

HUMBERTO RUBIO & CIA.

ABOGADOS

Cra. 7 # 74 – 64 Oficina 506
Tel: (571) 3132408 – 3132423 - 3132410 - 3131759
Fax: (571) 3131647 - 3132367
E-mail: mail@rubiolawyers.com
Apartado 1000
Bogotá

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 10-012466-00006-0000

Fecha: 2013-02-22 14:18:56
Tra. 11 PATENTE IYII
Act. 523 RESPUESTA

Dep. 2020 DIR.NUEVASCR
Eve: 378 FASENACIONALI
Folios: 26

Doctor

JOSE LUIS SALAZAR LOPEZ

Jefe División de Nuevas Creaciones (C)

Superintendencia de Industria y Comercio

E. S. D.

REF:	Expediente No.	10-012466
	Patente de Invención:	"METODO Y DISPOSICION PARA ESTABLECER UNA CLAVE DE SEGURIDAD"
	PCT:	PCT/SE2008/050591
	Clasificación Int.:	H 04 I 9/20
	Titular:	Telefonaktiebolaget L M Ericsson (publ)

RESPUESTA A REQUERIMIENTO

OFICIO No. 21962 NOTIFICADO POR FIJACION EN LISTA DE 4 DE DICIEMBRE DE 2012

HUMBERTO RUBIO CAMACHO, mayor de edad, domiciliado en Bogotá, D.C., identificado con la cédula de ciudadanía número 17'192.062 de Bogotá, abogado graduado portador de la Tarjeta Profesional No. 50.007 expedida por el Consejo Superior de la Judicatura, actuando en carácter de **Apoderado de Telefonaktiebolaget L M Ericsson (publ)**., domiciliada en SE-164 83, Estocolmo, Suecia, debidamente reconocido por su Despacho, encontrándome dentro de la debida oportunidad procesal para dar respuesta al auto proferido por su Despacho, mediante Oficio No.21962 notificado por fijación en lista de 4 de diciembre de 2012, me permito:

Manifestar:

I.- En el informe emitido sobre la presente invención, se han formulado las objeciones que a continuación resumimos:

a. No es una invención (Art 15 D 486 literal (e))

El objeto de las reivindicaciones 1 a 23 no se considera una invención, de acuerdo con el artículo citado, en el que se especifican los programas de ordenadores o el soporte lógico, como tal.

El objeto de la solicitud debe dirigirse a una de las dos categorías de la materia patentable: productos o procedimientos. Se debe tener en cuenta que un procedimiento es un acto o una serie de actos o pasos, que están vinculados a una determinada máquina, aparato ó dispositivo, o a la transformación de un artículo en particular a un estado u objeto diferente. También llamado Método ó Proceso. Por su parte, una máquina es un objeto concreto, tangible, que consta de partes, o de ciertos dispositivos y por la combinación e

interacción de dichos dispositivos. Esto incluye todos los dispositivos mecánicos, o una combinación de fuerzas mecánicas y dispositivos para realizar alguna función y producir un determinado efecto o resultado.

Si la materia reclamada, siendo dicha materia una excepción a la patentabilidad, es limitada en su aplicación a una determinada aplicación práctica, puede llegar a ser elegible a estudio. Para aclarar este concepto, una aplicación práctica se refiere a cómo materia no patentable, puede ser aplicada en un producto o un proceso real. Es decir, cuando la materia no patentable se reduce a una aplicación práctica particular, teniendo un uso real, entonces, la aplicación práctica reivindicada evidencia que la materia reclamada ya no es abstracta, ni puramente mental y no abarca sustancialmente todos los usos posibles de una ley de la naturaleza o un fenómeno natural.

En el caso de las categorías de producto, una aplicación práctica particular es generalmente evidente, cuando está basada en las limitaciones de la reivindicación que definan su campo particular tangible. En otras palabras, una aplicación práctica particular es una idea aplicada tangiblemente a una estructural no abstracta, es decir, cuando una ley de la naturaleza o fenómeno natural se aplica en forma práctica a una estructura, quedando la idea limitada a una aplicación particular.

Una reivindicación que incluya términos que impliquen que la invención está dirigida a un producto, por ejemplo, "una máquina que comprende...", pero que no incluya limitaciones tangibles de acuerdo con su interpretación más amplia razonable, no estará limitada a una aplicación práctica, sino más bien abarca o comprende el concepto total en el cual la invención está basada. Dicha reivindicación no es aceptable, porque dicha materia reclamada se extendería a cubrir todos los aspectos de la aplicación de la idea abstracta, ley de la naturaleza o fenómeno natural. La materia descrita debe ser evaluada para determinar si la materia tiene una relación funcional con la estructura subyacente, a fin de evaluar si se crea una distinción patentable sobre el estado de la técnica o si es simplemente materia no funcional descrita que no crea ninguna distinción patentable.

Los siguientes ejemplos enseñan la diferencia entre una realización tangible mostrando una aplicación práctica en particular y un concepto abstracto que no tiene aplicación práctica.

(A) Una reivindicación dirigida a una máquina, compuesta por una pluralidad de elementos estructurales que trabajen en conjunto en una disposición específica, basada en una relación matemática, tales como una serie de engranajes, poleas y correas, tendrá limitaciones estructurales mostrando ser un objeto tangible y aportando evidencia, que la relación matemática, se ha aplicado como una aplicación práctica. Además, esa materialización tangible se ve limitada por la conformación estructural reclamada y no abarcaría todos los usos prácticos posibles en la aplicación de dicha relación matemática. Así pues, la reivindicación sería materia elegible para estudio de patentabilidad.

(B) Por otra parte, una reivindicación dirigida a una máquina, definida como "Una máquina que funciona de acuerdo a $F=m*a$ ", pero que no incluya elementos estructurales tangibles en su interpretación más amplia razonable, abarcaría un principio de operación basado en una relación matemática donde el alcance de la reivindicación no tendría un límite. Por lo tanto, se estaría reclamando un objeto no tangible, sin evidencia de estar ante una aplicación práctica. No habría pruebas de una aplicación práctica.

Para ser aceptada una reivindicación de procedimiento, como materia elegible para estudio, debe pasar la prueba de patentabilidad, la cual asegura que el proceso se limita a una aplicación práctica en particular y, que no sea: una idea abstracta, un proceso mental o todas las aplicaciones posibles prácticas de una ley de la naturaleza o un fenómeno natural. Por lo tanto, no todos los métodos califican de ser aceptados como materia elegible a estudio de patentabilidad.

De acuerdo con lo anterior, el procedimiento reivindicado deberá: (1) estar vinculado a una determinada máquina, aparato o dispositivo, y (2) ser una transformación específica de un artículo determinado a un estado u objeto diferente. Se debe tener en cuenta, que un método reclamado que no requiera la aplicación de una máquina, o no cause una transformación específica de un artículo determinado a un estado u objeto diferente, no pasará la prueba y deberá ser rechazado.

Por otra parte, la sola presencia de un vínculo con una máquina o con una transformación, no es suficiente para pasar la prueba. Cuando se ha identificado el vínculo con una máquina o con una transformación, se deberá también determinar que dicho vínculo es con una máquina en particular, o con la transformación en particular de un artículo específico.

Además, la máquina o la transformación particular vinculada, debe cumplir con dos requisitos para pasar la prueba de materia elegible a estudio de patentabilidad: En primer lugar, el uso de una máquina particular o la transformación de un artículo particular, debe definir un límite significativo para el alcance de la reclamación. Por lo tanto, el hecho de tener una máquina vinculada a un único campo de actividad, podría no ser suficiente. En segundo lugar, el uso de la máquina particular o la transformación del objeto particular, debe implicar más que una actividad insignificante extra a la solución.

Una actividad insignificante extra a la solución, significa una actividad que no es fundamental para el objetivo del método inventado por el solicitante. Por ejemplo, la recopilación de datos para uso en un procedimiento, cuando todas las aplicaciones del procedimiento que requirieran alguna forma de recopilación de datos, no definieran un límite significativo en el alcance de la reivindicación.

