración de sesión, SMF; el método comprende (...)”. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

Tabla 2.

CARACTERÍSTICAS ESENCIALES	D1	D2
Un método mediante una Función de administración del acceso y la movilidad, AMF, de un sistema de comunicaciones que comprende.	(...) mensaje recibido en la AMF (...). (Pág. 5).	(...) función que admitirán los UE (...) (...) La política de seguridad del plano de usuario y el perfil de QoS están determinados por SMF (junto con PCF) como se muestra en la Figura 1 (...). (Pág. 1, Párr. 5).
Un nodo de acceso, AN, configurado para comunicarse a través de una interfaz de aire inalámbrica con equipos de usuario, UE.	(...) El nodo fuente NG-RAN estimó la continuidad del servicio para el UE (...). (Pág. 5).	(...) apoyado por la UE. En base a esto (junto con otra información relacionada con los requisitos de velocidad de datos para la sesión, etc.), la SMF decidirá si habilitar o no la protección de integridad UP e indicará esta decisión al gNB (...). (Pág. 1, Párr. 5).
Y que comprende una Función de administración de sesión, SMF.	No menciona.	(...) la SMF debe tener el conocimiento necesario sobre la velocidad de datos hasta la cual la protección de integridad es compatible con la UE (...). (Pág. 1, Párr. 5).
El método comprende.	(...) mensaje recibido en la AMF (...). (Pág. 5).	(...) función que admitirán los UE (...) (...) La política de seguridad del plano de usuario y el perfil de QoS están determinados por SMF (junto con PCF) como se muestra en la Figura 1 (...). (Pág. 1, Párr. 5).
La recepción (910) de una indicación de Protección Máxima de la Integridad del Portador de Radio de Datos, DRB-IP, una tasa que indica una capacidad máxima computacional del UE para procesar los DRB que tienen una protección de integridad durante las sesiones de la unidad de datos en paquetes, PDU, sesiones.	(...) la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la capacidad de seguridad del UE (...). (Pág. 1, Párr. 3). (...) Se ha acordado que la protección de integridad UP sea compatible con DRB (...). (Pág. 1, Párr. 1).	No menciona.



Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

	(...) En caso de que se establezcan múltiples sesiones de PDU que pertenecen a diferentes segmentos de red para un UE determinado, la política de seguridad UP (es decir, qué sesión de PDU será necesaria para activar la protección de integridad) (...) la tasa de datos habilitada para la integridad a fin de garantizar que no se exceda la capacidad del UE (...). (Pág. 1, Párr. 7).	
La recepción (920) de una unidad de datos en paquetes, PDU, estrato de acceso a la red de solicitud de sesión, NAS, mensaje del UE para establecer una sesión de PDU.	(...) conjunto de valores objetivo-recibidos (...). (Pág. 2, Párr. 6). (...) Señalar la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la capacidad de seguridad del UE (...). (Pág. 1, Párr. 3). (...) múltiples sesiones de PDU que pertenecen a diferentes segmentos de red para un UE determinado (...). (Pág. 1, Párr. 7).	No menciona.
La comunicación (930) de un mensaje de creación de sesión de PDU.	(...) el mensaje de AMF contenía sesiones de PDU (...). (Pág. 5).	No menciona.
Hacia la SMF; y.	No menciona.	(...) la SMF debe tener el conocimiento necesario sobre la velocidad de datos hasta la cual la protección de integridad es compatible con la UE (...). (Pág. 1, Párr. 5).
La recepción (940) de un mensaje de SMF.	No menciona.	(...) la SMF debe tener el conocimiento necesario sobre la velocidad de datos hasta la cual la protección de integridad es compatible con la UE (...). (Pág. 1, Párr. 5).
Que contiene una indicación de una tasa DRB-IP asignada para los DRB que deben ser protegidos en cuanto a su integridad para una sesión de PDU que se está estableciendo.	(...) conjunto de valores objetivo-recibidos (...). (Pág. 2, Párr. 6). (...) Señalar la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la capacidad de seguridad del UE (...). (Pág. 1, Párr. 3). (...) Qué sesión de PDU se requerirá para activar la protección de integridad (...). (Pág. 1, Párr. 7).	No menciona.

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 16, ya que divulga la protección de integridad UP para que sea compatible con DRB, NR PDCP para SA y MR-DC@5GC (...) acuerdos relacionados con la tasa de datos de protección de integridad: - Se deja a la red garantizar que no se supere la velocidad de datos admitida por el UE para la protección de la integridad. El UE no

Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

especifica el comportamiento cuando la velocidad de datos excede la velocidad admitida.
- Señale la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la seguridad del UE capacidad. Esto debe confirmarse con SA3/CT1/RAN3. - El valor más bajo posible para la velocidad de datos es 64 kbps (...) (Introducción).

La diferencia entre la invención definida entre la reivindicación 16 y el método mediante la función de administración del acceso y la movilidad divulgado en D1, consiste en una función de administración de sesión.

