(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 968 518**

(51) Int. Cl.:

H04W 12/0431 (2011.01)
H04L 9/40 (2012.01)
H04W 12/062 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.10.2007 E 20185797 (6)**

(97) Fecha y número de publicación de la concesión europea: **20.12.2023 EP 3761598**

(54) Título: **Generación de claves para protección en redes móviles de próxima generación**

(30) Prioridad:

20.10.2006 US 852967 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.05.2024

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

LI, CHANGHONG;
ZHANG, DAJIANG;
HIETALA, MIKA P. y
NIEMI, VALTTERI

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Generación de claves para protección en redes móviles de próxima generación

Referencia cruzada a solicitud relacionada:

Esta solicitud reivindica la prioridad de la Solicitud de Patente Provisional de Estados Unidos N° 60/852.967, presentada el 20 de octubre de 2006.

Campo y antecedentes de la invención

La presente invención se refiere al campo de la evolución de arquitectura de largo plazo (LTE/SAE) de 3GPP (Proyecto de Asociación de Tercera Generación). En particular, la invención se refiere a la generación de claves tales como claves de Cifrado (CKs) y claves de protección de integridad (IK) en 3GPP LTE/SAE.

3GPP LTE/SAE requiere claves separadas utilizadas para la protección de AS (estrato de acceso), NAS (estrato sin acceso) y plano U (plano de usuario).

En UMTS (Sistema Universal de Telecomunicaciones Móviles) se proporciona un mecanismo de seguridad usando un protocolo AKA (Autenticación y Acuerdo de Clave) basándose en una estrategia de "desafío-respuesta", en la que se obtiene una clave de cifrado y una clave de protección de integridad usando un valor aleatorio RAND.

La publicación de solicitud de patente de Estados Unidos Nº US-2006/171541 A1 se refiere a crear una primera clave criptográfica y una segunda clave criptográfica por un terminal de radio móvil y por un ordenador de la red de comunicaciones domésticas mediante el uso de materiales de clave de autenticación. La primera clave criptográfica se transmite al ordenador de la red de comunicaciones visitada, y la segunda clave criptográfica se transmite a un ordenador servidor de aplicaciones.

Resumen de la invención

Para en caso de que un UE (equipo de usuario) funcione desde un sistema de comunicación 2G/3G (segunda generación/tercera generación) a LTE, debería haber una forma de derivar las claves para el plano de AS, NAS y U.

En otras palabras, se necesitan claves separadas para la protección de señalización NAS entre el UE (Equipo de Usuario) y la MME (movilidad del elemento de gestión) y para la protección del plano de usuario entre el UE y el UPE. Además, también se necesita una clave diferente para proteger la señalización de RRC usada entre el eNB y el UE.

Según un aspecto de la presente invención, se proporciona un método, que comprende:

recibir identidades de entidades de red de una segunda red durante un proceso de traspaso del equipo de usuario de una primera red a la segunda red; y calcular un conjunto de claves asociadas para un proceso de autenticación que se realizará en la segunda red usando las identidades de las entidades de red, en donde el conjunto de claves asociadas comprende una clave de cifrado y una clave de protección de integridad, y en donde el cálculo comprende calcular el conjunto de claves asociadas basándose en un valor aleatorio usado en un proceso de autenticación de la primera red, una clave de cifrado usada en un proceso de autenticación de la primera red y una clave de protección de integridad usada en un proceso de autenticación de la primera red.

La primera red puede ser un sistema de comunicación 2G/3G, y la segunda red puede ser la LTE.

Las claves asociadas pueden ser las claves para el plano de AS, NAS y U.

Según una realización de la invención, un conjunto de valores aleatorios asociados a usar en el proceso de autenticación de la segunda red puede calcularse en base al valor aleatorio usado en el proceso de autenticación de la primera red, y el conjunto de claves asociadas puede calcularse basándose en el conjunto de valores aleatorios asociados.

El conjunto de valores aleatorios asociados puede calcularse basándose en el valor aleatorio usando identidades de entidades de red de la segunda red, asociadas las entidades de red a través del proceso de autenticación a realizar en la segunda red.

Según otra realización de la invención, las claves de un proceso de autenticación de la primera red se calculan basándose en el valor aleatorio, y el conjunto de claves asociadas se calcula basándose en las claves usando identidades de entidades de red de la segunda red, estando asociadas las entidades de red a través del proceso de autenticación a realizar en la segunda red.

El valor aleatorio de la primera red puede obtenerse durante un proceso de traspaso de un equipo de usuario desde la primera red a la segunda red. El valor aleatorio de la primera red también puede obtenerse durante un proceso de autenticación realizado en la segunda red.

Las entidades de red pueden comprender al menos una de una estación base, un elemento de gestión de movilidad y un elemento de plano de usuario.

El conjunto de claves asociadas comprende un conjunto de claves de cifrado asociadas y un conjunto de claves de protección de integridad asociadas.

El conjunto de claves asociadas puede comprender una clave utilizada para la protección de estrato de acceso, una clave utilizada para la protección de estrato sin acceso y una clave utilizada para la protección del plano de usuario.

La Figura 1 muestra un diagrama de bloques esquemático que ilustra un equipo de usuario y dispositivos de red según una realización de la invención.

Un dispositivo de red 30 tal como un MME (elemento de gestión de movilidad) comprende una unidad de recepción 31 y una unidad de cálculo 32. El MME 30 también puede comprender una unidad de transmisión 33. La unidad de recepción 31 recibe un valor aleatorio, tal como RAND, usado en un proceso de autenticación de una primera red, tal como un sistema de comunicación 2G/3G. La unidad de cálculo 32 calcula un conjunto de claves asociadas, tales como claves para el plano de AS, NAS y U, para que un proceso de autenticación se realice en una segunda red, tal como LTE, basándose en el valor aleatorio.