Si la máquina o la transformación sólo está presente en una limitación del campo de uso o en un paso que sólo es una actividad insignificante extra a la solución, el método reclamado no supera la prueba, a pesar de la presencia de una máquina o una transformación en la reivindicación.

En conclusión, los métodos de las reivindicaciones 1 a 6 y 7 a 12 no son elegibles como materia patentable debido a que no se identifica un vínculo con una máquina en particular y los dispositivos de las reivindicaciones 13 a 17 y 18 a 23 no son elegibles como materia patentable dado que no se encuentran caracterizados por sus características técnicas esenciales sino por su funcionalidad, la cual es producto de un software.

b. De la Solicitud de Patente

Reivindicaciones (Art 30 D 486, Art 22 PCT)

Se le sugiere al solicitante que indique al frente de la característica o del elemento, el número de referencia guardando correspondencia con el capítulo descriptivo, las gráficas o

dibujos y dicho capítulo reivindicatorio, con el objetivo de comprender mejor la invención al momento de hacer el análisis y distinguir los elementos de dicha invención.

Las reivindicaciones 13 y 18 no son claras porque mencionan: “medios”, siendo una frase de carácter general que sugiere de forma imprecisa que la protección se extiende a otras posibles variaciones o modificaciones. Se sugiere definir un rango preciso de dichos medios.

Las reivindicaciones 13 a 23 no son claras porque indican el uso que puede darse al producto reivindicado, el cual no es una característica técnica que defina a la invención. Lo anterior, según los siguientes fragmentos: “...para recibir una SOLICITUD DE SERVICIO NAS del UE, solicitud que indica un número de secuencia NAS de enlace ascendente, NAS_U_SEQ... para derivar a K_eNB de al menos dicho NAS_U_SEQ recibido y de una clave de Entidad de Administración de Acceso de Seguridad almacenada, K_ASME, compartida con dicho UE... para enviar dicho K_eNB derivado al eNodeB que presta servicio a dicho UE.”, “...para derivar el K_eNB del NAS_U_SEQ y el K_ASME usando una Función Seudo-Aleatoria, PRF.”, “...dispuesta para reconstruir el número de secuencia completo NAS de enlace ascendente NAS_U_SEQ de los bits de bajo orden recibidos.”, “...dispuesta para comprobar la integridad la Solicitud de Servicio NAS recibida del UE (11).”, “...dispuesta para reenviar (54) una indicación del NAS_U_SEQ al eNodeB (12), para ser regresada (55) al UE (11) del eNodeB.”, “...para enviar una SOLICITUD DE SERVICIO NAS a una MME (13), solicitud que indica un número de secuencias NAS de enlace ascendente, NAS_U_SEQ...” , “...para derivar un K_eNB de al menos dicho NAS_U_SEQ, y de una clave de Entidad de Administración de Acceso de Seguridad almacenada, K_ASME, compartida con dicha MME (13).”, “... dispuesto para derivar el K_eNB de el NAS_U_SEQ y el K_ASME usando una Función Seudo-Aleatoria, PRF.”, “...dispuesto para proteger la integridad de la Solicitud de Servicio NAS enviada a la MME (13).”, “...dispuesto para almacenar el NAS_U_SEQ de la Solicitud de Servicio NAS enviado a la MME (13).”, “...dispuesto para recibir una indicación del NAS_U_SEQ del Servicio NAS. Solicitud enviada a la MME (13), de regreso de la MME por medio del eNodeB (12).”, “...dispuesto para derivar el K_eNB después de la recepción de un mensaje de configuración de seguridad del eNodeB (12).”. Se sugiere realizar las aclaraciones respectivas.

Las reivindicaciones 1, 7 y 13 no son claras porque el término: “al menos”, es impreciso, por lo cual no permite distinguir la invención del estado de la técnica. Se sugiere sustituirlo por un término preciso o un rango concreto.

Descripción (Art 28 D 486)

Error en la digitación, redacción y/o traducción de la descripción, según los siguientes fragmentos: “...entre la MME dl Núcleo de Paquetes Evolucionados...” (Fl. 11, línea 21), “...los números de secuencia se usan para evitarla repetición de mensajes viejos...” (Fl. 11, líneas 25 y 26), “...para la protección del trafico UP/RRC entre el UE y su eNobeB de servicio...” (Fl. 12, línea 8), “...En la señal SI y S2...” (Fl. 12, líneas 13 y 14), “...de un Sistema de Paquetes Evolucionado, EPC...” (Fl. 13, línea 28), “...número de secuencia NAS de enlace ascendente, NAS_U_SEQ; Derivar la clave...” (Fl. 13, línea 32), “...El concepto of la invención...” (Fl. 16, línea 20), “...De ahí en adelante, el eNodeB y el UE establecerá el contexto de seguridad...” (Fl. 17, líneas 11 y 11), “...del mensaje inicial del SOLICITUD DE SERVICIO NAS, en al señal S21...” (Fl. 17, línea 25), “...o solo bits de bajo orden que indica el NAS_U_SEQ, y derive el K_eNB...” (Fl. 17, línea 27), “...En el paso 35, dicho UE derivará el mismo K_eNB... y establecer el contexto de seguridad...” (Fl. 18, líneas 18 a 20). Se sugiere al solicitante hacer las aclaraciones necesarias.

Hay inconsistencia entre los números de referencia de los dibujos (Fl. 28) y la descripción (Fl. 19 línea 3). Se sugiere realizar la corrección correspondiente.

c. Determinación del Estado de la Técnica

El estado de la técnica se determinó con base en la fecha de presentación de la solicitud de prioridad: septiembre 17 de 2007 y se encontró el siguiente documento que anticipa el objeto de esta solicitud:

D1: US 2007/011550 "Rank step-down for MIMO SCW design employing HARQ"

El documento D1 divulga sistemas y metodologías que facilitan a reducir el rango de un número de transmisiones que van en aumento (Pág. 1, resumen).

d. Examen de Patentabilidad (Art 14 D 486)

Novedad (Art 16 D486)

La reivindicación 13 consiste en: "Una entidad de administración de movilidad (13), MME, adaptada para un Sistema de Paquetes Evolucionado, EPS, la MME que se dispone para establecer una clave de seguridad, K_eNB, para la protección del tráfico RRC/UP entre un UE (11) y un eNodeB (12) que presta servicio al UE, donde la MME se caracteriza por..." (Fl. 22).

De acuerdo con la tabla comparativa del examen de patentabilidad, las características esenciales de la Entidad de Administración de Movilidad (MME) de la reivindicación 13, habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

El documento D1 además revela un transmisor (824) que transmite a uno o más dispositivos de usuario (804) a través de antenas transmisoras (808) (Pág. 7, Párr. 76, Fig. 8).

En consecuencia, la reivindicación 13 no es nueva, según lo divulgado en el documento D1.

Las reivindicaciones dependientes 14 a 17 no mencionan alguna característica que haga nueva a la MME de la reivindicación 13, por lo cual se considera que no son nuevas.

Por otra parte, el equipo de usuario reclamado en la solicitud no es nuevo, teniendo en cuenta que, la reivindicación 18 consiste en: "Un equipo de usuario (11), UE, adaptado para un Sistema de Paquetes Evolucionado, EPS, UE que se dispone para establecer una clave de seguridad, K_eNB, para proteger el tráfico RRC/UP intercambiado con un eNodeB de servicio (12), UE que se caracteriza por..." (Fl. 23).

Comparación de las características técnicas esenciales, con las del Estado de la Técnica:

De acuerdo con la tabla comparativa del examen de patentabilidad, las características esenciales del equipo de usuario (UE) de la reivindicación 18, habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

En consecuencia, la reivindicación 18 no es nueva, según lo divulgado en el documento D1.

Las reivindicaciones dependientes 19 a 23 no mencionan alguna característica que haga nuevo al equipo de usuario de la reivindicación 18, por lo cual se considera que no son nuevas.

f. Conclusión

Los requisitos de Patentabilidad de la presente solicitud están afectados por las objeciones de los numerales 4 y 5, de la siguiente manera:

El documento D1 afecta en cuanto a la novedad y el nivel inventivo las reivindicaciones de la 13 a la 23.

