



Industria y Comercio
SUPERINTENDENCIA

Delegatura de Propiedad Industrial
División de Nuevas Creaciones

PCT

SOLICITUD
PATENTE DE INVENCION

21. **EXPEDIENTE No.** **10-12466**

54. **TÍTULO** "Metodo y disposicion en un sistema de telecomunicaciones"

51. **CLASIFICACIÓN INTERNACIONAL**

71. **SOLICITANTE** Telefonaktiebolaget LM Ericsson (publ)

DOMICILIO Estocolmo, Suecia

74. **APODERADO** Humberto Rubio Camacho
Ced 4134

22. **BOGOTÁ, D.C.,** 5 de febrero / 2010

(FORMA P-10)

Título, Cursus
17-04-2010

Rubio Rubio
09-70588



No. 10-012466-00000-0000

Fecha: 2010-02-05 12:40:19 Dep. 2020 DIR. NUEVASCR
Tra. 11 PATENTE/II Evs. 378 FASE NACIONAL
Act. 411 PRESENTACION Folios: 32

PETITORIO

FORMULARIO ÚNICO DE SOLICITUD DE PATENTE
PCT
ENTRADA EN FASE NACIONAL

SOLICITUD DE:

☒ Patente de Invención

Patente de Modelo de Utilidad

☒ Capítulo I

Capítulo II

SOLICITANTE (71) Nombre y **Telefonaktiebolaget L M Ericsson (publ)**
Dirección: **SE-164 83, Estocolmo, Suecia**
Lugar de constitución: **Estocolmo, Suecia**

REPRESENTANTE Nombre: **HUMBERTO RUBIO CAMACHO** IDENTIFICACIÓN
O APODERADO (74) Dirección: **Carrera 7 No. 74 - 64, Of. 506** C.C. **17'192.062**
Teléfono: **3132408** Fax: **3131647** T.P. **50.007 CSI**

INVENTOR(ES) (72) Nombre y **1) Rolf BLOM**
Dirección: **Svärdvägen 2**
SE-175 68 JÄRFÄLLA, SUECIA
2) Gunnar MILDH
Turebergs Allé 7
SE-191 62 SOLLENTUNA, SUECIA
3) Karl NORRMAN
Stigbergsgatan 32A
SE-116 28 ESTOCOLMO, SUECIA

PCT (86)

Solicitud Internacional No. **PCT/SE2008/050591** Fecha **20 DE MAYO DE 2008**
Publicación Internacional No. **WO 2009/038522** Fecha **26 DE MARZO DE 2009**

TÍTULO (54) **"Método y disposición en un sistema de telecomunicaciones"** (Folio 40)

Clasificación Internacional (51) **A04L 9/08, H04L 9/32, H04L 29/06**

Prioridad (33) País de origen (32) Fecha (31) Número de solicitud
SI ☒ NO **ESTADOS UNIDOS DE AMERICA 17 DE SEPTIEMBRE DE 2007 60/972,955**

Comprobante de pago No. **10-6,490** Fecha: **28 DE ENERO DE 2010**
10-6,494 **28 DE ENERO DE 2010**

**EXTRACTO PARA PUBLICACIÓN
SOLICITUD DE PATENTE DE INVENCION
DELEGATURA PROPIEDAD INDUSTRIAL**

(21) No. SOLICITUD: (51) INT. CL.:
(22) FECHA DE PRESENTACIÓN: (71) SOLICITANTE: **Telefonaktiebolaget L M Ericsson (publ)**
(30) PRIORIDAD: **ESTADOUNIDENSE**
(31) No. DE SOLICITUD: **60/972,955** (72) INVENTORES: **Rolf BLOM
Gunnar MILDH
Karl NORRMAN**
(32) FECHA DE PRESENTACIÓN: **17 DE SEPTIEMBRE DE 2007**
(33) PAÍS: **ESTADOS UNIDOS DE AMERICA** (74)APODERADO: **Humberto RUBIO CAMACHO**

Solicitud Internacional No. **PCT/SE2008/050591** Fecha **20 DE MAYO DE 2008**
Publicación Internacional No. **WO 2009/038522** Fecha **26 DE MARZO DE 2009**

FECHA ENTRADA EN FASE NACIONAL:

(54) TITULO: "Método y disposición en un sistema de telecomunicaciones"

RESUMEN:

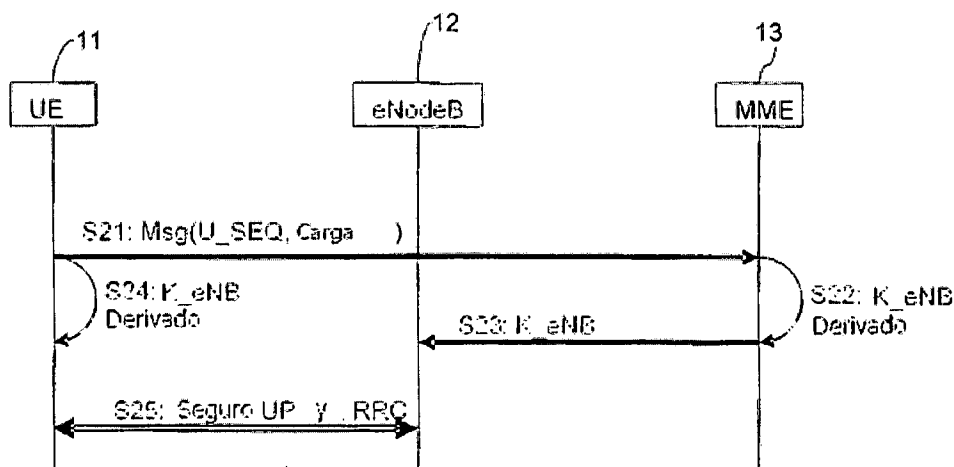
Un método en una Entidad de Administración de Movilidad (13), MME, de un Sistema Evolucionado de Paquetes, EPS, de establecer una clave de seguridad, K_{eNB}, para proteger el tráfico RRC/UP entre un Equipo de Usuario (11), UE, y un eNodeB (12) que presta servicio al UE, método que comprende los siguientes 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 al menos dicho NAS_{U_SEQ} recibido y de una clave almacenada de Entidad de Administración de Acceso de Seguridad, K_{ASME}, compartida con dicho UE;
- Reenviar (34) dicho K_{eNB} derivado al eNodeB (12) que presta servicio al UE.

ANEXOS

- X Comprobante de pago de la tasa de presentación de la solicitud.
- X Comprobante de pago de la tasa por excedente de Reivindicaciones.
- X Documento que acredita la existencia y representación legal cuando el solicitante sea persona jurídica. *Copia autentica reposa en el Exp 09-070582*
- X Poderes, si fuere el caso. *Copia autentica reposa en el Expediente 09-070582*
- Documento de cesión del inventor al solicitante o a su causante.
- Declaraciones
 - X Copia de la publicación PCT
 - X Copia informe búsqueda internacional.
 - Copia de Opinión escrita
 - X Traducción de la solicitud internacional al castellano. (Resumen, descripción, reivindicaciones, dibujos)
 - Copia del informe del examen preliminar internacional efectuado por la Autoridad Internacional (IPEA). (Incluye modificaciones)
 - Traducción de los anexos del examen preliminar internacional.
 - Copia de las modificaciones efectuadas de acuerdo con el Artículo PCT en Fase Nacional.
 - De ser el caso, certificado de depósito del material biológico.
- X Arte final 12 x 12
- De ser el caso, modificaciones efectuadas a la solicitud internacional.
- Otros

(11) Figura característica:



(12)

HUMBERTO RUBIO CAMACHO

FIRMA

C.C. 17'192.062 de Bogotá

T.P. 50.007 Consejo Superior de La Judicatura

COMO PARTE DE LA CANCELACION DE UNA TARIFA VIGENTE Y NO PODRA SER
SUSTITUIDA POR NINGUN RECIBO.