La unidad de recepción 31 puede recibir claves del proceso de autenticación de la primera red, tal como CK e IK.

La unidad de recepción 31 puede recibir el valor aleatorio y las claves de un servidor de abonado local. Alternativamente, la unidad de recepción 31 puede recibir el valor aleatorio y las claves de otro elemento de red de la primera red, y la unidad de transmisión 33 puede transmitir las claves al servidor de abonado local. La unidad de recepción 31 puede recibir entonces claves modificadas, tales como CK_{HO} e IK_{HO}, del proceso de autenticación de la primera red desde el servidor de abonado local, y la unidad de cálculo 32 puede calcular el conjunto de claves asociadas basándose en las claves modificadas.

La unidad de cálculo 32 puede calcular el conjunto de claves asociadas usando identidades de entidades de red de la segunda red, estando asociadas las entidades de red a través del proceso de autenticación a realizar en la segunda red, en donde las entidades de red incluyen dicho dispositivo de red.

Según una realización alternativa, la unidad de transmisión 33 transmite las identidades de las entidades de red de la segunda red al servidor de abonado local, y la unidad de recepción 31 recibe un conjunto de claves asociadas para que el proceso de autenticación se realice en la segunda red desde el servidor de abonado local. La unidad de recepción 31 puede recibir el valor aleatorio de antemano desde un otro elemento de red de la primera red, y la unidad de transmisión 33 puede transmitir también el valor aleatorio al servidor de abonado local. La unidad de transmisión 33 puede transmitir las identidades de las entidades de red hacia dichas entidades de red.

Un dispositivo de red 20 mostrado en la Figura 1, tal como un SGSN, comprende una unidad de transmisión 21 que transmite el valor aleatorio usado en el proceso de autenticación de la primera red a un dispositivo de red, tal como el MME 30, de la segunda red durante un proceso de traspaso de un equipo de usuario 10 de la primera red a la segunda red. La unidad de transmisión 21 también puede transmitir las claves del proceso de autenticación de la primera red al dispositivo de red de la segunda red.

El equipo de usuario (UE) 10 mostrado en la Figura 1 comprende una unidad de recepción 11 que recibe las identidades de las entidades de red de la segunda red, y una unidad de cálculo 12 que calcula un conjunto de claves asociadas para el proceso de autenticación que se va a realizar en la segunda red usando las identidades de las entidades de red. El UE 10 puede recibir las identidades del MME 30. Las identidades pueden recibirse durante un acceso inicial hacia la segunda red y/o durante un proceso de traspaso del UE 10 de la primera red a la segunda red.

Un dispositivo de red tal como un eNB o eRAN (red de acceso por Radio evolucionada) 50 que se muestra en la Figura 1 comprende una unidad de cálculo 51 que calcula un conjunto de claves asociadas para que el proceso de autenticación se realice en la segunda red mediante el uso de identidades de entidades de red de la segunda red, las entidades de red que se asocian a través del proceso de autenticación a realizar en la segunda red, en donde las entidades de red incluyen dicho dispositivo de red 50.

Finalmente, un dispositivo de red tal como un HSS 40 mostrado en la Figura 1 comprende una unidad de recepción 41 que recibe las claves del proceso de autenticación de la primera red, una unidad de cálculo 42 que calcula claves modificadas basándose en las claves, y una unidad de transmisión 43 que transmite las claves modificadas a un elemento de red de la segunda red, tal como el MME 30. Las claves pueden ser recibidas por la unidad de recepción 41 del MME 30.

Según una realización alternativa, la unidad de recepción 41 recibe el valor aleatorio usado en el proceso de autenticación de la primera red y las identidades de las entidades de red de la segunda red, las entidades de red están asociadas a través de un proceso de autenticación que se realizará en la segunda red, la unidad de cálculo 42 calcula un conjunto de claves asociadas para que el proceso de autenticación se realice en la segunda red basándose en el valor aleatorio usando las identidades, y la unidad de transmisión 43 transmite el conjunto de claves asociadas a un elemento de red de la segunda red, tal como el MME 30. El valor aleatorio y las identidades pueden ser recibidos por la unidad receptora 41 del MME 30.

Según una realización adicional, la unidad de transmisión 43 del HSS 40 transmite el valor aleatorio y las claves del proceso de autenticación de la primera red al MME 30, por ejemplo, tras una solicitud de datos de autenticación transmitida desde la unidad de transmisión 33 del MME 30 al HSS 40.

Cabe señalar que los dispositivos de red y el terminal y el equipo de usuario que se muestran en la Figura 1 pueden tener una funcionalidad adicional para trabajar, por ejemplo, como SGSN, MME, eRAN, HSS y UE. Aquí las funciones de los dispositivos de red y el equipo de usuario relevantes para comprender los principios de la invención se describen utilizando bloques funcionales como se muestra en la Figura 1. La disposición de los bloques funcionales de los dispositivos de red y el equipo de usuario no se considera limitativa de la invención, y las funciones pueden realizarse en un bloque o dividirse en subbloques.

Para el fin de la presente invención, como se ha descrito anteriormente, se debe tener en cuenta que

- las etapas del método que probablemente se implementarán como partes de código de software y se ejecutarán usando un procesador en uno de los dispositivos de red o el terminal son independientes del código de software y se pueden especificar usando cualquier lenguaje de programación conocido o desarrollado en el futuro;

- las etapas y/o unidades del método que probablemente se implementarán como componentes de hardware en uno de los dispositivos de red o en el terminal son independientes del hardware y se pueden implementar usando cualquier tecnología de hardware conocida o desarrollada en el futuro o cualquier híbrido de estas, tales como MOS, CMOS, BiCMOS., ECL, TTL, etc., usando por ejemplo componentes ASIC o componentes DSP, como ejemplo;

- generalmente, cualquier etapa del método es adecuada para implementarse en software o hardware sin cambiar la idea de la presente invención.