II.- En contestación a las observaciones anteriores, manifestamos lo siguiente:

a. No es una invención (Art 15 D 486 literal (e))

El examinador considera que el objeto de las reivindicaciones 1 a 23 no es una invención de conformidad con el artículo citado, el cual se refiere a programas de ordenadores o soporte lógico, como tal.

El solicitante considera que la presente invención no es simplemente un programa de ordenador, sino que implica una aplicación particular práctica, al menos en el sentido de que el método reivindicado se implementa en un nodo físico (la MME y el UE, respectivamente) y en que esta afecta el mundo físico, por ejemplo mediante la influencia de señales de radio que se transmiten a través del aire.

En particular, las reivindicaciones del MME se dirigen al nodo físico en sí, que está configurado para realizar el método reivindicado.

Entendemos que la presente invención justamente cae dentro de la concepción de la materia que puede considerarse patentable, ya que la misma se limita en su aplicación a una determinada aplicación práctica particular, pues se aplica a productos o procesos reales. Es decir, consideramos que la materia reclamada no es abstracta, ni puramente mental y no abarca sustancialmente todos los usos posibles de una ley de la naturaleza o un fenómeno natural.

Por consiguiente, entendemos que esta objeción del examinador se debe reconsiderar.

b. De la Solicitud de Patente

Reivindicaciones (Art 30 D 486, Art 22 PCT)

En cuanto a la observación que para cada característica o elemento que aparece en las reivindicaciones se debe incluir el número de referencia correspondiente como aparece en el capítulo descriptivo y los dibujos para la mejor comprensión de la invención al momento de hacer el análisis y distinguir los elementos de dicha de la invención, en el documento de descripción y en el capítulo reivindicatorio que se adjuntan a esta respuesta esta deficiencia se ha superado, incluyendo la respectiva numeración para el equipo de usuario UE (11), la Entidad de Administración de Movilidad MME (13) y el eNodeB (12) que presta servicio al UE (11), según se solicita.

En relación a la objeción de que las reivindicaciones 13 y 18 no son claras porque mencionan: "medios", siendo una frase de carácter general que sugiere de forma imprecisa

que la protección se extiende a otras posibles variaciones o modificaciones, discrepamos respetuosamente de la misma, ya que utilizar en las reivindicaciones una expresión de "medios más función", es una forma usual de reivindicar este tipo de objeto de invención, lo cual está expresamente permitido en nuestra práctica según aparece en el **Manual para el Examen de Solicitudes de Patentes de Invención en las Oficinas de Propiedad Industrial de los Países de la Comunidad Andina**, preparado por la Oficina Internacional de la OMPI (Public. 2004), en su página 35, acápite 4.2, cuando se refiere al contenido de las reivindicaciones, se plantea lo siguiente:

4.2 Contenido de las reivindicaciones

Las reivindicaciones deben contener todas las características técnicas esenciales de la invención las cuales definen a la invención y la hacen o pudieran hacerla distintiva del estado de la técnica. Estas características esenciales definen la solución al problema técnico que intenta resolver la invención.

Para efectos del examen, no se toma en cuenta como característica técnica de la invención la inclusión de términos relativos a aspectos no técnicos, como por ejemplo las ventajas comerciales, dado que el resultado o fin alcanzado de la invención no es una característica esencial a estos efectos. Sin perjuicio de ello, la inclusión de elementos no técnicos pueden afectar la claridad de la reivindicación.

Una reivindicación debe incluir no solamente una enumeración de elementos, sino también indicar su funcionamiento y la relación funcional entre los mismos cuando para la persona versada en la materia ello no se desprenda de forma obvia de la misma definición del elemento.

Las características pueden ser estructurales (forma de una pieza, fórmula química, etc.) o funcionales (del tipo: elemento, medios o pieza para hacer una función, por ejemplo "elemento para medir la presión").

Por ejemplo, en el INSTRUCTIVO PARA EL EXAMEN DE SOLICITUDES DE PATENTES DE INVENCION Y MODELO DE UTILIDAD, recientemente publicado por la SIC, en su página 111, se incluye el siguiente ejemplo:

INSTRUCTIVO EXAMEN DE SOLICITUDES DE PATENTES DE INVENCION Y MODELO DE UTILIDAD

Código: PI02-I06

Revisión: Versión inicial

Página 111 de 152

Estado de la Técnica más cercano GB 953617 A

Diferencia Medios de calefacción con una alta producción de calor.

Medios de calefacción con alta producción de calor.

Efecto Técnico Los medios de calefacción con alta producción de calor atraen a los cerditos y los medios de calefacción con baja producción de calor protegen a la madre del estrés calorífico.

Problema solucionado ¿Cómo modificar el corral de GB 953617 A para atraer a los cerditos y que al mismo tiempo la madre no padezca estrés calorífico?

¿Es obvio? No

Los elementos técnicos distintivos de la reivindicación 7, en relación con el documento GB 953617 A son los medios de calefacción con una alta producción de calor y los medios de calefacción con una baja producción de calor.

GB 953617 A no sugiere los medios de calefacción con alta producción de calor con el fin de atraer a los cerditos, proporcionarles calor, condiciones favorables para su supervivencia, viabilidad, y al mismo tiempo,

los medios de calefacción con baja producción de calor para proteger a la madre de estrés calorífico.

La reivindicación 7 es inventiva a la vista del documento GB 953617 A, siguiendo el "método problema solución".

En consecuencia, si en la explicación de uno de los ejemplos del manual de examen preparado por esa autoridad se utiliza esta expresión y fácilmente se distingue la invención del estado de la técnica, no entendemos por qué el examinador objeta que en la presente invención este tipo de expresión no puede utilizarse.

Por otra parte el examinador también considera que las reivindicaciones 13 a 23 no son claras porque indican el uso que puede darse al producto reivindicado, el cual no es una característica técnica que defina a la invención, respetuosamente discrepamos también de esta objeción, ya que el examinador debe entender que las invenciones en campos avanzados como el de las telecomunicaciones como el caso que nos ocupa, están más relacionadas con los tipos de funciones realizadas por los diferentes elementos que conforman estos sistemas de comunicaciones o por su utilización para desempeñar una función determinada, que con la estructura física mediante la cual se implementan cada una de dichas funciones.

Si se consideran otras invenciones pertenecientes a este campo técnico, y particularmente a las clasificaciones internacionales de patentes con las cuales se relaciona la invención, a saber la H04L 9/20, se podrá verificar que las reivindicaciones de las mismas se definen en términos similares a los de la presente invención. Pedimos al examinador que nos ponga un ejemplo de este tipo de invención donde las características de la invención se definan en términos diferentes a los de las reivindicaciones de la presente solicitud, según las exigencias que parecen en el examen de patentabilidad.

En cuanto a la objeción de que las reivindicaciones 1, 7 y 13 no son claras porque el término "al menos", es impreciso, por lo cual no permite distinguir la invención del estado de la técnica, aunque no estamos de acuerdo con esta apreciación, en aras de expedir el examen de esta solicitud, eliminamos el mismo de las nuevas reivindicaciones que se adjuntan.

Descripción (Art 28 D 486)

En cuanto a los errores de digitación señalados por el examinador en el capítulo descriptivo, en el nuevo documento que se adjunta, los mismos se han rectificado.

c. Determinación del Estado de la Técnica

El examinador ha citado el documento D1: US 2007/011550 como relevante para la patentabilidad de la presente invención.

d. Examen de Patentabilidad (Art 14 D 486)

Novedad (Art 16 D486)

La reivindicación 13 consiste en: "Una entidad de administración de movilidad (13), MME, adaptada para un Sistema de Paquetes Evolucionado, EPS, la MME que se dispone para establecer una clave de seguridad, K_eNB, para la protección del tráfico RRC/UP entre un UE (11) y un eNodeB (12) que presta servicio al UE, donde la MME se caracteriza por..." (Fl. 22).

De acuerdo con la tabla comparativa del examen de patentabilidad, el examinador concluye que las características esenciales de la Entidad de Administración de Movilidad (MME) de la reivindicación 13, habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

El examinador también concluye que el documento D1 además revela un transmisor (824) que transmite a uno o más dispositivos de usuario (804) a través de antenas transmisoras (808) y que en consecuencia, la reivindicación 13 no es nueva, según lo divulgado en el documento D1.