**PARA USO EXCLUSIVO DE
HUMBERTO RUBIO & CIA. LTDA.**

SOLICITUD DE PATENTE FASE NACIONAL
PCT/SE2009/050591

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 10 - 6.490
FECHA : ENERO 28 DE 2010

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 10-012466- -00000-0000

Fecha: 2010-02-05 12:40:19 Dep. 2020 DIR.NUEVASOR
Tra. 11 PATENTEIYII Eva. 378 FASENACIONALI
Act. 411 PRESENTACION Folios. 32

******* CONSIGNACION *******

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
HUMBERTO RUBIO & CIA ABOG	CONSIGNACION	BANCO DE BOGOTA	062754387	80848154	28/01/2010	8,736,000.00

******* CONCEPTO *******

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-01	SOLICITUDES	
		1 TRAMITES DE SOL. DE PATENTE DE IN	554,000.00
		TOTAL :	\$ 554,000.00

SON: QUINIENTOS CINCUENTA Y CUATRO MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

**PARA USO EXCLUSIVO DE
HUMBERTO RUBIO & CIA. LTDA.**

EXCEDENTE REIVINDICACIONES
PCT/SE2008/050591

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

CERTIFICACION DE EXCEDENTE : 10 - 6,494
FECHA : ENERO 28 DE 2010

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 10-012466- -00000-0000

Fecha: 2010-02-05 12:40:19 Dep. 2020 DIR.NUEVASOR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folia: 32

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
HUMBERTO RUBIO & CIA ABOGCONSIGNACION		BANCO DE BOGOTA	062754387	80848154	28/01/2010	8,736,000.00

***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-09	OTROS SERVICIOS DE PROPIEDAD I	
		99 OTROS SERVICIOS ADMINISTRATIVOS	338,000.00
		TOTAL :	\$ 338,000.00

SON: TRESCIENTOS TREINTA Y OCHO MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

ESTA CERTIFICACION DE EXCEDENTE DE PAGO SOLO PODRA SER UTILIZADA
COMO PARTE DE LA CANCELACION DE UNA TARIFA VICENTE Y NO PODRA SER

S



- (51) International Patent Classification:
H04L 9/08 (2006.01) H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
- (21) International Application Number:
PCT/SE2008/050591
- (22) International Filing Date: 20 May 2008 (20.05.2008)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/972,955 17 September 2007 (17.09.2007) US
- (71) Applicant (for all designated States except US): TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)
[SE/SE]; S-164 33 Stockholm (SE).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): BLOM, Rolf
[SE/SE]; Svändvägen 2, S-175 62 Järfälla (SE). MILDH,
Gunnar [SE/SE]; Turebergs Allé 7, S-191 62 Sollentuna
(SE). NORRMAN, Karl [SE/SE]; Stigbergsgatan 32A,
S-116 28 Stockholm (SE).
- (74) Agent: HASSELGREN, Joakim; Ericsson AB, Patent
Unit LTE, S-164 30 Stockholm (SE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BE, BG, BH, BR, BW, BY, BZ, CA, CH, CI, CO, CP, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GE, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MP, NE, NI, TD, TG).

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

[Continued on next page]

(54) Title: METHOD AND ARRANGEMENT IN A TELECOMMUNICATION SYSTEM

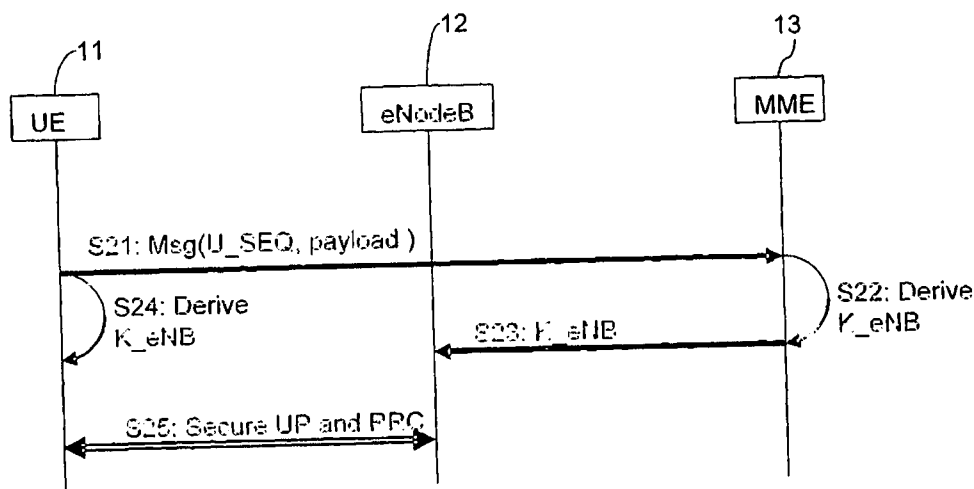


Fig. 2

(57) Abstract: A security key, K_{eNB} , for protecting RRC/UP traffic between a User Equipment, UE, (11) and a serving eNodeB (12) is established by a method and an arrangement in a Mobility Management Entity (13), MME, and in said UE (11), of an Evolved Packet System, EPS. The MME and the UE derives the security key, K_{eNB} , from at least an NAS uplink sequence number, NAS_U_SEQ, sent from the UE to the MME, and from an Access Security Management Entity-key, K_{ASME} , shared between the MME and the UE.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE2008/050591

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	NOKIA: 'Generation of separate keys for NAS/UP/RRC during initial access and handover', S3-060648, 3GPP TSG SA WG3 Security S3#45, 31 October - 3 November, 2006, Dulles, USA. [retrieved on 2008-04-21] Retrieved from the Internet: < http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_45_Ashburn/Docs/ > See whole document	1-23
	--	
A	NOKIA, ERICSSON: 'MAC, RLC and RRC Layer Security', S3-060456, 3GPP TSG SA WG3 Security #44, July 11-14, 2006, Tallinn, Estonia. [retrieved on 2008-04-21] Retrieved from the Internet: < http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_44_Tallinn/Docs/ > See whole document	1-23
	--	

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 4 December 2008	Date of mailing of the international search report 10-12-2008
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Christian Wall/PR Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/050591

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 0124560 A1 (SIMOCO INTERNATIONAL LIMITED), 5 April 2001 (05.04.2001), abstract --	1-23
A	WO 2007022731 A1 (HUAWEI TECHNOLOGIES CO., LTD.), 1 March 2007 (01.03.2007), abstract -- -----	1-23

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/050591

International patent classification (IPC)

H04L 9/08 (2006.01)

H04L 29/06 (2006.01)

H04L 9/32 (2006.01)

Download your patent documents at www.prv.se

The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.

The password is **LXZWIYDIID**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT
Information on patent family members

01/11/2008

International application No.

PCT/SE2008/050591

WO	0124560	A1	05/04/2001	AU	7534900	A	30/04/2001
				GB	0023682	D	00/00/0000
				GB	2359464	A	22/08/2001
				GB	9922847	D	00/00/0000

WO	2007022731	A1	01/03/2007	CN	1921682	A	28/02/2007

Método y disposición en un sistema de telecomunicaciones

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 Evolucionado de Paquetes), 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) y un UE (Equipo de Usuario) para un EPS (Sistema Evolucionado de Paquetes) para establecer una clave de seguridad para proteger el tráfico RRC/UP.