- los dispositivos pueden implementarse como dispositivos individuales, pero esto no excluye que se implementen de forma distribuida a través de todo el sistema, siempre que se conserve la funcionalidad del dispositivo.

La presente invención proporciona una extensión que no requiere cambios en el protocolo AKA.

Según una realización de la invención, tampoco se requieren cambios en un servidor de abonado local.

Breve descripción de los dibujos

La Figura 1 muestra un diagrama de bloques esquemático que ilustra un equipo de usuario y elementos de red según una realización de la invención.

La Figura 2 muestra un diagrama de señalización que ilustra la generación de claves según la presente invención durante un acceso inicial.

La Figura 3 muestra un diagrama de señalización que ilustra la distribución/conversión de claves durante un procedimiento de traspaso a partir de un sistema de comunicación 2G/3G a LTE.

Descripción de las realizaciones preferidas

Para generar claves separadas para la protección de tipo AS, NAS y U, según una solución (1) un valor aleatorio más largo y (es decir, 3 veces más largo que el RAND usado en UMTS) se usa, que puede seccionarse en RANDrrc, RANDnas y RANDupe.

$$RAND=RANDrrc||RANDnas||RANDupe$$

Las claves de cifrado separadas y las claves de protección de integridad para el plano de AS, NAS y U pueden calcularse de la siguiente manera:

$$CKrrc = f3(K, RANDrrc)$$

$$CKnas = f3(K, RANDnas)$$

CKupe = f3(K, RANDupe)

IKrrc = f4(K, RANDrrc)

IKnas = f4(K, RANDnas)

IKupe = f4(K, RANDupe)

en donde CKrrc es la clave de cifrado para AS, CKnas es la clave de cifrado para NAS y CKupe es la clave de cifrado para el plano U, IKrrc es la clave de protección de integridad para AS, IKnas es la clave de protección de integridad para NAS e IKupe es la clave de protección de integridad para plano U. f3 y f4 son funciones para generar los conjuntos de claves anteriores y pueden predeterminarse de antemano. K en las fórmulas anteriores puede ser una clave de cifrado o una clave de protección de integridad en sí misma o un parámetro predeterminado.

Sin embargo, preferiblemente la longitud de RAND es la misma que en el UMTS. Según una realización de la invención presentada por la solución (2), RAND se usa junto con diferentes identidades de plano de AS y NAS para generar RANDrrc, RANDnas y RANDupe.

RANDrrc = KDF (RAND, IDas)

RANDnas = KDF (RAND, IDnas)

RANDupe = KDF (RAND, IDupe)

Por ejemplo, KDF puede ser una función XOR, IDas puede ser la identidad de una BS (Estación Base) o eNB (Nodo B evolucionado), IDnas puede ser la identidad de un MME (Elemento de Gestión de Movilidad) e IDupe puede ser la identidad de un UPE (Elemento de Plano de Usuario).

A continuación, RANDrrc, RANDnas y RANDupe se usan para generar las correspondientes CK e IK para el plano de AS o RRC (Control de Recursos de Radio), NAS y U.

CKrrc = f3(K, RANDrrc)

Cknas = f3(K, RANDnas)

Ckupe = f3(K, RANDupe)

Ikrrc = f4(K, RANDrrc)

Iknas = f4(K, RANDnas)

Ikupe = f4(K, RANDupe)

en donde CKrrc es la clave de cifrado para AS o RRC, CKnas es la clave de cifrado para NAS y CKupe es la clave de cifrado para el plano U, IKrrc es la clave de protección de integridad para AS, IKnas es la clave de protección de integridad para NAS e IKupe es la clave de protección de integridad para el plano U. f3 y f4 son funciones para generar los conjuntos de claves anteriores y pueden predeterminarse de antemano. K en las fórmulas anteriores puede ser una clave de cifrado o una clave de protección de integridad en sí misma o un parámetro predeterminado.

Según una realización alternativa de la invención presentada por la solución (3), CK e IK se generan a partir de K y RAND como en UMTS y se usan para derivar las CK e IK usadas para el plano de AS, NAS y U.

CKrrc = f3 (CK, IDas)

Cknas = f3 (CK, IDnas)

Ckupe = f3 (CK, IDupe)

Ikrrc = f4 (IK, IDas)

Iknas = f4 (IK, IDnas)

Ikupe = f4 (IK, IDupe)

en donde CKrrc es la clave de cifrado para AS o RRC, CKnas la clave de cifrado para NAS y CKupe es la clave de cifrado para el plano U, IKrrc es la clave de protección de integridad para AS, IKnas es la clave de protección de integridad para NAS e IKupe es la clave de protección de integridad para el plano U. f3 y f4 son funciones para generar los conjuntos de claves anteriores y pueden ser predeterminados de antemano, e IDas puede ser la identidad de un BS o eNB, IDnas puede ser la identidad de un MME e Idupe puede ser la identidad de un UPE.

Según una alternativa adicional a las soluciones (1) y (2) como se describió anteriormente, las IK también pueden generarse a través de una función f2 como se define en UMTS.

Las CK e IK deben mantenerse en MME como se describirá más adelante y no se transmitirán a otros elementos de red.