Por otra parte, en su opinión, las reivindicaciones dependientes 14 a 17 no mencionan alguna característica que haga nueva a la MME de la reivindicación 13, por lo cual se considera que tampoco son nuevas.

En su análisis también concluye que las características esenciales del equipo de usuario (UE) de la reivindicación 18, habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva, y que las reivindicaciones dependientes 19 a 23 no mencionan alguna característica que haga nuevo al equipo de usuario de la reivindicación 18, por lo cual se considera que no son nuevas tampoco.

Sin embargo, al parecer el examinador no ha logrado entender correctamente ni la invención ni sus méritos.

El documento D1 citado en el examen de patentabilidad no parece tener ninguna relación con el caso que nos ocupa, pues al parecer el examinador ha ignorado el verdadero método que se reivindica y sólo se ha focalizado en los elementos físicos comprendidos en el nodo (por ejemplo, el transmisor, el receptor, etc.).

Como explicamos previamente, en el campo de las telecomunicaciones de manera particular, los dispositivos que se utilizan por lo general son convencionales, sin embargo la configuración que se les proporciona para resolver los problemas técnicos que se abordan, son los que le dan su distintividad y utilidad. Considérese además que la materia reivindicada en la solicitud, a saber, un método para establecer una clave de seguridad, K_{eNB}, para proteger el tráfico RRC/UP entre un Equipo de Usuario UE (11), y un eNodeB (12) que presta servicio al UE (11) y los dispositivos involucrados para llevar a cabo dicho método, son categorías de reivindicaciones totalmente patentables según la Decisión Andina 486, por lo cual pensamos que la patentabilidad de la materia reivindicada debe ser reconocida.

Deseamos señalar además que aunque la invención se puede implementar en el hardware existente, aunque también puede implementarse en un hardware particular, por ejemplo, en un ASIC.

Habiendo superado los errores formales de la solicitud original y demostrado el cumplimiento de los requisitos de patentabilidad por la presente invención, solicito que, sobre la base de los documentos que aquí se adjuntan, se proceda a la concesión de la patente colombiana correspondiente.

Teniendo en cuenta lo expuesto anteriormente consideramos que la presente solicitud de invención cumple con lo establecido en los artículos 16, 18 y 30 de la Decisión 486, es decir, la solicitud en estudio es una invención novedosa, tiene nivel inventivo y no se deriva de manera evidente del estado de la técnica, es susceptible de aplicación industrial, por tanto cumple con los requisitos establecidos en nuestra legislación para que sea otorgado el privilegio de invención.

Anexar:

- i. Nuevo capítulo Descriptivo
- ii. Nuevo capítulo Reivindicatorio.

Petición:

Conforme a lo anterior, una vez atendidos los requerimientos y exigencias del examinador y al tener en cuenta el nuevo capítulo descriptivo y reivindicatorio, además de lo manifestado anteriormente, solicito muy respetuosamente a su Despacho, continuar el trámite de rigor y de ser el caso se hagan las correspondientes observaciones con el ánimo de hacer lo pertinente dentro del presente trámite.

Atentamente,



HUMBERTO RUBIO CAMACHO

C.C. 17'192.062 de Bogotá

**T.P. 50.007 Consejo Superior
de la Judicatura**

COD. 4134

METODO Y DISPOSICIONES PARA ESTABLECER UNA CLAVE DE SEGURIDAD

CAMPO TÉCNICO

La presente invención se relaciona con los métodos y disposiciones en un sistema de telecomunicaciones, y en particular con una solución de seguridad en el EPS (Sistema de Paquetes Evolucionado), es decir la E-UTRAN (Evolved UMTS Terrestrial Radio Access Network) y la EPC (Evolved Packet Core network), para solicitudes de servicios accionadas por el UE. Más específicamente, la presente invención se relaciona con un método y una disposición en una MME (Mobility Management Entity) (13) y un UE (Equipo de Usuario) (11) para un EPS (Sistema de Paquetes Evolucionado) para establecer una clave de seguridad para proteger el tráfico RRC/UP.

ANTECEDENTES

En la arquitectura EPS, la autenticación de suscriptor se realiza entre un UE (11) y una MME (Mobility Management Entity) MME (13), y la MME (13) controla por ejemplo la movilidad, las identidades del UE (11) y los parámetros de seguridad. La base para definir el procedimiento de seguridad en el EPS es una clave de seguridad, K_ASME, que se comparte entre la MME (13) y el UE (11), y se establece en la autenticación del UE (11). Una entidad funcional de la arquitectura EPS llamada ASME (Access Security Management Entity) puede por ejemplo colocarse con la MME (13), y la ASME recibe y almacena la clave de seguridad K_ASME derivada de las claves CK/IK confinadas en la red. De la clave de seguridad, K_ASME, la ASME deriva un contexto de seguridad NAS usado para proteger la señal NAS, es decir una señal de Estrato Sin Acceso (Non Access Stratum) entre la MME (13) del Núcleo de Paquetes Evolucionados (Evolved Packet Core o EPC) y un UE (11). El contexto de seguridad NAS contiene parámetros para codificar y proteger la integridad de la señal NAS, tales como K_NAS_enc, K_NAS_int, así como números de secuencia de enlace ascendente y enlace descendente, NAS_U_SEQ y NAS_D_SEQ, y los números de secuencia se usan para evitar la repetición de mensajes viejos, así como para entradas para los procedimientos de codificación y protección de integridad. La ASME proporciona a la MME (13) con el contexto de seguridad NAS, y un contexto de seguridad NAS se mantiene en la MME (13), y un contexto de seguridad NAS correspondiente se mantiene en el UE (11), y la protección de repetición, protección de integridad y codificación se basan en que los números de secuencia de los contextos de seguridad NAS de la MME (13) y el UE (11) no son reusados.

Preferiblemente, el contexto de seguridad para la protección del tráfico UP/RRC entre un UE (11) y el eNodeB de servicio (12) (por ejemplo, una estación de radio base en una arquitectura EPS) también está basado en dicha clave de seguridad, K_ASME. El procedimiento para establecer el contexto de seguridad UP/RRC implica derivar una llave llamada K_eNB, a partir de la cual la clave de codificación K_eNB_UP_enc se deriva para proteger el UP (User Plane), por ejemplo, los datos de usuario final transferidos por EPC y E-UTRAN, así como la clave de codificación, K_eNB_RRC_enc, y la llave de protección de integridad, K_eNB_RRC_int, para proteger el RRC (Radio Resource Control).

- La Figura 1 ilustra un ejemplo flujo de señales convencional para una transición de estado INACTIVO a ACTIVO iniciada por un UE en una arquitectura EPS. Un UE (11) INACTIVO solo es conocido por el EPC (Evolved Packet Core) del EPS, y no existe ningún contexto de seguridad UP/RRC entre el eNodeB (12) y el UE (11). Un UE (11) en el estado ACTIVO es conocido tanto en el EPC como en el EUTRAN, y un contexto de seguridad UP/RRC se ha establecido para la protección del tráfico UP/RRC entre el UE (11) y su eNodeB de servicio (12).

La Figura 1 ilustra un UE (11), un eNodeB (12), una MME (13), una GW de servicio (Gateway) (14), una PDN Gateway (15), y el HSS (Home Subscriber Server) (16). La Gateway de Servicio (14) es el nodo del EPC que termina la interfaz hacia EUTRAN, y la PDN Gateway (15) es el nodo del EPC que termina la interfaz hacia un PDN (Packet Data Network). Si un UE (11) accede a múltiples PDNs, puede haber múltiples PDN Gateways (15) para ese UE (11). En la señal S1 y la señal S2, la Solicitud de Servicio NAS es enviada transparentemente del UE (11) a la MME (13), y la Solicitud de Servicio NAS se protege en su integridad basándose en NAS_U_SEQ. En la señal opcional S3, el UE (11) se autentica mediante la MME (13) y se establece el K_ASME, usando datos del suscriptor almacenados en el HSS (Home Subscriber Server), y la MME (13) envía la Solicitud de Configuración de Contexto Inicial al eNodeB (12), en S4. En las señales S5 y S6, el eNodeB (12) establece el portador de radio con el UE (11) y envía datos de enlace ascendente, y regresa un mensaje de Configuración Inicial de Contexto-Completa a la MME (13) en la señal S7. En la señal S8, la MME (13) envía una solicitud de actualización de portador a la GW de Servicio (14), y la GW de Servicio (14) responde en la señal S9.