El efecto que se logra al incluir específicamente una función de administración de sesión es asegurar que la tasa asignada no exceda la tasa disponible proporcionada por la AMF en la operación y proporcionar una indicación de la tasa DRB-IP que se asigna a la sesión de PDU.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar el método mediante la función de administración del acceso y la movilidad divulgado en D1 para asegurar que la tasa asignada no exceda la tasa disponible proporcionada por la AMF en la operación y proporcionar una indicación de la tasa DRB-IP que se asigna a la sesión de PDU?

Sin embargo, el incluir una función de administración de sesión para asegurar que la tasa asignada no exceda la tasa disponible proporcionada por la AMF en la operación y proporcionar una indicación de la tasa DRB-IP que se asigna a la sesión de PDU, ya está divulgado en D2 que se refiere a una función que admitirán los UE (...) La política de seguridad del plano de usuario y el perfil de QoS están determinados por SMF (junto con PCF) como se muestra en la Figura 1 (...) la SMF debe tener el conocimiento necesario sobre la velocidad de datos hasta la cual la protección de integridad es compatible con la UE (...) (Pág. 1, Párr. 5).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir una función de administración de sesión del D2 en el método mediante la función de administración de sesión de D1, para así llegar al objeto de la reivindicación 16. Por lo cual se considera obvia.

Así mismo, D1 divulga las características de las reivindicaciones dependientes de la siguiente manera:

- Reivindicación 18: (...) mensaje recibido en la AMF (...). (Pág. 5). (...) El nodo fuente NG-RAN estimó la continuidad del servicio para el UE (...) (Pág. 5). (...) la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la capacidad de seguridad del UE (...). (Pág. 1, Párr. 3). (...) Se ha acordado que la protección de integridad UP sea compatible con DRB (...) (Pág. 1, Párr. 1). (...) En caso de que se establezcan múltiples sesiones de PDU que pertenecen a diferentes segmentos de red para un UE determinado, la política de seguridad UP (es decir, qué sesión de PDU será necesaria para activar la protección de integridad) (...) la tasa de datos habilitada para la integridad a fin de garantizar que no se exceda la capacidad del UE (...) (Pág. 1, Párr. 7). (...) conjunto de valores objetivo-recibidos (...) (Pág. 2, Párr. 6). (...) Señalar la capacidad del UE para la velocidad de datos máxima admitida para DRB IP en NAS como parte del resto de la capacidad de seguridad del UE (...) (Pág. 1, Párr. 3). (...) múltiples sesiones de PDU que pertenecen a diferentes segmentos de red para un UE determinado (...) (Pág. 1, Párr. 7). (...) conjunto de valores objetivo-recibidos (...) (Pág. 2, Párr. 6). (...) Qué sesión de PDU se requerirá para activar la protección de integridad (...) (Pág. 1, Párr. 7).

Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

La reivindicación dependiente 18 no menciona alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al método de la reivindicación 16, por lo cual se considera que carece de nivel inventivo.

7. Conclusión

Los requisitos de Patentabilidad de la presente solicitud están afectados así:

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	ZTE	1, 16 y 18	Nivel inventivo
D2	ZTE Corporation, Sanechips	1 y 16	Nivel inventivo

En cumplimiento del artículo 45 de la Decisión 486 de 2000, se le indica que debe dar respuesta dentro del término de sesenta (60) días contados a partir de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Si como respuesta a este requerimiento, el solicitante modifica el capítulo reivindicatorio, deberá observar las instrucciones contenidas en el numeral 1.2.2.1.1., del Capítulo Primero del Título X de la Circular Única de esta Superintendencia. De igual forma, deberá tener presente que de conformidad con el literal a) del numeral 1.2.2.5.1. de la norma ibidem, será necesario acreditar el pago de la tasa por concepto de modificación a solicitudes en trámites, de conformidad con el valor establecido en la resolución de tasas vigentes.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 6.2 del Capítulo Sexto del Título I de la Circular Única, informándoles que contra el mismo no procede recurso alguno en actuación administrativa.