Como CK e IK son un producto de protocolo de autenticación AKA (desafío-respuesta), para la solución (1) un HSS (Servidor de abonado local) solo necesita generar un RAND más largo como parte del vector de autenticación y el RAND se seccionará en el MME en RANDrrc, RANDnas y RANDupe.

Para la solución (2) se requiere una función de derivación de clave para generar RANDrrc, RANDnas y RANDupe, e IDas, IDnas e Idupe deben definirse.

La Figura 2 muestra un diagrama de señalización que ilustra la generación de claves según la presente invención durante un acceso inicial.

En un acceso inicial hacia un sistema SAE/LTE, un UE emite una solicitud de acceso inicial a un MME del sistema SAE/LTE (comunicación 1 en la Figura 2). En una comunicación 2, el MME envía una solicitud de datos de autenticación a un HLR (Registro de Ubicación Local) o HSS que es una base de datos ubicada en una red doméstica del UE, y recibe vectores de autenticación (AV) y un valor aleatorio RAND, una clave de cifrado CK y una clave de protección de integridad IK, AUTN

(autenticador para la pregunta (AUTN) y XRES (respuesta prevista) en una respuesta de datos de autenticación del HLR en comunicación 3.

En una comunicación 4 en la Figura 2, el MME envía solicitudes de autenticación & cifrado hacia el UE a través de un eNB, incluyendo la petición el valor aleatorio RAND y una identidad del MME, MMEid, así como AUTN. En una comunicación 5 en la Figura 2, el UE responde con una respuesta de autenticación & cifrado RES, que se transmite hacia el MME a través del eNB.

Después de una autenticación exitosa, MME y UE usarán CK, IK acordados con RAND usado actualmente como clave de techo para crear claves de segundo nivel para protección, CKnas e IKnas en los bloques 6b y 6a en la Figura 2, como se describió anteriormente.

En la comunicación 7 en la Figura 2, el MME envía una solicitud de creación de contexto de IP a un UPE, que se reconoce en la comunicación 8, y en la comunicación 9 el MME envía un registro de L3 que incluye una identidad del UPE, UPEid, al UE. A continuación, en los bloques 10a y 10b, el UE y el MME usan CK, IK acordados con RAND usado actualmente como clave de techo para crear segundas claves de nivel para protección, CKupe e IKupe, como se describió anteriormente.

El mismo principio se aplica para la generación de clave de RRC en UE y MME. UE y MME usan una identidad del eNB, eNBid, para derivar las claves de RRC CKrrc e IKrrc como se describió anteriormente. Las funciones de derivación de clave son las funciones de UMTS f3 y f4.

En particular, con referencia a la solución (2) descrita anteriormente, UE y MME deben ser capaces de derivar CKnas, IKnas, CKup, IKup, CKrrc, IKrrc usando la función de UMTS existente f3 y f4 después de cada autenticación exitosa.

$$RANDrrc = KDF\ (RAND,\ IDas$$

$$RANDnas = KDF\ (RAND,\ IDnas)$$

$$RANDupe = KDF\ (RAND,\ IDupe)$$

donde:

$$KDF = RAND\ XOR\ IDs$$

Las ID son id de MME (utilizadas en la protección NAS), id. de UPE (usadas en la protección de UP) o id de eNB (usadas en la protección de RRC);

CKrrc = f3(K, RANDrrc)

CKnas = f3(K, RANDnas)

CKupe = f3(K, RANDupe)

IKrrc = f4(K, RANDrrc)

IKnas = f4(K, RANDnas)

IKupe = f4(K, RANDupe)

donde:

K= CK/IK

Una alternativa de usar f3/f4 es reutilizar KDF definida en TS3220 Anexo B, es decir, SAE_keys = KDF (Ks, "cadena estática", RAND, IMPI, SAE_ids). Ks se genera concatenando CK e IK. Se podría obtener IMPI (identidad privada Multimedia IP) del IMSI (identidad de abonado móvil internacional) como se especifica en TS 23.003. SAE_ids podrían ser, por ejemplo, MME_id, id de eNB y UPE_id o nombres de MME, eNB y UPE. SAE_keys expresarán a continuación MME_key, UPE_key, RRC_key. "cadena estática" podría ser "LTE_CK" y "LTE_IK" para generar CKs e IKs.

En un proceso de traspaso entre un sistema 2G/3G y un sistema SAE/LTE, se realiza la distribución de datos de seguridad (vectores de autenticación no utilizados y/o datos de contexto de seguridad actuales, por ejemplo, CK, IK, RAND etc.) entre SGSNs (2G/3G) y MME. Los siguientes casos se distinguen con respecto a la distribución de datos de seguridad entre ellos.

– Caso 1, Traspaso de Inter-RAT (tecnología de acceso por Radio) (con un anclaje 3GPP separado): LTE a 2G/3G:

Los vectores de autenticación UMTS y GSM pueden distribuirse entre MME y SGSN 2G/3G. Obsérvese que originalmente todos los vectores de autenticación (quintetos para abonados UMTS/SAE y tripletes para abonados GSM) son proporcionados por el RPP/AuC (Centro de autenticación). Los datos de contexto de seguridad actuales pueden distribuirse entre MME y SGSN 2G/3G. MME debe ser capaz de realizar la conversión CK, IK->Kc y XRES->SES

– Caso 2, Traspaso Inter-RAT (con anclaje 3GPP separado): 2G/3G -> LTE:

La señalización de alto nivel para este caso se ilustra en la Figura 3.

Como se muestra por la comunicación 1a y 1b en la Figura 3, se establece un servicio de portadora IP (Protocolo de Internet) entre el UE, un nodo de acceso 2G/3G, un SGSN 2G/3G y una aplicación 3GPP. En la comunicación 2 en la Figura 3, se emite una solicitud de traspaso desde el nodo de acceso 2G/3G al SGSN 2G/3G.