En soluciones anteriores, la derivación del K_eNB por el UE (11) y MME (13) para el contexto de seguridad RRC/UP se basa, por ejemplo, en un mensaje de ACEPTACIÓN DE SERVICIO NAS u otra información explícita enviada desde la

MME (13) al UE (11). Sin embargo, como se ilustra en el ejemplo de flujo de señal EPS convencional en la Figura 1, la MME (13) normalmente no enviará ninguna ACEPTACIÓN DE SERVICIO NAS tras recibir una SOLICITUD DE SERVICIO NAS de un UE (11) en un EPS. Por lo tanto, no será posible derivar el K_{eNB} a partir de la información en un mensaje de ACEPTACIÓN DE SERVICIO NAS.

De acuerdo con una solución de ejemplo conocida, el K_{eNB} se deriva por la MME (13) del K_{ASME} y el NAS_D_SEQ usados por la MME (13) en el mensaje de ACEPTACIÓN DE SERVICIO NAS, y el UE deriva el mismo K_{eNB} obteniendo el número de secuencia, NAS_D_SEQ, a partir del mensaje de ACEPTACIÓN DE SERVICIO NAS y realizando la misma derivación K_{eNB} de la MME (13). La MME (13) transfiere el K_{eNB} al eNodeB (12) cuando este configura la conexión SI con el eNodeB (12). Sin embargo, un inconveniente de esta solución conocida es que si no se ha definido un mensaje explícito de ACEPTACIÓN DE SERVICIO NAS desde la MME (13) para el UE (11), como en el ejemplo de flujo de señal EPS convencional en la Figura 1, no es posible que el UE (11) derive el mismo K_{eNB} de la MME (13). Aún cuando es técnicamente posible que el UE (11) estime un número de secuencia de vínculo descendente del NAS actual, NAS_D_SEQ, esta estimación puede ser errónea, ya que la MME (13) puede haber enviado mensajes NAS que se perdieron y nunca fueron recibidos por el UE (11). En dicho caso, la MME (13) habría actualizado su NAS_D_SEQ, sin que el UE (11) estuviese al tanto de la actualización, llevando a una NAS_D_SEQ errónea en el UE (11).

De acuerdo con otra solución de ejemplo conocida, la derivación del K_{eNB} se basa en un número de secuencia diferente conservado específicamente para la derivación del K_{eNB}, y este número de secuencia está sincronizado explícitamente durante el procedimiento de Solicitud de Servicio NAS bien sea cuando el UE (11) lo envía a la MME (13), o cuando la MME (13) lo envía al UE (11). Sin embargo, una desventaja de esta solución es la complejidad adicional del número de secuencia diferente, ya que tiene que mantenerse tanto en el UE (11) como en la MME (13) con el fin de evitar ataques de repetición.

SUMARIO

El objeto de la presente invención es atender el problema antes mencionado, y este objetivo y otros se cumplen por el método y disposición de acuerdo con las reivindicaciones independientes, y mediante las representaciones de acuerdo con las reivindicaciones dependientes.

La idea básica de la presente invención es que el K_eNB se deriva del K_ASME y del NAS_U_SEQ del mensaje de Solicitud de Servicio NAS del UE (11) a la MME (13), activando así el establecimiento de un contexto de seguridad UP/RRC en el eNodeB (12).

- 5 Una ventaja de la presente invención es que no se requiere un mensaje explícito de enlace descendente de ACEPTACIÓN DE SERVICIO NAS ni número de secuencia de la MME (13) para el UE (11), y que la funcionalidad de protección de repetición del contexto de seguridad NAS se reutiliza en los contextos de seguridad RRC y UP.
- 10 De acuerdo con un aspecto, la invención ofrece un método en una Entidad de Administración de Movilidad, MME (13), de un Sistema de Paquetes Evolucionado, EPS, de establecer una clave de seguridad, K_eNB, para proteger el tráfico RRC/UP entre un Equipo de Usuario, UE (11), y un eNodeB (12) que presta servicios al UE (11). El método comprende los pasos de recibir una
- 15 SOLICITUD DE SERVICIO NAS del UE (11), solicitud que indica un número de secuencia NAS de enlace ascendente, NAS_U_SEQ; derivar la clave de seguridad, K_eNB, de al menos dicho NAS_U_SEQ recibido y a partir de una clave almacenada de Entidad de Administración de Acceso de Seguridad, K_ASME, compartido con dicho UE (11); y reenviar dicho K_eNB derivado al
- 20 eNodeB (12) que presta servicio a dicho UE (11).

- De acuerdo con un segundo aspecto, la invención ofrece una Entidad de Administración de Movilidad, MME (13), para un Sistema de Paquetes Evolucionado, EPS. La MME (13) se configura para establecer una clave de seguridad, K_eNB, para la protección del tráfico RRC/UP entre un UE (11) y un
- 25 eNodeB (12) que presta servicio al UE (11). La MME (13) comprende medios para recibir una SOLICITUD DE SERVICIO NAS del UE (11), solicitud que indica un número de secuencia NAS de enlace ascendente, NAS_U_SEQ; medios para derivar un K_eNB de al menos dicho NAS_U_SEQ recibido y de una clave almacenada de Entidad de Administración de Acceso de Seguridad, K_ASME,
- 30 compartida con dicho UE (11), así como medios para enviar dicho K_eNB derivado al eNodeB (12) que presta servicio a dicho UE (11).

- El primer y segundo aspecto además ofrece métodos, así como los correspondientes medios, de acuerdo con los cuales la MME (13) puede derivar el K_eNB del NAS_U_SEQ y el K_ASME usando una Función Seudo-Aleatoria,
- 35 PRF. La MME (13) puede además reconstruir el número completo de secuencia

NAS de enlace ascendente NAS_U_SEQ de bits recibidos de bajo orden y revisar la integridad de la Solicitud de Servicio NAS recibida del UE (11). Adicionalmente, la MME (13) puede regresar una indicación de la NAS_U_SEQ recibida al UE (11), y el NAS_U_SEQ puede incluirse en el mensaje de configuración que reenvía el K_eNB al eNodeB (12). Por lo tanto, el UE (11) no tiene que recordar el NAS_U_SEQ enviado a la MME (13).

De acuerdo con un tercer aspecto, la invención ofrece un método en un Equipo de Usuario, UE (11), de un Sistema de Paquetes Evolucionado, EPS, de establecer una clave de seguridad, K_eNB, para proteger el tráfico RRC/UP intercambiado con un eNodeB de servicio. El método comprende los pasos de enviar una SOLICITUD DE SERVICIO NAS a una Entidad de Administración de Movilidad, MME (13), solicitud que indica un número de secuencia NAS de enlace ascendente, NAS_U_SEQ; y derivar el K_eNB de al menos dicha NAS_U_SEQ y de una clave almacenada de Entidad de Administración de Acceso de Seguridad, K_ASME, compartida con dicha MME (13).

De acuerdo con un cuarto aspecto, la invención ofrece un Equipo de Usuario, UE (11), adaptado para un Sistema de Paquetes Evolucionado, EPS. El UE (11) se configura para establecer una clave de seguridad, K_eNB, para proteger el tráfico RRC/UP intercambiado con un eNodeB de servicio. El UE comprende medios para enviar una SOLICITUD DE SERVICIO NAS a una MME (13), solicitud que indica un número de secuencia NAS de enlace ascendente, NAS_U_SEQ, así como medios para derivar un K_eNB de al menos dicho NAS_U_SEQ, y de una clave almacenada de Entidad de Administración de Acceso de Seguridad, K_ASME, compartida con dicha MME (13).