ANTECEDENTES

En la arquitectura EPS, autenticación de subscriber se realiza entre un UE y una MME (Mobility Management Entity), y la MME controla por ejemplo la movilidad, las identidades de UE 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 y el UE, y se establece en la autenticación del UE. Una entidad funcional de la arquitectura EPS llamada ASME (Access Security Management Entity) puede por ejemplo colocarse con la MME, 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 al Núcleo de Paquetes Evolucionados (Evolved Packet Core o EPC) y un UE. 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 evitarla repetición de mensajes viejos, así como para entradas para los procedimientos de codificación y protección de integridad. La ASME proporciona la MME con el contexto de seguridad NAS, y un contexto de seguridad NAS se mantiene en la MME, y un contexto de seguridad NAS correspondiente se mantiene en el UE, 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 y el UE no son reusados.

Preferiblemente, el contexto de seguridad para la protección del tráfico UP/RRC entre un UE y el eNodeB de servicio (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 INACTIVO solo es conocido por el EPC (Evolved Packet Core) del EPS, y no existe ningún contexto de seguridad UP/RRC entre el eNodeB y el UE. Un UE 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 y su eNodeB de servicio.

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

En soluciones previas, la derivación del K_{eNB} por el UE y MME 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 al UE. Sin embargo, como se ilustra en el ejemplo de flujo de señal EPS convencional en la Figura 1, la MME normalmente no enviará ninguna ACEPTACIÓN DE SERVICIO NAS tras recibir una SOLICITUD DE SERVICIO NAS de un UE 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 del K_{ASME} y el NAS_D_SEQ usados por la MME 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. La MME transfiere el K_{eNB} al eNodeB cuando este configura la conexión SI con el eNodeB. 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 para el UE, como en el ejemplo de flujo de señal EPS

convencional en la Figura 1, no es posible que el UE derive el mismo K_{eNB} de la MME. Aún cuando es técnicamente posible que el UE estime un número de secuencia de vínculo descendente del NAS actual, NAS_D_SEQ , esta estimación puede ser errónea, ya que la MME puede haber enviado mensajes NAS que se perdieron y nunca fueron recibidos por el UE. En dicho caso, la MME habría actualizado su NAS_D_SEQ , sin que el UE estuviese al tanto de la actualización, llevando a una NAS_D_SEQ errónea en el UE.

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 lo envía a la MME, o cuando la MME lo envía al UE. 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 como en la MME con el fin de evitar ataques de repetición.

RESUMEN

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 a la MME, activando así el establecimiento de un contexto de seguridad UP/PPC en el eNodeB.

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 para el UE, y que la funcionalidad de protección de repetición del contexto de seguridad NAS se reutiliza en los contextos de seguridad PPC y UP.

De acuerdo con un aspecto, la invención ofrece un método en una Entidad de Administración de Movilidad, MME, de un Sistema de Paquetes Evolucionado, EPC, de establecer una clave de seguridad, K_{eNB} , para proteger el tráfico PPC/UP entre un Equipo de Usuario, UE, y un eNodeB que presta servicios al UE. El método comprende los pasos de recibir una SOLICITUD DE SERVICIO NAS del UE, 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; y reenviar dicho K_{eNB} derivado al eNodeB que presta servicio a dicho UE.

- De acuerdo con un segundo aspecto, la invención ofrece una Entidad de Administración de Movilidad, MME, para un Sistema de Paquetes Evolucionado, EPS. La MME se configura para establecer una clave de seguridad, K_{eNB} , para la protección del tráfico RRC/UP entre un UE y un eNodeB que presta servicio al UE. La MME comprende medios para recibir una SOLICITUD DE SERVICIO NAS del UE, 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} , compartida con dicho UE, así como medios para enviar dicho K_{eNB} derivado al eNodeB que presta servicio a dicho UE.
- El primer y segundo aspecto además ofrece métodos, así como los correspondientes medios, de acuerdo con los cuales la MME puede derivar el K_{eNB} del NAS_U_SEQ y el K_{ASME} usando una Función Seudo-Aleatoria, PRF. La MME 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. Adicionalmente, la MME puede regresar una indicación de la NAS_U_SEQ recibida al UE, y el NAS_U_SEQ puede incluirse en el mensaje de configuración que reenvía el K_{eNB} al eNodeB. Por lo tanto, el UE no tiene que recordar el NAS_U_SEQ enviado a la MME.
- De acuerdo con un tercer aspecto, la invención ofrece un método en un Equipo de Usuario, UE, de un Sistema Evolucionado de Paquetes, 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, 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.
- De acuerdo con un cuarto aspecto, la invención ofrece un Equipo de Usuario, UE, adaptado para un Sistema de Paquetes Evolucionado, EPS. El UE 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, 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.
- 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. Adicionalmente, el UE puede almacenar el NAS_U_SEQ de la Solicitud de Servicio NAS enviada a la MME, o, alternativamente,

recibir una indicación de la NAS_U_SEQ de la Solicitud de Servicio NAS enviada a la MME, regresada de la MME por medio del eNodeB. Esta representación alternativa tiene la ventaja de que el UE no tiene que recordar el NAS_U_SEQ enviado a la MME. El UE 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.

BREVE DESCRIPCIÓN DE LAS GRÁFICAS

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

- La Figura 1 es un diagrama de señales que ilustra una Solicitud de Servicio convencional accionada por un UE 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 en un mensaje de SOLICITUD DE SERVICIO NAS;
- La Figura 3 es un diagrama de flujo que ilustra la derivación del K_eNB por parte del UE y la MME;
- La Figura 4 es un diagrama de señales que ilustra una segunda representación de esta invención en la cual la MME regresa el NAS_U_SEQ recibido al UE;
- 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), y la Figura 6b ilustra a manera de esquema un UE, ambos provistos con medios para derivar la clave de seguridad K_eNB.

DESCRIPCIÓN DETALLADA

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.

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 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 contador de secuencia del enlace ascendente, NAS_U_SEQ , del mensaje de Solicitud de Servicio NAS enviado del UE a la MME, accionando así el establecimiento del contexto de seguridad UP/PPC en el eNodeB.

Cuando el UE está en modo INACTIVO, existe un contexto de seguridad NAS y comprende es decir, los anteriormente descritos K_{NAS_enc} , K_{NAS_int} , 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, en particular los algoritmos de codificación e integridad.

La protección de los mensajes NAS se basa en las claves de seguridad NAS, 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 orden y los bits de bajo orden recibidos.

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

En S1 y S2 del diagrama convencional de señales en la Figura 1, una SOLICITUD DE SERVICIO NAS, que comprende un contador de secuencia del enlace ascendente, NAS_U_SEQ , se reenvía del UE a la MME, y el mensaje de Solicitud de Servicio NAS se protege en su integridad basándose en dicho NAS_U_SEQ . La MME 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 antes.

De ahí en adelante, de acuerdo con esta invención, la MME 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 enviará el K_{eNB} derivado al eNodeB, o simultáneamente, en el mensaje de señal, la Solicitud de Configuración de Contexto Inicial (SI-AP).

En la señal S5, el eNodeB envía un Emplazamiento de Portador de Radio y un mensaje de configuración de seguridad (Comando de Modo de Seguridad) al UE. 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 implícitamente será una confirmación de la SOLICITUD DE SERVICIO NAS de los UEs, 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 deriva el K_{eNB} basándose al menos en el NAS_U_SEQ y el K_{ASME} , usando una función convencional de derivación de claves, tras la recepción del mensaje en la señal S5, si no se realizó antes. De ahí en adelante, el eNodeB y el UE establecerá 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 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 incluye el contador de secuencia del enlace ascendente, NAS_U_SEQ, o solo bits de bajo orden que indica el NAS_U_SEQ, en el mensaje de configuración SI-AP, en la señal S4, enviada al eNodeB, en cuyo caso esta información es reenviada al UE del eNodeB durante el establecimiento del contexto RRC/UP. En este caso, el UE podrá retomar la indicación del NAS_U_SEQ del eNodeB para la derivación del K_{eNB} , y no tiene que conservar el NAS_U_SEQ del mensaje de SOLICITUD DE SERVICIO NAS enviado a la MME en las señales S1 y S2.