Posteriormente, durante el tiempo de preparación del traspaso, el SGSN 2G/3G distribuye los datos de seguridad al MME (comunicación 3 en la Figura 3). Los datos de seguridad incluyen CK, IK y RAND usados actualmente así como a AV no usados.

Después de recibir la confirmación de eNB (comunicación 4 en la Figura 3), el MME genera tres claves separadas para NAS, UPE (bloques 5a, 5b en la Figura 3) y RRC (no mostrado en la Figura 3). El MME también suministra id de MME, id de UPE al UE con, por ejemplo, comando de traspaso (comunicación 6 en la Figura 3). Por lo tanto, el UE puede generar también las mismas claves para NAS, UPE (bloques 7a, 7b en la Figura 3).

Además de los casos anteriores, en un traspaso de MME a MME en una PLMN (red móvil terrestre pública), los datos de seguridad pueden distribuirse en tal caso sin cambio.

Según la presente invención, cuando un UE interactúa desde el sistema de comunicación 2G/3G a LTE, según una realización de la invención representada por una solución (a), un SGSN 2G/3G (Nodo de Soporte de GPRS (Servicio General de Radio por Paquetes) envía un RAND actual usado en el sistema de comunicación 2G/3G junto con una CK/IK derivada del RAND actual en el sistema de comunicación 2G/3G a un MME en comunicación 3 en la Figura 3. A continuación, el MME usa f3 y f4 para generar diferentes conjuntos de claves con identidades de un plano de AS, NAS y U como se ha descrito anteriormente. El K en la fórmula será CK o IK.

Las identidades de MME y UPE pueden enviarse al UE a través de un comando de traspaso como se muestra en comunicación 6 en la Figura 3. El UE también puede generar conjuntos CK/IK correspondientes para NAS y UPE. El mismo principio se aplica a AS excepto que el MME no necesita enviar el ID de AS al BS, RRC o eNB. Las nuevas

funciones fx y se pueden definir para generar los conjuntos de claves para RRC, MME y UPE. Si f3 y f4 se reutilizan, el UE debe distinguir cuando usarlos para generar CK/IK y cuándo usarlos para generar los conjuntos de claves para RRC, MME y UPE.

Según una realización alternativa presentada por una solución (b), hay varias etapas más en comparación con la solución (a) para derivar una variante de la CK/IK recibida del SGSN. La CK/IK derivada del SGSN se enviará desde el MME a un HSS del UE y se usará como RAND para derivar un par de nuevas CK e IK, CK_{HO} e IK_{HO}, a través de f3 y f4, es decir, CK_{HO}= f3 (K, CK) e IK_{HO} = f4 (K, IK). These CK_{HO} and IK_{HO} will be used to generate the CK/IK sets for AS, NAS and UPE in the MME, the UE and the AS entity (i.e. the BS, RRC or eNB). Las CK_{HO} e IK_{HO} correspondientes también pueden generarse en el UE/USIM (Módulo de identidad de abonado UMTS) y en la entidad AS.

Según una realización alternativa adicional representada por una solución (c), cuando el UE pasa del sistema de comunicación 2G/3G a LTE, el SGSN 2G/3G envía el RAND actualmente usado al MME en comunicación 3 en la Figura 3 similar a la solución (a). A continuación, el MME envía este RAND junto con identidades de MME (NAS), AS y UPE (plano U) al HSS del UE y solicita vectores de autenticación. El HSS usa este RAND y las identidades del plano de AS, NAS y U para generar nuevos vectores de autenticación (CnKnas IKnas, Ckrrc, IKrrc, etc., como se describió anteriormente) y los envía de vuelta al MME. El K en la fórmula es entonces un K permanente almacenado en HSS y USIM. Las identidades de MME y UPE pueden enviarse al UE a través del comando de traspaso como se muestra en comunicación 6 en la Figura 3. El UE también puede generar conjuntos CK/IK correspondientes para NAS y UPE. El mismo principio se aplica a AS, excepto que el MME no necesita enviar el ID de AS al eNB.

Según la solución (c), el valor aleatorio RAND utilizado para generar CK/IK en el sistema de comunicación 2G/3G necesita enviarse al HSS desde el MME. Según las soluciones (a) a (c), las identidades de al menos MME y UPE deben enviarse al UE a través del comando de traspaso. f3 y f4 se usan para generar los conjuntos de claves para el uso en LTE.

Para la solución (a), MME y UE necesitan implementar f3 y f4 o funciones similares llamadas fx y fx. Para la solución (b) hay más etapas para generar CKHO e IKHO. Para la solución (c) el HSS debe modificarse para generar vectores de autenticación más largos.

Según la solución (a) no hay cambio en el HSS. Sin embargo, la solución (c) es más segura. La descripción de CK/IK en 2G/3G no afectará a los conjuntos CK/IK usados en LTE. La solución (b) también es segura porque la CK/IK no provocará la descripción de los conjuntos CK/IK usados en LTE.

Se ha de entender que la descripción anterior es ilustrativa de la invención y no se ha de interpretar como limitante de la invención. A los expertos en la técnica se les pueden ocurrir diversas modificaciones y aplicaciones.