El tercer y cuarto aspecto además ofrecen métodos, así como los correspondientes medios, de acuerdo con los cuales el UE puede derivar el K_eNB del NAS_U_SEQ y el K_ASME usando una Función Seudo-Aleatoria, PRF, y proteger la integridad de la Solicitud de Servicio NAS enviada a la MME (13). Adicionalmente, el UE (11) puede almacenar el NAS_U_SEQ de la Solicitud de Servicio NAS enviada a la MME (13), o, alternativamente, recibir una indicación de la NAS_U_SEQ de la Solicitud de Servicio NAS enviada a la MME (13), regresada de la MME (13) por medio del eNodeB (12). Esta representación alternativa tiene la ventaja de que el UE (11) no tiene que recordar el NAS_U_SEQ enviado a la MME (13). El UE (11) puede además derivar el K_eNB del NAS_U_SEQ y el K_ASME después de la recepción de un mensaje de configuración de seguridad del eNodeB (12).

BREVE DESCRIPCIÓN DE LAS GRÁFICAS

La presente invención ahora será descrita en más detalle, y con referencia a las gráficas adjuntas, en las cuales:

- 5 - La Figura 1 es un diagrama de señales que ilustra una Solicitud de Servicio convencional accionada por un UE (11) en un EPS;
- La Figura 2 es un diagrama de señales que ilustra la primera representación de esta invención, de acuerdo con la cual el UE recuerda el NAS_U_SEQ enviado a la MME (13) en un mensaje de SOLICITUD DE SERVICIO NAS;
- 10 - La Figura 3 es un diagrama de flujo que ilustra la derivación del K_eNB por parte del UE (11) y la MME (13);
- La Figura 4 es un diagrama de señales que ilustra una segunda representación de esta invención en la cual la MME (13) regresa el NAS_U_SEQ recibido al UE (11);
- 15 - La Figura 5 es un diagrama de flujo que ilustra la segunda representación descrita en la Figura 4; y
- La Figura 6a ilustra a manera de esquema una MME (Mobility Management Entity) (13), y la Figura 6b ilustra a manera de esquema un UE (11), ambos provistos con medios para derivar la clave de seguridad K_eNB.

DESCRIPCIÓN DETALLADA

- 20 En la siguiente descripción, se establecen detalles específicos, tales como una arquitectura y secuencias de pasos particulares con el fin de ofrecer una explicación completa de la presente invención. Sin embargo, es aparente para una persona diestra en la materia que la presente invención puede practicarse en otras representaciones que pueden partir de estos detalles específicos.
- 25 Además, es aparente que las funciones descritas pueden implementarse usando funciones de software en conjunto con un microprocesador programado o un computador de propósito general, y/o usando un circuito integrado de aplicación específica. En donde la invención se describe en forma de un método, la invención también pueden representarse en un producto de programa de
- 30 computadora, así como en un sistema que comprenda un procesador de

computadora y una memoria, en donde la memoria es codificada con uno o más programas que pueden realizar las funciones descritas.

El concepto o la invención es que la clave de seguridad, K_{eNB} , se deriva de la clave de la Entidad de Administración de Acceso de Seguridad, K_{ASME} , y del
5 contador de secuencia del enlace ascendente, NAS_U_SEQ , del mensaje de Solicitud de Servicio NAS enviado del UE (11) a la MME (13), accionando así el establecimiento del contexto de seguridad UP/RRC en el eNodeB (12).

Cuando el UE (11) está en modo INACTIVO, existe un contexto de seguridad NAS y comprende es decir, los anteriormente descritos K_{NAS_enc} , K_{NAS_int} ,
10 NAS_U_SEQ y NAS_D_SEQ , y los mensajes NAS están protegidos tanto en integridad y posiblemente en confidencialidad. El contexto de seguridad NAS entonces también contiene las capacidades de seguridad del UE (11), en particular los algoritmos de codificación e integridad.

La protección de los mensajes NAS se basa en las claves de seguridad NAS,
15 K_{NAS_enc} , K_{NAS_int} , y los contadores de secuencia de enlaces ascendente y descendente, NAS_U_SEQ o NAS_D_SEQ , para la dirección del mensaje. El contador de secuencia completo normalmente no se transmite con el mensaje NAS, solo algunos de los bits de bajo orden, y el número de secuencia completo se reconstruirá en el extremo receptor de un estimativo local de los bits de alto
20 orden y los bits de bajo orden recibidos.

El concepto de la invención puede explicarse en el contexto del diagrama de señales para solicitudes de servicio accionadas por el UE (11), como se describe en la Figura 1 antes descrita:

En S1 y S2 del diagrama convencional de señales en la Figura 1, una SOLICITUD
25 DE SERVICIO NAS, que comprende un contador de secuencia del enlace ascendente, NAS_U_SEQ , se reenvía del UE (11) a la MME (13), y el mensaje de Solicitud de Servicio NAS se protege en su integridad basándose en dicho NAS_U_SEQ . La MME (13) revisa la integridad del mensaje y lo acepta si no es una repetición, y esto garantiza que el NAS_U_SEQ es fresco y no se ha usado
30 antes.

De ahí en adelante, de acuerdo con esta invención, la MME (13) deriva el K_{eNB} basándose al menos en el contador de secuencia del enlace ascendente NAS_U_SEQ recibido y en el K_{ASME} , usando una función convencional de derivación de claves, y esto no se incluye en el diagrama convencional de señales

que se ilustra en la Figura 1. Por consiguiente, el contador de secuencia puede solo reconfigurarse en la autenticación. La MME (13) enviará el K_eNB derivado al eNode, o simultáneamente, en el mensaje de señal, la Solicitud de Configuración de Contexto Inicial (S1-AP).

- 5 En la señal S5, el eNodeB (12) envía un Emplazamiento de Portador de Radio y un mensaje de configuración de seguridad (Comando de Modo de Seguridad) al UE (11). Estos mensajes pueden enviarse cómo dos mensajes separados o combinados en un mensaje, como en la Figura 1, y la recepción de estos mensajes por el UE (11) implícitamente será una confirmación de la SOLICITUD
- 10 DE SERVICIO NAS de los UEs (11), en la señal S1. El Comando de Modo de Seguridad determinará por ejemplo cuándo debe iniciar la protección y qué algoritmo usar.

De acuerdo con esta invención, el UE (11) deriva el K_eNB basándose al menos en el NAS_U_SEQ y el K_ASME, usando una función convencional de derivación

15 de claves, tras la recepción del mensaje en la señal S5, si no se realizó antes. De ahí en adelante, el eNodeB (12) y el UE (11) establecerán el contexto de seguridad UP/RRCs, y este no es el que se ilustra en el diagrama convencional de señales en la Figura 1.

De acuerdo con una primera representación de esta invención, el UE (11)

20 almacena el contador de secuencia del enlace ascendente, NAS_U_SEQ, que se incluye en la SOLICITUD DE SERVICIO NAS inicial en la señal S1, y usa el NAS_U_SEQ almacenado para la derivación del K_eNB.

Sin embargo, de acuerdo con una segunda representación, la MME (13) incluye el contador de secuencia del enlace ascendente, NAS_U_SEQ, o solo bits de bajo

25 orden que indica el NAS_U_SEQ, en el mensaje de configuración S1-AP, en la señal S4, enviada al eNodeB, en cuyo caso esta información es reenviada al UE (11) del eNodeB (12) durante el establecimiento del contexto RRC/UP. En este caso, el UE (11) podrá retomar la indicación del NAS_U_SEQ del eNodeB (12) para la derivación del K_eNB, y no tiene que conservar el NAS_U_SEQ del

30 mensaje de SOLICITUD DE SERVICIO NAS enviado a la MME (13) en las señales S1 y S2.

La Figura 2 ilustra la primera representación de esta invención, en donde el UE (11) conserva el NAS_U_SEQ del mensaje inicial de la SOLICITUD DE SERVICIO NAS, en la señal S21, para la derivación de K_eNB en la señal S24. La

35 MME (13) recibirá el NAS_U_SEQ del UE (11) en la señal S21, o solo bits de bajo

orden que indican el NAS_U_SEQ, y derivan el K_eNB basándose en el NAS_U_SEQ y el K_ASME en S22. La MME (13) reenvía el K_eNB derivado al eNodeB (12) en la señal S23.