La Figura 2 ilustra la primera representación de esta invención, en donde el UE conserva el NAS_U_SEQ del mensaje inicial del SOLICITUD DE SERVICIO NAS, en la señal S21, para la derivación de K_{eNB} en la señal S24. La MME recibirá el NAS_U_SEQ del UE en la señal S21, o solo bits de bajo orden que indica el NAS_U_SEQ, y derive el K_{eNB} basándose en el NAS_U_SEQ y el K_{ASME} en S22. La MME reenvía el K_{eNB} derivado al eNodeB en la señal S23.

De ahí en adelante, no ilustrado en la Figura 2, el eNodeB y el UE 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; $K_{eNB} = \text{PRF}(K_{ASME}, \text{NAS_U_SEQ}, \dots)$.

Además, como se ilustra con los puntos en la función PPF antes descrita, la función de derivación K_{eNB} puede tener valores adicionales de entrada convencionales, tales como la identidad eNodeB.

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 recibe el mensaje de Solicitud de Servicio NAS del UE, 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 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 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/PPC 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 a la MME en el paso 31, y establecer el contexto de seguridad UP/PPC del K_{eNB} derivado.

En la primera representación de esta invención, el UE almacena el NAS_U_SEQ transmitido a la MME en el mensaje inicial de SOLICITUD DE SERVICIO NAS, y usa el número de secuencia almacenado para derivar el K_{eNB} .

La Figura 4 es un diagrama de señales que ilustra una segunda representación de esta invención, en donde el UE no tiene que almacenar el NAS_U_SEQ. Por el contrario, la MME regresará una indicación del NAS_U_SEQ recibido al UE, por medio del eNodeB. 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 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 reenviará el NAS_U_SEQ al UE, en la señal S44. De ahí en adelante, el UE derivará el K_{eNB} de al menos el K_{ASME} y del NAS_U_SEQ regresado por la MME, en la señal S45. De la clave de seguridad derivada, K_{eNB} , el eNodeB y el UE establecerá el contexto de seguridad UP/PPC, permitiendo así un tráfico UP/PPC 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 por la MME. 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 recibe el mensaje de Solicitud de Servicio NAS del UE, 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 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 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 usa la clave de seguridad recibida, K_eNB, para establecer un contexto de seguridad UP/PPC. El NAS_U_SEQ recibido se reenvía al UE 11 por el eNodeB, en el paso 55, y en el paso 56, el UE 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/PPC compartido con el eNodeB.

La derivación del K_eNB por la MME, en el paso 53, y por el UE, 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 de tráfico UP/PPC entre un UE y un eNodeB de servicio. La MME 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 por medio de una interfaz SI-MME. Además, en la MME 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.

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 (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 que presta servicio al UE.

La Figura 6b ilustra un UE 11 (Entidad de Usuario) de acuerdo con esta invención, el UE 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/PPC intercambiado con su eNodeB de servicio. El UE 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.

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, por medio del eNodeB de servicio, 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 y el UE, 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.

REIVINDICACIONES

1. Un método en una Entidad de Administración de Movilidad (13), MME, de un Sistema Evolucionado de Paquetes, EPS, de establecer una clave de seguridad, K_{eNB} , para proteger el tráfico RRC/UP entre un Equipo de Usuario (11), UE, y un eNodeB (12) que presta servicio al UE, 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 al menos dicho NAS_U_SEQ recibido y de una clave almacenada de Entidad de Administración de Acceso de Seguridad, K_{ASME} , compartida con dicho UE;
 - Reenviar (34) dicho K_{eNB} derivado al eNodeB (12) que presta servicio al UE.
2. Un método en una MME 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 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 de acuerdo con cualquiera de las reivindicaciones previas, 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 de acuerdo con cualquiera de las reivindicaciones previas, 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 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 Evolucionado de Paquetes, 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, solicitud que indica un número de secuencia NAS de enlace ascendente, NAS_U_SEQ;

- Derivar (55, 56) el 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.
- 5 6. Un método en un UE de acuerdo con la reivindicación 7, en donde el K_{eNB} se deriva del NAS_U_SEQ y el K_{ASME} usando una Función Seudo-Aleatoria, PRF.
- 9. Un método en un UE 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.
- 10 10. Un método en un UE 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.
- 11. Un método en un UE de acuerdo con cualquiera de las reivindicaciones 7 - 9, que comprende el paso de recibir (55) una indicación del NAS_U_SEQ de la Solicitud de Servicio NAS enviada a la MME, de regreso de la MME (13) por medio del eNodeB (12).
- 15 12. Un método en un UE 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.
- 13. 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 EPC/UP entre un UE (11) y un eNodeB (12) que presta servicio al UE, donde la MME se caracteriza por:
 - 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 al menos dicho NAS_U_SEQ recibido y de una

25 clave de Entidad de Administración de Acceso de Seguridad almacenada, K_{ASME} , compartida con dicho UE;
 - Medios (64) para enviar dicho K_{eNB} derivado al eNodeB que presta servicio a dicho UE.
- 14. Una MME de acuerdo con la reivindicación 13, dispuesta para derivar el K_{eNB} del

30 NAS_U_SEQ y el K_{ASME} usando una Función Seudo-Aleatoria, PRF.
- 15. Una MME 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 de acuerdo con cualquiera de las reivindicaciones 13 - 15, dispuesta para comprobar la integridad la Solicitud de Servicio NAS recibida del UE (11).

17. Una MME 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.

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 EPC/UP intercambiado con un eNodeB de servicio (12), UE que se caracteriza por:

10 - 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;

- Medios (67) 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).

15 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 Pseudo-Aleatoria, PRF.

20. Un UE 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).

21. Un UE 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 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 por medio del eNodeB (12).