REIVINDICACIONES

1. Un equipo de usuario (10) que comprende:

una unidad de recepción para recibir identidades de entidades de red de una segunda red durante un proceso de traspaso del equipo de usuario (10) de una primera red a la segunda red; y
una unidad de cálculo para calcular un conjunto de claves asociadas para un proceso de autenticación que se realizará en la segunda red mediante el uso de las identidades de las entidades de red, en donde el conjunto de claves asociadas comprende una clave de cifrado y una clave de protección de integridad, y en donde la unidad de cálculo está configurada para calcular el conjunto de claves asociadas en base a un valor aleatorio usado en un proceso de autenticación de la primera red, una clave de cifrado usada en un proceso de autenticación de la primera red y una clave de protección de integridad usada en un proceso de autenticación de la primera red.

2. El equipo de usuario (10) según la reivindicación 1, en donde la unidad de recepción está configurada para recibir las identidades de las entidades de red de un elemento de gestión de movilidad de la segunda red.

3. El equipo de usuario (10) según cualquiera de las reivindicaciones anteriores, en donde la unidad de recepción está configurada para recibir una solicitud de autenticación y cifrado de un elemento de gestión de movilidad a través de un eNB, la solicitud de autenticación y cifrado que comprende las identidades de las entidades de red y un valor aleatorio usado en un proceso de autenticación de la primera red.

4. El equipo de usuario (10) según la reivindicación 3, en donde el equipo de usuario (10) está configurado para responder a la solicitud de autenticación y cifrado con una respuesta de autenticación y cifrado, transmitiéndose la respuesta de autenticación y cifrado hacia el elemento de gestión de movilidad a través del eNB.

5. El equipo de usuario (10) según la reivindicación 2, en donde la unidad de recepción está configurada para recibir, en un comando de traspaso del elemento de gestión de movilidad, las identidades de las entidades de red durante el proceso de traspaso del equipo de usuario de la primera red a la segunda red; y

en donde las entidades de red son el elemento de gestión de movilidad y un elemento de plano de usuario.

6. Un método para un equipo de usuario (10), comprendiendo el método:

recibir identidades de entidades de red de una segunda red durante un proceso de traspaso del equipo de usuario (10) de una primera red a la segunda red; y
calcular un conjunto de claves asociadas para un proceso de autenticación que se realizará en la segunda red mediante el uso de las identidades de las entidades de red, en donde el conjunto de claves asociadas comprende una clave de cifrado y una clave de protección de integridad, y en donde el cálculo comprende calcular el conjunto de claves asociadas en base a un valor aleatorio usado en un proceso de autenticación de la primera red, una clave de cifrado usada en un proceso de autenticación de la primera red y una clave de protección de integridad usada en un proceso de autenticación de la primera red.

7. El método según la reivindicación 6, en donde la recepción comprende recibir las identidades de las entidades de red de un elemento de gestión de movilidad de la segunda red.

8. El método según cualquiera de las reivindicaciones 6 a 7, en donde la recepción comprende recibir una solicitud de autenticación y cifrado de un elemento de gestión de movilidad a través de un eNB, la solicitud de autenticación y cifrado que comprende las identidades de las entidades de red y un valor aleatorio usado en un proceso de autenticación de la primera red.

9. El método según la reivindicación 8, que comprende además responder a la solicitud de autenticación y cifrado con una respuesta de autenticación y cifrado, transmitiéndose la respuesta de autenticación y cifrado hacia el elemento de gestión de movilidad a través del eNB.

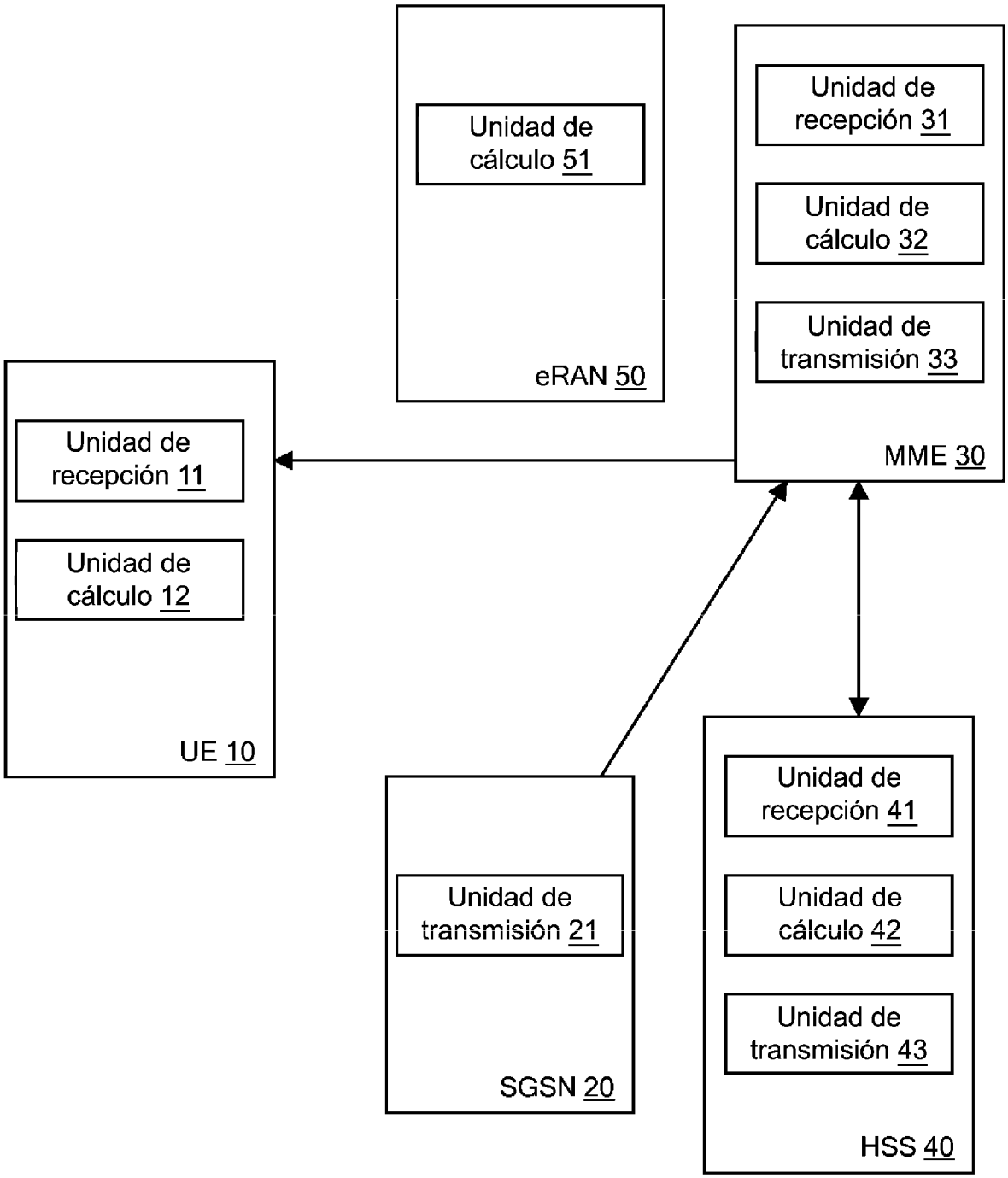
Unidad de cálculo 51
eRAN 50
Unidad de recepción 31
Unidad de cálculo 32
Unidad de transmisión 33
MME 30
Unidad de recepción 11
Unidad de cálculo 12
UE 10
Unidad de transmisión 21
SGSN 20
Unidad de recepción 41
Unidad de cálculo 42
Unidad de transmisión 43
HSS 40