De ahí en adelante, no ilustrado en la Figura 2, el eNodeB (12) y el UE (11) establecerán el contexto de seguridad UP/RRC usando el K_eNB, el contexto de seguridad UP/RRCs que comprende la clave de codificación, K_eNB_UP_enc para proteger el tráfico UP, así como la clave de codificación y la llave de protección de integridad, K_eNB_RRC_enc y K_eNB_RRC_int, respectivamente, para proteger el tráfico RRC, por lo tanto permitiendo un tráfico UP/RRC seguro, en la señal S25.

La derivación del K_eNB se realiza por medio de una función convencional de derivación de clave, es decir mediante una Función Seudo-Aleatoria; $K_{eNB} = PRF(K_{ASME}, NAS_U_SEQ, \dots)$.

Además, como se ilustra con los puntos en la función PRF antes descrita, la función de derivación K_eNB puede tener valores adicionales de entrada convencionales, tales como la identidad eNodeB (12).

La Figura 3 es un diagrama de flujo que ilustra el método de acuerdo con esta invención, y en el paso 31, el UE (11) envía en el mensaje inicial de SOLICITUD DE SERVICIO NAS a la MME (13), el mensaje que indica el contador de secuencia NAS del enlace ascendente, NAS_U_SEQ, normalmente solo enviando los bits de bajo orden del contador. En el paso 32, la MME (13) recibe el mensaje de Solicitud de Servicio NAS del UE (11), obteniendo el NAS_U_SEQ, y reconstruyendo la secuencia completa a partir de los bits de bajo orden recibidos. En el paso 33, la MME (13) deriva la clave de seguridad, K_eNB, de al menos el NAS_U_SEQ recibido y el K_ASME del ASME (Access Security Mobility Entity), usando una función de derivación de clave adecuada, es decir una Función Seudo-Aleatoria.

De ahí en adelante, la MME (13) reenvía el K_eNB derivado al eNodeB (12), en el paso 34, para ser usado por el eNodeB para establecer el contexto de seguridad UP/RRC completo compartido con el UE. En el paso 35, dicho UE derivará el mismo K_eNB de al menos el K_ASME almacenado y del NAS_U_SEQ del mensaje inicial del SOLICITUD DE SERVICIO NAS transmitido del UE (11) a la MME (13) en el paso 31, y establecerá el contexto de seguridad UP/RRC del K_eNB derivado.

En la primera representación de esta invención, el UE (11) almacena el NAS_U_SEQ transmitido a la MME (13) en el mensaje inicial de SOLICITUD DE SERVICIO NAS, y usa el número de secuencia almacenado para derivar el K_eNB.

- 5 La Figura 4 es un diagrama de señales que ilustra una segunda representación de esta invención, en donde el UE (11) no tiene que almacenar el NAS_U_SEQ. Por el contrario, la MME (13) regresará una indicación del NAS_U_SEQ recibido al UE (11), por medio del eNodeB (12). En la señal S41, correspondiente a la señal S21 en la Figura 2, el UE (11) transmite una SOLICITUD DE SERVICIO NAS inicial a la MME (13), indicando un número de secuencia de enlace ascendente, NAS_U_SEQ, y MME recibirá el NAS_U_SEQ y derivará el K_eNB basándose en al menos el NAS_U_SEQ y el K_ASME, en S42. Sin embargo, de acuerdo con esta segunda representación, la MME (13) incluirá una indicación de dicho NAS_U_SEQ recibido en la señal S43 transmitida al eNodeB (12) junto con el K_eNB derivado, y el eNodeB (12) reenviará el NAS_U_SEQ al UE (11), en la señal S44. De ahí en adelante, el UE (11) derivará el K_eNB de al menos el K_ASME y del NAS_U_SEQ regresado por la MME (13), en la señal S45. De la clave de seguridad derivada, K_eNB, el eNodeB (12) y el UE (11) establecerán el contexto de seguridad UP/RRC, permitiendo así un tráfico UP/RRC seguro, en la señal S46.

- La Figura 5 es un diagrama de flujo que ilustra el método antes descrito de acuerdo con una segunda representación de esta invención, en donde una indicación del NAS_U_SEQ se regresa al UE (11) por la MME (13). En el paso 41, el UE (11) envía en el mensaje inicial de SOLICITUD DE SERVICIO NAS a la MME (13), el mensaje que indica el contador de secuencia NAS del enlace ascendente, NAS_U_SEQ, normalmente los bits de bajo orden. En el paso 52, la MME (13) recibe el mensaje de Solicitud de Servicio NAS del UE (11), obteniendo así el NAS_U_SEQ, y, de ser necesario, reconstruir el NAS_U_SEQ completo a partir de los bits de bajo orden recibidos. En el paso 53, la MME (13) deriva la clave de seguridad, K_eNB, de al menos el NAS_U_SEQ recibido y el K_ASME, usando una función de derivación de clave adecuada.

- De ahí en adelante, la MME (13) incluye una indicación del contador de secuencia NAS del enlace ascendente, NAS_U_SEQ, en el mensaje que reenvía el K_eNB derivado al eNodeB (12), en el paso 54, y el eNodeB (12) usa la clave de seguridad recibida, K_eNB, para establecer un contexto de seguridad UP/RRC. El NAS_U_SEQ recibido se reenvía al UE (11) por el eNodeB (12), en el paso 55, y

en el paso 56, el UE (11) deriva la clave de seguridad, K_{eNB} , de al menos el K_{ASME} y de dicho NAS_U_SEQ recibido, con el fin de establecer el contexto de seguridad UP/RRC compartido con el eNodeB (12).

La derivación del K_{eNB} por la MME (13), en el paso 53, y por el UE (11), en el paso 56, se realiza por medio de una función convencional de derivación de clave adecuada, es decir una Función Seudo-Aleatoria; $K_{eNB} = PRF(K_{ASME}, NAS_U_SEQ, \dots)$. Normalmente, la función de derivación de clave tendrá valores de entradas convencionales adicionales, es decir la identidad eNodeB.

La Figura 6a ilustra una MME (13) (Entidad de Administración de Movilidad) para un EPS, de acuerdo con esta invención, además se dispone para establecer una clave de seguridad, K_{eNB} , para un contexto de seguridad para la protección del tráfico UP/RRC entre un UE (11) y un eNodeB de servicio (12). La MME (13) está provista de medios de comunicación convencional, no ilustrados en la figura, para comunicarse con los nodos en el EPS, es decir con los eNodeBs (12) por medio de una interfaz SI-MME. Además, en la MME (13) de la Figura 1, una ASME (Entidad de Administración de Acceso de Seguridad) 61 es ilustrada por líneas punteadas, ya que esta entidad funcional de un EPS puede ser colocada con la MME (13).

Los medios de la MME (13) que se ilustran en la Figura 6a para establecer la clave de seguridad, K_{eNB} , comprenden medios de recepción 62 para recibir un mensaje de SOLICITUD DE SERVICIO NAS incluyendo un NAS_U_SEQ de un UE (11) (por medio del eNodeB de servicio; medios de derivación de clave 63 para derivar una clave de seguridad, K_{eNB} basándose en al menos el NAS_U_SEQ recibido y un K_{ASME} almacenado, usando una función convencional de derivación de claves; y enviando medios 64 para enviar el K_{eNB} derivado al eNodeB (12) que presta servicio al UE (11).

La Figura 6b ilustra un UE (11) (Equipo de Usuario) de acuerdo con esta invención, el UE (11) adaptado para un EPS, y adecuado además para establecer una clave de seguridad, K_{eNB} , para un contexto de seguridad para la protección del tráfico UP/RRC intercambiado con su eNodeB de servicio (12). El UE (11) está provisto de medios de comunicación convencional, no ilustrados en la figura, para comunicarse con los nodos en el EPS por medio de una interfaz LTE-Uu con su eNodeB de servicio (12).