23. Un UE 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)

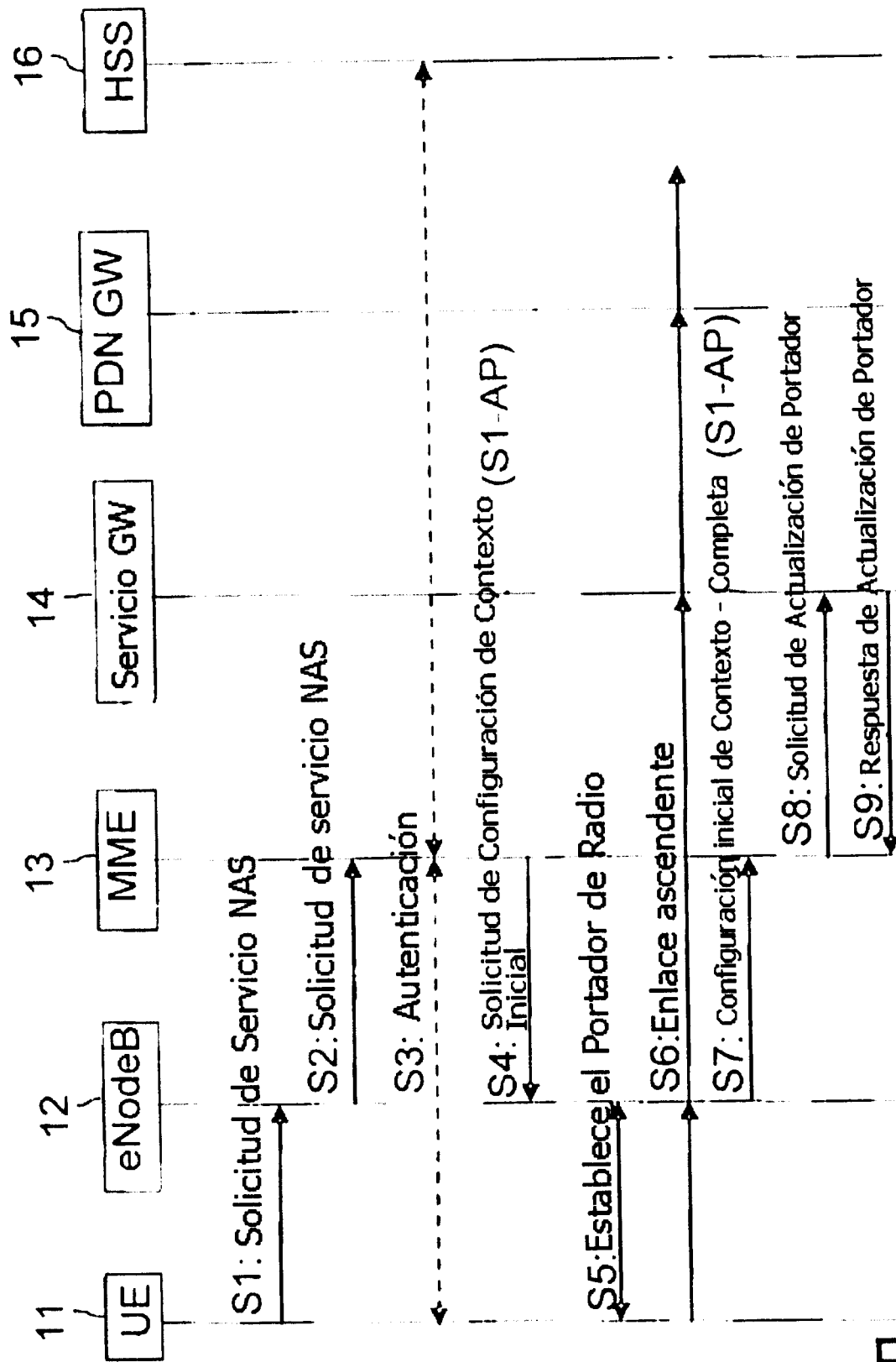


Fig. 1

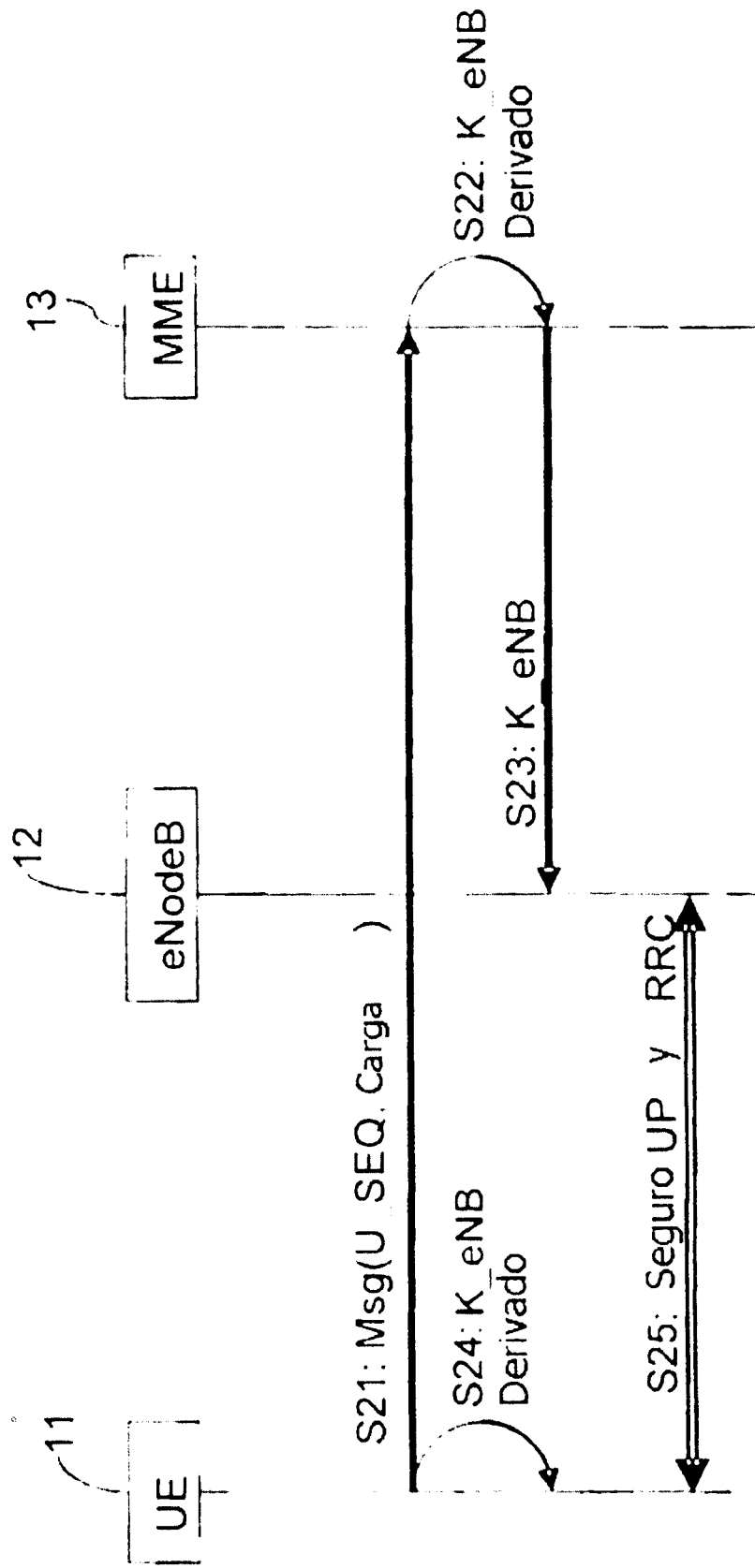


Fig. 2

3/6

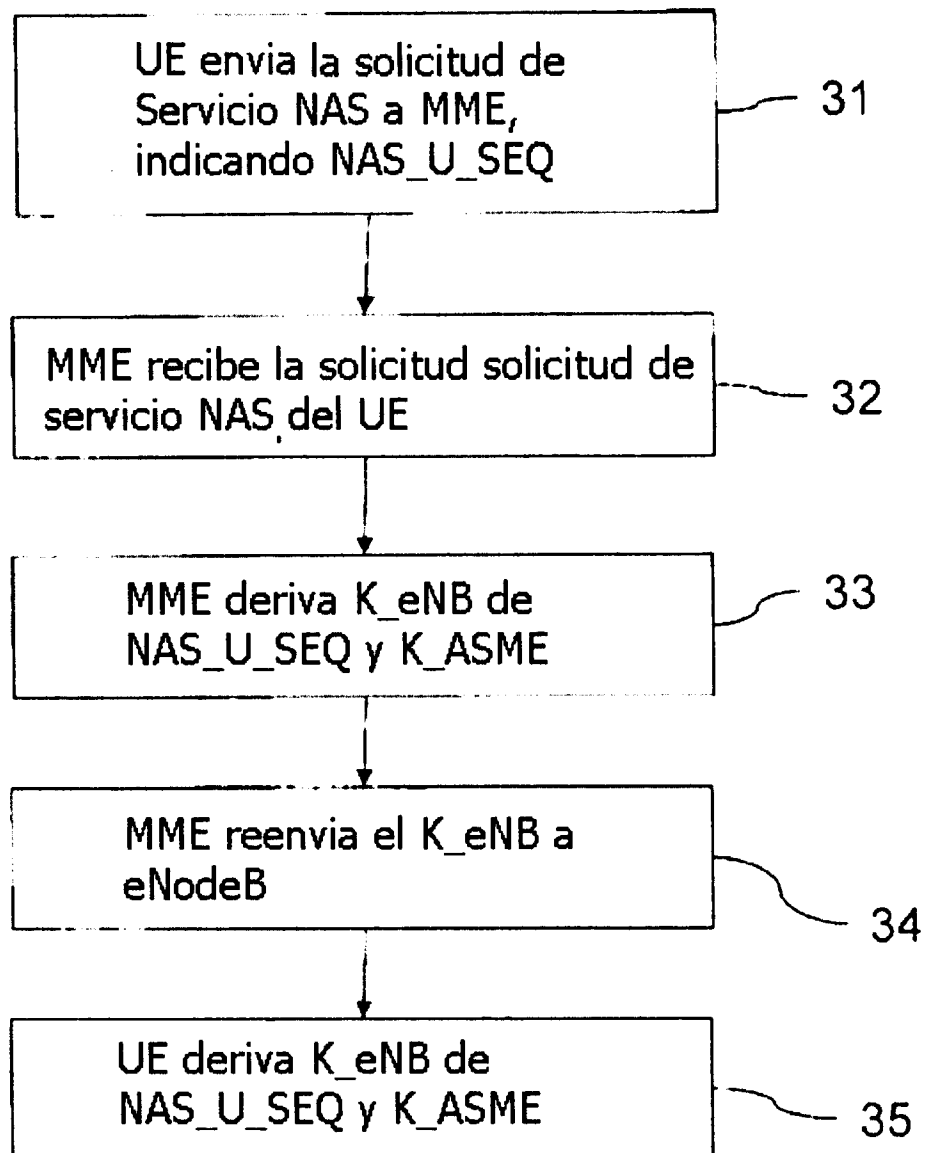


Fig. 3

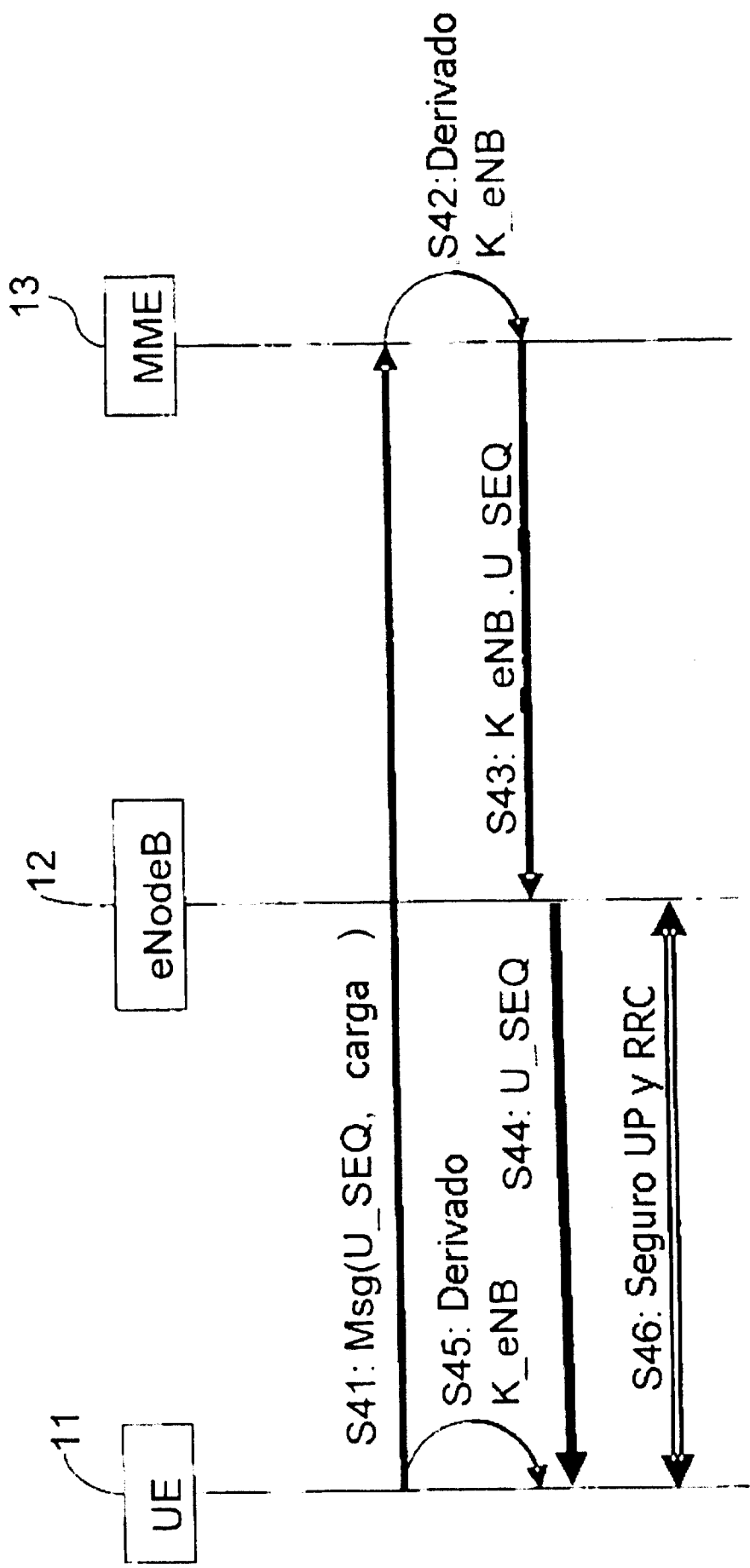


Fig. 4

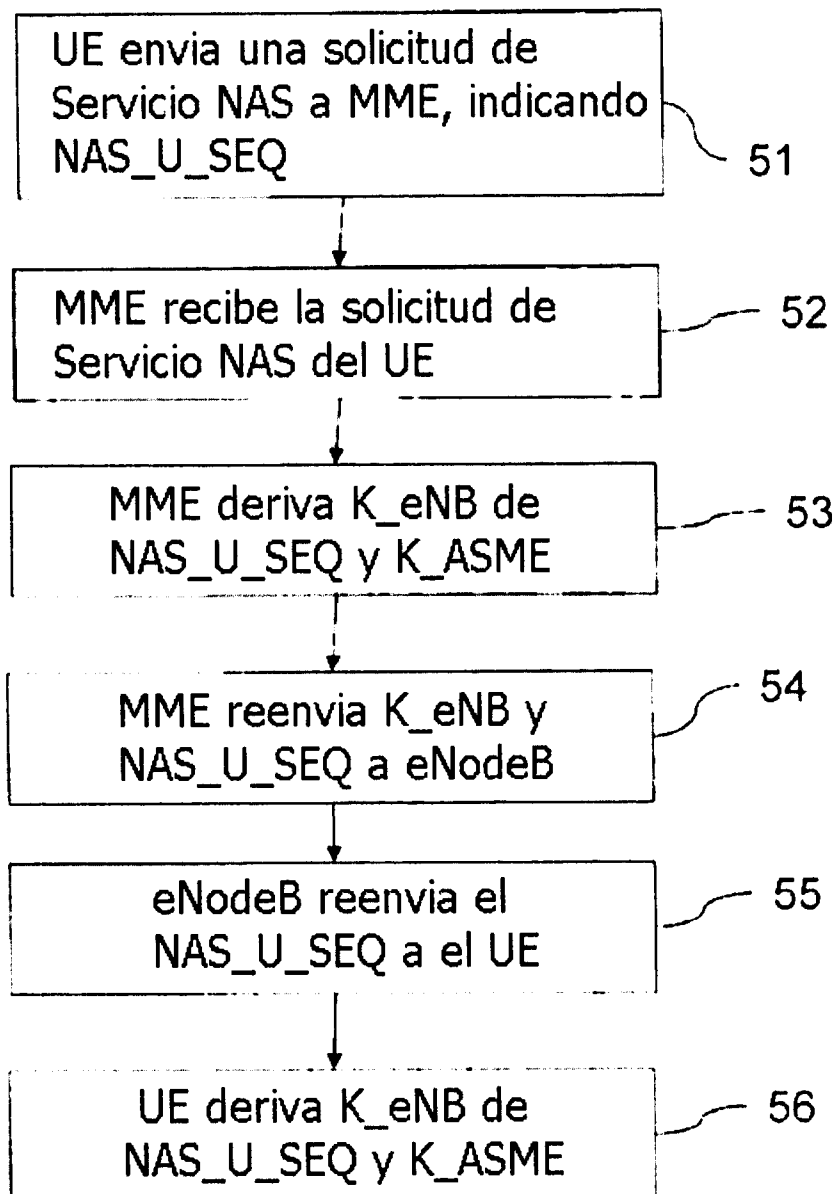


Fig. 5



Industria y Comercio

SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

DIVISIÓN DE NUEVAS CREACIONES

TARJETA ARCHIVO PROPIETARIOS

PATENTE DE INVENCION ____ PCT X MODELO DE UTILIDAD ____ DISEÑO INDUSTRIAL ____

(21) N° de solicitud:

(22) Fecha de solicitud: 5 DE FEBRERO DE 2010

(51) Clasificación Internacional:

(71) Solicitante(s) **Telefonaktiebolaget L M Ericsson (publ)**

(72) Inventor(es) **Rolf BLOM; Gunnar MILDH y Karl NORRMAN**

(74) Agente: **HUMBERTO RUBIO CAMACHO**

(30) Prioridad

(31) No. Prioridad

(32) Fecha

(33) País

ESTADOUNIDENSE

60/972,955

17/09/2007

ESTADOS UNIDOS DE AMERICA

(85) Fecha inicio fase nacional:

(87) Publicación internacional

(86) Datos relativos a la presentación de la solicitud PCT

Fecha: **26/03/2009**

Fecha de presentación de la solicitud: **20/05/2008**

N° publicación: **WO 2009/038522**

No. de solicitud: **PCT/SE2007/050683**

(54) Título: **Método y disposición en un sistema de telecomunicaciones**

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

DIVISION DE NUEVAS CREACIONES

TARJETA ARCHIVO TEMATICO

PATENTE DE INVENCION _____ PCT X MODELO DE UTILIDAD _____ DISEÑO INDUSTRIAL _____

(1) N° de solicitud: _____ (22) Fecha de solicitud: **5 DE FEBRERO DE 2010**

(3) Clasificación Internacional: _____

(71) Solicitante(s) **Telefonaktiebolaget L M Ericsson (publ)**

(72) Inventor(es) **Rolf BLOM; Gunnar MILDH y Karl NORRMAN**

(74) Agente: **HUMBERTO RUBIO CAMACHO**

(30) Prioridad	(31)	No. Prioridad	(32)	Fecha	(33)	País
ESTADOUNIDENSE		60/972,955		17/09/2007		ESTADOS UNIDOS DE AMERICA

(35) Fecha inicio fase nacional:

(36) Datos relativos a la presentación de la solicitud PCT

Fecha de presentación de la solicitud: **20/05/2008**