Figura 1

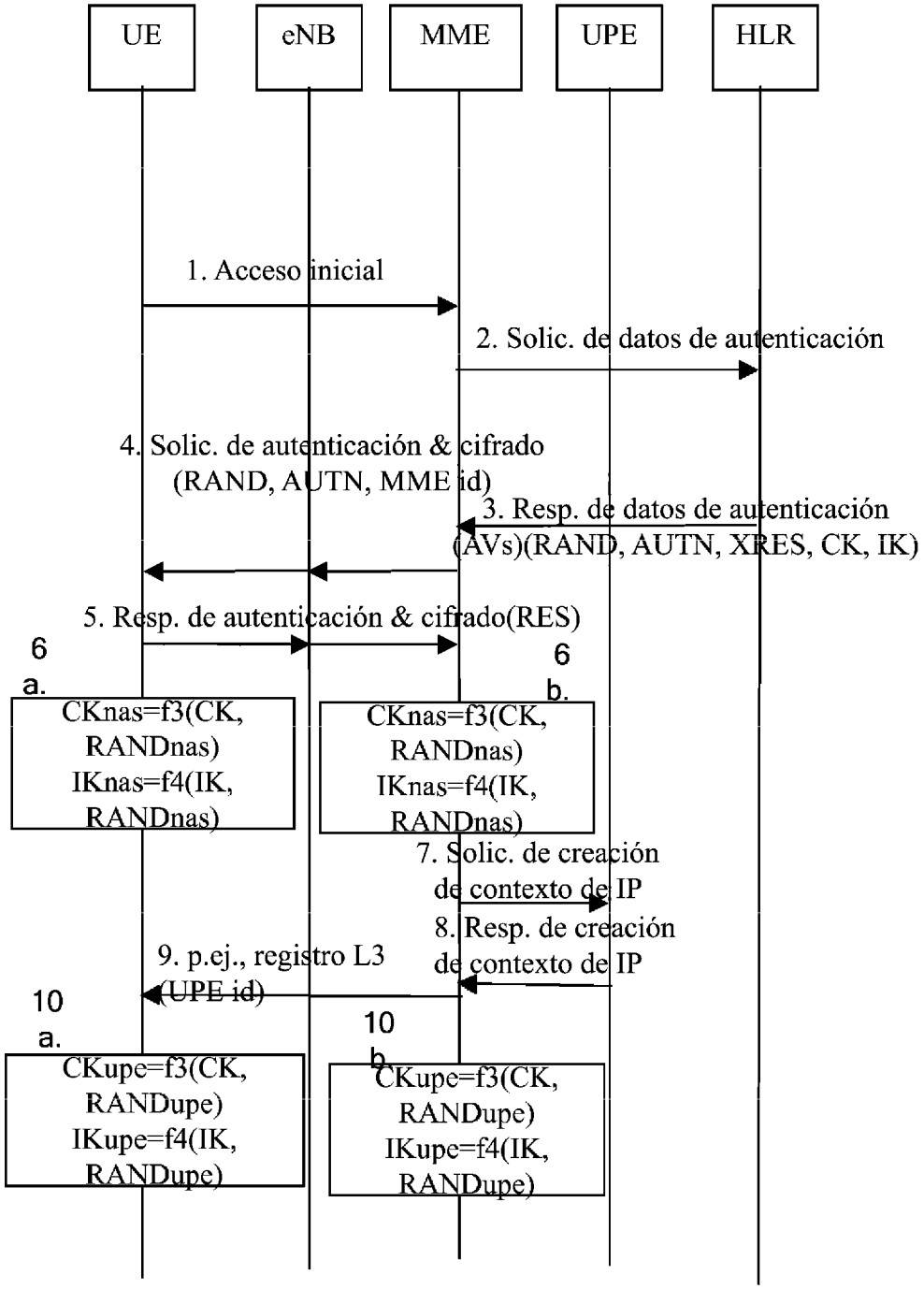
UE
eNB
MME
UPE
HLR
1. Acceso inicial
2. Solic. de datos de autenticación
4. Solic. de autenticación & cifrado
(RAND, AUTN, MME id)
3. Resp. de datos de autenticación
(AVs)(RAND, AUTN, XRES, CK, IK)
5. Resp. de autenticación & cifrado(RES)
6
a.
CKnas=f3(CK,
RANDnas)
IKnas=f4(IK,
RANDnas)
6
b.
CKnas=f3(CK,
RANDnas)
IKnas=f4(IK,
RANDnas)
7. Solic. de creación
de contexto de IP
8. Resp. de creación
de contexto de IP
9. p.ej., registro L3
(UPE id)
10
a.
CKupe=f3(CK,
RANDupe)
IKupe=f4(IK,
RANDupe)
10
b.
CKupe=f3(CK,
RANDupe)
IKupe=f4(IK,
RANDupe)