Edna Marcela Ramirez Orozco
DIRECTORA DE NUEVAS CREACIONES

Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2020/0011164		1°	X	2°		3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/EP2019/058623		5 de abril de 2019							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
9/04/2018				X					
Solicitante									
TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)									
Reivindicaciones que no son objeto de búsqueda por:									
Art. 14	-	Art. 15	-	Art. 20	-	Art. 25 (Falta de unidad de invención)		-	
CRITERIOS DE BÚSQUEDA									
Reivindicaciones objeto de búsqueda				1 a 25					
Palabras clave utilizadas				AMF, PDU, SMF, security, policy, protection, 5G, session, DRB, access, mobility, wireless, interface					
Clasificaciones utilizadas para la búsqueda				CIP:	H04W 12/10, H04L 29/06, H04W 8/22				
DOCUMENTOS CONSIDERADOS RELEVANTES (Documentos patente, Literatura no patente (LNP): Artículos, catálogos, etc.)									
Informes de búsqueda / Bases de datos consultadas	N° de solicitud de patente / N° de patente / Autor LNP ⁽¹⁾	Fecha de Publicación /Presentación (DD/MM/AAAA)	Reivindicaciones /Secuencias afectadas	Citas relevantes del estado de la técnica			Categoría del documento citado ⁽²⁾		
SIPI	NC2022/0004053	19/04/2022	-	-			E		
WIPO	ZTE ¹	5/04/2018	1, 16 y 18	1 Pág. 5; Pág. 1, Párr. 10; Pág. 1, Párr. 3; Pág. 1, Párr. 1; Pág. 1, Párr. 7; Pág. 2, Párr. 6; Pág. 1, Párr. 3; Pág. 1, Párr. 7; Pág. 2, Párr. 6.			Y		
				16 Pág. 5; Pág. 1, Párr. 10; Pág. 1, Párr. 3; Pág. 1, Párr. 1; Pág. 1, Párr. 7; Pág. 2, Párr. 6; Pág. 1, Párr. 3; Pág. 1, Párr. 7; Pág. 2, Párr. 6.					
				18 Pág. 5; Pág. 1, Párr. 10; Pág. 1, Párr. 3; Pág. 1, Párr. 1; Pág. 1, Párr. 7; Pág. 2, Párr. 6; Pág. 1, Párr. 3; Pág. 1, Párr. 7; Pág. 2, Párr. 6.					
	Intel Corporation ²	7/04/2018	-	-			A		
	ZTE Corporation, Sanechips ³	15/02/2018	1 y 16	1 Pág. 1, Párr. 5.			Y		
				16 Pág. 1, Párr. 5.					
USPTO	US2019260811	22/08/2019	-	-			E		
	US2020322804	8/10/2020	-	-			E		
	US2021084130	18/03/2021	-	-			E		
Patbase	US2022286895	08/09/2022	-	-			E		
Googlepatent	US20220345889	27/10/2022	-	-			E		



Oficio N° 15830 de 28 de septiembre de 2023

Ref. Expediente N° NC2020/0011164

(¹) Cita completa literatura no patente (LNP) Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Volumen(Número), pp-pp. O Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Recuperado de http://xxxxxxx.	¹ ZTE (2018). “Guarantee the UE Max Data Rate for Integrity Protection”. 3GPP Draft; R3-181691 Guarantee the UE Max Data Rate for Integrity Protection v2, 20180405 3rd Generation Partnership Project (3GPP), Mobile Competence Centre; 650, route des Lucioles; F-06921 Sophia-Antipolis Cedex; France. Source info:Vol: RAN WG3, Nr: Sanya, China; 20180416 – 20180420. Recuperado desde: https://www.3gpp.org/ftp/TSG_RAN/WG3_lu/TSGR3_99bis/Docs/R3-181691.zip (Última vez consultado el 15 de agosto de 2023).
	² Intel Corporation, Sanechips (2018). “Support for UE capability related to integrity protection of DRBs”. 3GPP Draft; R3-182295_UEcap_DRB-IP (vS), 20180407 3rd Generation Partnership Project (3GPP), Mobile Competence Centre; 650, route des Lucioles; F-06921 Sophia-Antipolis Cedex; France. Source info:Vol: RAN WG3, Nr: Sanya, China; 20180416 – 20180420. Recuperado desde: https://www.3gpp.org/ftp/tsg_ran/WG3_lu/TSGR3_99bis/Docs/R3-182295.zip (Última vez consultado el 15 de agosto de 2023).
	³ ZTE Corporation, Sanechips (2018). “Framework for DRB integrity protection”. 3GPP Draft; R2-1802049_R2-1800466_uplIntegrityCheck, 20180215 3rd Generation Partnership Project (3GPP), Mobile Competence Centre; 650, route des Lucioles; F-06921 Sophia-Antipolis Cedex; France. Source info:Vol: RAN WG2, Nr: Athens, Greece; 20180226 - 20180302. Recuperado desde: https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_101/Docs/R2-1802049.zip (Última vez consultado el 15 de agosto de 2023).
(²) Categorías de documentos citados	
“A” Documento que define el estado general de la técnica no considerado como particularmente relevante. “E” Solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior. “L” Documento citado para llamar la atención sobre por ejemplo, dudas acerca de una reivindicación de prioridad o para determinar la fecha de publicación de otra cita, siempre van acompañados de una explicación, por la cual se citan. “O” Documento del tipo actas de conferencia, este tipo de documentos siempre estará acompañado por otra letra que indique la pertinencia del documento, por ejemplo, O,X, O,Y o bien O,A. “P” Documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.	“T” Documento publicado en fecha posterior a la de presentación o la de prioridad de la solicitud internacional y no entra en conflicto con dicha solicitud, pero puede ser útil para la mejor comprensión del principio o teoría en que se basa la invención, o para demostrar que el razonamiento o los hechos en los que se basa dicha invención son incorrectos. “X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado. “Y” Documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.
Fecha del reporte de búsqueda: (15/08/2023)	