No. de solicitud: **PCT/SE2008/050591**

(37) Publicación internacional:

Fecha: **26/03/2009**

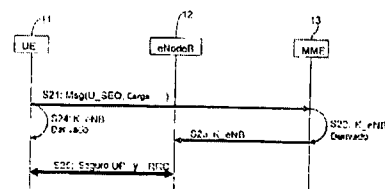
No. de publicación: **WO 2009/038522**

(54) Título: **Método y disposición en un sistema de telecomunicaciones**

Resumen:

Un método en una Entidad de Administración de Movilidad (13), MME, de un Sistema Evolucionado de Paquetes, EPS, de establecer una clave de seguridad, K_{eNB}, para proteger el tráfico RRC/UP entre un Equipo de Usuario (11), UE, y un eNodeB (12) que presta servicio al UE, 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 al menos dicho NAS_{U_SEQ} recibido y de una clave almacenada de Entidad de Administración de Acceso de Seguridad, K_{ASME}, compartida con dicho UE;
- Reenviar (34) dicho K_{eNB} derivado al eNodeB (12) que presta servicio al UE.



HUMBERTO RUBIO & CIA LTDA.
ABOGADOS

Propiedad Industrial e Intelectual
BOGOTA - COLOMBIA

PODER

El abajo firmado

TELEFONANTIEBOLAGET L. M. ERICSSON
(publ.)
domiciliado en
SE-164 83 Stockholm, Suecia

por el presente conferimos poder amplio y suficiente

HUMBERTO RUBIO y/o TINENE STOL

para solicitar ante las oficinas y autoridades correspondientes la obtención de registros, renovaciones, trasposes y en general todo lo relacionado con el mantenimiento, obtención y protección de sus marcas de fábrica, denominaciones comerciales, marcas de comercio y patentes, licencias sanitarias a cuyo efecto la facultad para dar ante dichas autoridades todos los pasos necesarios en cumplimiento del objeto indicado; elevar solicitudes, descripciones, protestas, declaraciones, apelaciones y reclamos; abonar todos los impuestos y costas de cualquier otro pago determinados por la Ley; recibir todos los documentos presentados, solicitar testimonios, desistirse y enmendar solicitudes, cobrar y percibir para oponerse y protestar contra cualquier solicitud, que a juicio del apoderado, pudieran prestarse a confusión o infringir o de cualquier modo perjudicar las marcas, denominaciones o patentes del Mandante. A los mandatarios se les otorga autorización amplia y bastante para contestar todos los reclamos y las demandas presentadas ante autoridades administrativas y judiciales, desistirse de procedimientos, transar conflictos, pudiendo así mismo sustituir este Poder en todo o en parte y revocar dichas sustituciones.