Figura 2

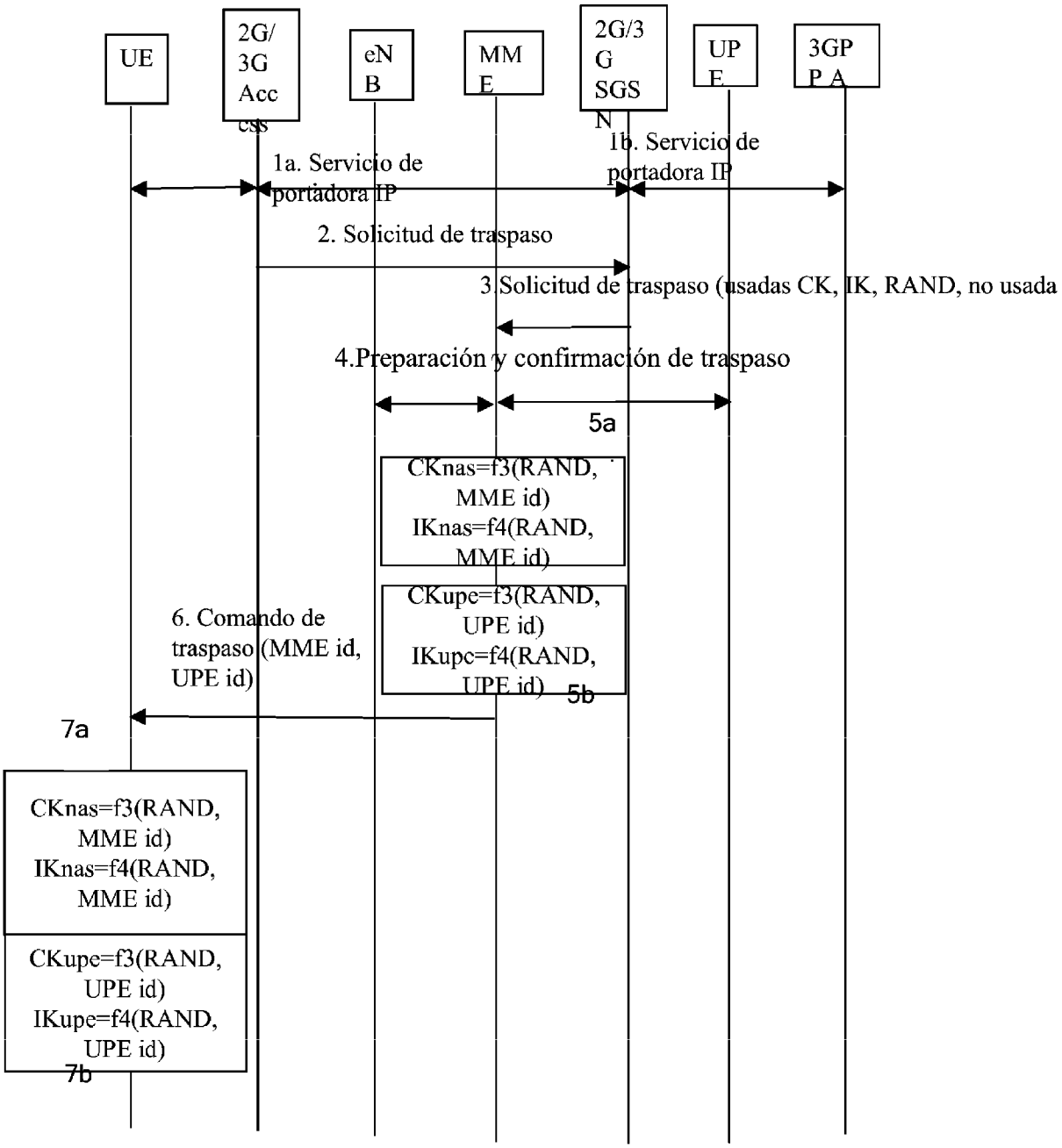
UE
2G/ 3G Acc ess
eN B
MM E
2G/3 G SGS N
UP E
3GP P A
1a. Servicio de portadora IP
1b. Servicio de portadora IP
2. Solicitud de traspaso
3 Solicitud de traspaso (usadas CK, IK, RAND, no usada
4.Preparación y confirmación de traspaso
5a
CKnas=f3(RAND, MME id)
IKnas=f4(RAND, MME id)
CKupe=f3(RAND, UPE id)
IKupe=f4(RAND, UPE id)
5b
6. Comando de traspaso (MME id, UPE id)
7a
CKnas=f3(RAND, MME id)
IKnas=f4(RAND, MME id)
CKupe=f3(RAND, UPE id)
IKupe=f4(RAND, UPE id)
7b

Figura 3