Los medios del UE (11) que se ilustran en la Figura 6b para establecer la clave de seguridad, K_{eNB} , comprende el envío de medios 66 para enviar un mensaje de

SOLICITUD DE SERVICIO NAS a la MME (13), por medio del eNodeB de servicio (12), solicitud que indica un número de secuencia de enlace ascendente, NAS_U-SEQ, y los medios para establecer una clave de seguridad, K_eNB, comprende medios de derivación de clave 67 para derivar una clave de seguridad, K_eNB basándose en al menos el NAS_U-SEQ y un K_ASME almacenado, usando una función convencional de derivación de claves.

Los medios antes descritos de la MME (13) y el UE (11), como se ilustra en las figuras 6a y 6b, implementan las funciones descritas usando una combinación adecuada de software y hardware, es decir un microprocesador programado o un circuito integrado específico para la aplicación, así como transmisores y receptores de radio convencionales.

Aunque la invención ha sido descrita con referencia a representaciones de ejemplo específicas, la descripción es general y solo pretende ilustrar el concepto inventivo y no debe ser tomada como si limitara el alcance de la invención, el cual debe considerarse las reivindicaciones que se adjuntan.

REIVINDICACIONES

1. Un método en una Entidad de Administración de Movilidad MME (13), de un Sistema de Paquetes Evolucionado, EPS, de establecer una clave de seguridad, K_eNB, para proteger el tráfico RRC/UP entre un Equipo de Usuario UE (11), y un eNodeB (12) que presta servicio al UE (11), método que comprende los siguientes pasos:
 - recibir (32, 52) una SOLICITUD DE SERVICIO NAS del UE, solicitud que indica un número de secuencia NAS de enlace ascendente, NAS_U_SEQ;
 - derivar (33, 53) la clave de seguridad, K_eNB, de dicho NAS_U_SEQ recibido y de una clave almacenada de Entidad de Administración de Acceso de Seguridad, K_ASME, compartida con dicho UE (11);
 - reenviar (34) dicho K_eNB derivado al eNodeB (12) que presta servicio al UE (11).
2. Un método en una MME (13) de acuerdo con la reivindicación 1, en donde el K_eNB se deriva del NAS_U_SEQ y el K_ASME usando una Función Seudo-Aleatoria, PRF.
3. Un método en una MME (13) de acuerdo con la reivindicación 1 o 2, que comprende el paso adicional de reconstruir el número de secuencia completo NAS de enlace ascendente NAS_U_SEQ de los bits de bajo orden recibidos.
4. Un método en una MME (13) de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende el paso adicional de comprobar la integridad de la Solicitud de Servicio NAS recibida del UE (11).
5. Un método en una MME (13) de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende el paso adicional de regresar (54,55) una indicación del NAS_U_SEQ recibido del UE (11).
6. Un método en una MME (13) de acuerdo con la reivindicación 5, en donde el NAS_U_SEQ se incluye en el mensaje de configuración que reenvía el K_eNB al eNodeB (12).
7. Un método en a Equipo de Usuario (11), UE, de un Sistema de Paquetes Evolucionado, EPS, de establecer una clave de seguridad, K_eNB, para proteger

el tráfico RRC/UP intercambiado con un eNodeB de servicio (12), el método que comprende los siguientes pasos:

- enviar (31, 51) una SOLICITUD DE SERVICIO NAS a una Entidad de Administración de Movilidad, MME (13), solicitud que indica un número de
5 secuencia NAS de enlace ascendente, NAS_U_SEQ;

- derivar (35, 56) el K_eNB de dicho NAS_U_SEQ y de una clave almacenada de Entidad de Administración de Acceso de Seguridad, K_ASME, compartida con dicha MME (13).

8. Un método en un UE (11) de acuerdo con la reivindicación 7, en donde el
10 K_eNB se deriva del NAS_U_SEQ y el K_ASME usando una Función Seudo-Aleatoria, PRF.

9. Un método en un UE (11) de acuerdo con cualquiera de las reivindicaciones 7 - 8, que comprende el paso adicional de proteger la integridad de la Solicitud de Servicio NAS enviada a la MME (13).

15 10. Un método en un UE (11) de acuerdo con cualquiera de las reivindicaciones 7 - 9, que comprende el paso de almacenar el NAS_U_SEQ de la Solicitud de Servicio NAS enviada a la MME (13).

11. Un método en un UE (11) de acuerdo con cualquiera de las reivindicaciones 7 - 9, que comprende el paso de recibir (55) una indicación del NAS_U_SEQ de la
20 Solicitud de Servicio NAS enviada a la MME (13), de regreso de la MME (13) por medio del eNodeB (12).

12. Un método en un UE (11) de acuerdo con cualquiera de las reivindicaciones 10 u 11, en donde el K_eNB se deriva del NAS_U_SEQ y el K_ASME después de la recepción de un mensaje de configuración de seguridad del eNodeB (12).

25 13. Una Entidad de Administración de Movilidad MME (13), adaptada para un Sistema de Paquetes Evolucionado, EPS, la MME (13) que se dispone para establecer una clave de seguridad, K_eNB, para la protección del tráfico RRC/UP entre un UE (11) y un eNodeB (12) que presta servicio al UE (11), donde la MME (13) se caracteriza por:

30 - medios (62) para recibir una SOLICITUD DE SERVICIO NAS del UE, solicitud que indica un número de secuencia NAS de enlace ascendente, NAS_U_SEQ;

- medios (63) para derivar a K_{eNB} de dicho NAS_{U_SEQ} recibido y de una clave de Entidad de Administración de Acceso de Seguridad almacenada, K_{ASME}, compartida con dicho UE (11);

5 - medios (64) para enviar dicho K_{eNB} derivado al eNodeB (12) que presta servicio a dicho UE (11).

14. Una MME (13) de acuerdo con la reivindicación 13, dispuesta para derivar el K_{eNB} del NAS_{U_SEQ} y el K_{ASME} usando una Función Seudo-Aleatoria, PRF.

10 15. Una MME (13) de acuerdo con la reivindicación 13 o 14, dispuesta para reconstruir el número de secuencia completo NAS de enlace ascendente NAS_{U_SEQ} de los bits de bajo orden recibidos.

16. Una MME (13) de acuerdo con cualquiera de las reivindicaciones 13 - 15, dispuesta para comprobar la integridad la Solicitud de Servicio NAS recibida del UE (11).

15 17. Una MME (13) de acuerdo con cualquiera de las reivindicaciones 13 - 16, dispuesta para reenviar (54) una indicación del NAS_{U_SEQ} al eNodeB (12), para ser regresada (55) al UE (11) del eNodeB (12).

20 18. Un Equipo de Usuario (11), UE, adaptado para un Sistema de Paquetes Evolucionado, EPS, UE que se dispone para establecer una clave de seguridad, K_{eNB}, para proteger el tráfico RRC/UP intercambiado con un eNodeB de servicio (12), UE (11) que se caracteriza por:

- medios (66) para enviar una SOLICITUD DE SERVICIO NAS a una MME (13), solicitud que indica un número de secuencia NAS de enlace ascendente, NAS_{U_SEQ};

25 - medios (67) para derivar un K_{eNB} de dicho NAS_{U_SEQ}, y de una clave de Entidad de Administración de Acceso de Seguridad almacenada, K_{ASME}, compartida con dicha MME (13).

30 19. Un UE (11) de acuerdo con la reivindicación 18, dispuesto para derivar el K_{eNB} de el NAS_{U_SEQ} y el K_{ASME} usando una Función Seudo-Aleatoria, PRF.

20. Un UE (11) de acuerdo con cualquiera de las reivindicaciones 18 - 19, dispuesto para proteger la integridad de la Solicitud de Servicio NAS enviada a la MME (13).

5 21. Un UE (11) de acuerdo con cualquiera de las reivindicaciones 18 - 20, dispuesto para almacenar el NAS_U_SEQ de la Solicitud de Servicio NAS enviado a la MME (13).

22. Un UE (11) de acuerdo con cualquiera de las reivindicaciones 18 - 20, dispuesto para recibir una indicación del NAS_U_SEQ del Servicio NAS. Solicitud enviada a la MME (13), de regreso de la MME (13) por medio del eNodeB (12).

10 23. Un UE (11) de acuerdo con cualquiera de las reivindicaciones 21 o 22, dispuesto para derivar el K_eNB después de la recepción de un mensaje de configuración de seguridad del eNodeB (12).