Dado y firmado hoy
24 de septiembre de 1999
en Estocolmo
Suecia

Firma

NOTARIZATION AND LEGALIZATION BEFORE
COLOMBIAN CONSULATE IS REQUIRED.

Para patentes, marcas, diseños, marcas de fábrica de comercio y servicios, marcas y nombres comerciales, licencias y registro sanitario.
For patents, designs, trademarks, design, commercial names, licenses, health registrations

POWER OF ATTORNEY

The undersigned

TELEFONANTIEBOLAGET L. M. ERICSSON
(publ.)
From

SE-164 83 Stockholm, Sweden
hereby grant full and sufficient Power of Attorney to

HUMBERTO RUBIO y/o TINENE STOL

to apply before the proper officers and authorities the issue of registrations, renewals, assignments, proofs of renewals and in general all that is related to the maintenance, obtention and protection of its trademarks, tradenames, commercial marks, patents and sanitary licenses; to which and it empowers them to take all steps necessary before said authorities for the object stated; to file petitions, prepare descriptions, make protests, declarations, appeals and objections; pay taxes and other charges required by law; apply for certifications, receive documents and take testimony abandon and amend applications and collect refunds; to oppose, ask for the cancellation of and protest any application or registration which in their judgment could lead to confusion or could be considered an infringement or could in any form prejudice the undersigned's trademarks, tradenames, patents and commercial marks. To the said mandataries sufficient Power is granted hereby to answer in the matter of all claims and demands that maybe presented, before administrative or judicial officers of any state, giving them likewise Power to abandon proceeding, settle conflicts, substitute these present in whole or in part and revoke such substitutions.

Given and signed this
24th day of September 1999
in Stockholm, Sweden

Signature TELEFONANTIEBOLAGET L. M.
ERICSSON (publ.)

Erling Blomné
Senior Vice
President

Walo von Greyer
Vice President
Intellectual
Property





HUMBERTO RUBIO & CIA LTDA.
ABOGADOS

Propiedad Industrial e Intelectual



CERTIFICADO NOTARIAL (Individual)

A los 19 días del mes de Septiembre de 1999 ante mí,
Notario Público de comparecencia personalmente

a quien(es) doy fe de conocer y me consta que es(son)
la(s) persona(s) firmante(s) del documento que
precede, y quien(es) tiene(n) capacidad legal para
otorgarlo.

CERTIFICADO NOTARIAL (SOCIEDAD)

Hoy 20 de Septiembre 19 99
comparecieron personalmente
los señores Erling Blommé y
Walo von Greyerz

a quienes conozco como la(s) persona(s) que
firma(n) este documento en representación de la
sociedad/compañía denominada

TELEFONANTIEBOLAGET LM ERICSSON (publ) TELEFONANTIEBOLAGET LM ERICSSON (publ)

Certifico:

a) Que

TELEFONANTIEBOLAGET LM ERICSSON (publ) That TELEFONANTIEBOLAGET LM ERICSSON (publ)
es una sociedad/compañía legalmente constituida y
existente de acuerdo con las Leyes de
Suecia

b) Que el domicilio de dicha sociedad/compañía es
SE-164 83 Estocolmo, Suecia

c) Que el objeto u objetos para los cuales se otorga el
presente poder están comprendidos dentro del objeto
social de la mencionada sociedad/compañía.

d) Que los señores Erling Blommé y
Walo von Greyerz
están autorizados para otorgar el presente poder. Lo
anterior está probado por medio de los siguientes
documentos, que certifico he visto:

Certificado otorgado por
Autoridad competente

Ciudad Estocolmo, hoy 20 de Septiembre
de 1999

[Signature]
Notario Público



NOTARIAL CERTIFICATE (Individual)

On this 19 day of September 19 99 before me, a Notary
Public of Sweden personally appeared to
me known, and known to me to be the person(s) who
executed the foregoing document, and who has
(have) legal capacity to execute it.

NOTARIAL CERTIFICATE (Corporation)

On this 20 day of September 19 99
personally appeared

whom I know to be the person(s) who signed this
document as representative(s) of the
corporation/company named

I Certify:

a) That TELEFONANTIEBOLAGET LM ERICSSON (publ)
is a corporation/company legally constituted and in
existence accordance with the law of

Sweden

b) That the domicile of said corporation/company is
SE-164 83 Stockholm, Sweden

c) That the purpose or purposes for which the present
Power of Attorney is granted are comprised within
the object set forth in the charter of the mentioned
corporation/company.

d) That Mr(s).

is authorized to grant the present Power of Attorney.
The aforesaid were duly proven through the
following documents and I duly verify having seen
them State
This day of 19

Public Notary

EL CONSUL DE COLOMBIA

En Estocolmo, Suecia

CERTIFICA:

Que el señor Erling Blomme
Walo van Frijns
quien firma el documento que antecede ejercia para la
fecha el cargo de Representantes

de la Sociedad Telefonistiebolaget
LM Ericsson (publ)
que existe de conformidad con las leyes de Suecia

según se acreditó con los documentos que tuve a la vista.

Fecha 1999-10-01 No: 211

Maria Smith Rueda
MARIA SMITH RUEDA
Encargada de las Funciones Consulares



PAGADO	
Impuesto de Timbre	
<i>Grete</i>	Dólares US\$ <u>7</u>
Derechos Consulares	
<i>Green</i>	Dólares US\$ <u>100</u>

NO SE ASUME
RESPONSABILIDAD DEL TEXTO
1999 OCT 11 A O 38
JEFE DE LEGALIZACIONES
MAYOR EN JEFE

MINISTERIO DE RELACIONES
EXTERIORES
Ramiro
199622
CITA PARA APARECER EN EL
QUOTIDIANO DESEMPLEO
AL SERVICIO DE FUNDACIONES





PATENTE DE INVENCION ☐

MODELO

- ☐ Indicación que se solicita una patente.
 - ☐ Datos de identificación del solicitante o de la persona que presenta la solicitud
 - ☐ Descripción de la invención
 - ☐ Dibujos de ser estos pertinentes
 - ☐ Comprobante de pago de las tasas establecidas (De ser el caso formato de descuento)
- Completa ☐ Incompleta ☐

PATENTE DE INVENCION PCT ☒ MODELO DE UTILIDAD PCT ☐ Art.33 Decisión 486/00, Circular Única

- ☒ Indicación que se solicita una PCT
 - ☒ Copia de la solicitud en español, tal como fue presentada inicialmente (capítulo descriptivo, reivindicatorio, resumen)
 - ☒ Dibujos de ser estos pertinentes
 - ☒ Comprobante de pago de las tasas establecidas (de ser el caso formato de descuento)
- Completa ☒ Incompleta ☐

DISEÑO INDUSTRIAL ☐

(Art. 119 Decisión 486/00)

- ☐ Indicación que se solicita Diseño industrial
 - ☐ Datos de identificación del solicitante o de la persona que presenta la solicitud
 - ☐ Representación gráfica y fotográfica del Diseño industrial o muestra del material que incorpora el diseño
 - ☐ Comprobante de pago de las tasas establecidas
- Completa ☐ Incompleta ☐

ESQUEMA DE TRAZADO ☐

(Art. 92 Decisión 486/00)

- ☐ Indicación que se solicita un esquema de trazado
 - ☐ Datos de identificación del solicitante o de la persona que presenta la solicitud
 - ☐ Representación gráfica de un esquema de trazado
 - ☐ Comprobante de pago de las tasas establecidas
- Completa ☐ Incompleta ☐



Bogotá D.C.,
2020

Doctor(a)
RUBIO CAMACHO HUMBERTO
Apoderado(a) y/o Representante de
TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)

REFERENCIA	Radicación No.	10 012466
	Solicitud internacional	PCT/SE2008/050591
	Fecha inicio fase nacional	17/04/2010
	Trámite	11
	Evento	378
	Actuación	430
	Oficio No.	<u>06.149</u>

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

1. El solicitante debe presentar un nuevo título que permita identificar la materia de la cual trata la solicitud, ya que el título relacionado no se encuentra con la precisión necesaria para identificar claramente el objeto de la solicitud de patente. (Regla 4.3 PCT, Art 26-27 D-486, Circular única 5.2.9)

2. La solicitud no contiene la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante, conforme a lo establecido por el artículo 26 literal f) de la Decisión 486 de la Comisión de la Comunidad Andina. Cuando se trate de documentos otorgados en el extranjero, estos deberán legalizarse de conformidad con lo dispuesto por los artículos 259 y 260 del Código de Procedimiento Civil. Cuando se trate de las declaraciones a que hace referencia la Regla 4.17 ii) del Tratado de Cooperación en Materia de Patentes PCT., el alcance de las tales declaraciones se determinará según indiquen claramente una cesión de derechos del inventor al solicitante o su causante, de conformidad con lo dispuesto en el numeral 5.2.15 del Capítulo Quinto, Título X de la Circular Única de Superintendencia de Industria y Comercio.

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Continúa en la página siguiente...