(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 675 326**

(51) Int. CI.:

H04W 36/00 (2009.01)
H04W 36/14 (2009.01)
H04W 12/04 (2009.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.06.2010 E 14156773 (5)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 2739086**

(54) Título: **Método y aparato en un sistema de telecomunicación**

(30) Prioridad:

05.10.2009 US 248583 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.07.2018

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

NORDSTRAND, INGRID y
PALM, HÅKAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y aparato en un sistema de telecomunicación

Campo de la invención

La presente invención se refiere a un procedimiento de transferencia Inter RAT.

Antecedentes

La presente invención se refiere a una transferencia Inter RAT (Tecnología de Acceso por Radio – Radio Access Technology, en inglés) en una red de comunicación. Dentro del alcance de la E-UTRAN del 3GPP, también llamado estandarización de Evolución a Largo Plazo, LTE (Long Term Evolution, en inglés), se han acordado soluciones de transferencia Inter RAT. Tal como se utiliza en esta memoria, E-UTRAN denota el sistema de radio de telefonía móvil desarrollado y estandarizado mediante el 3GPP, y el eNodoB (eNB) denota un nodo de estación de base de radio de la E-UTRAN. Tal eNodoB podría servir a múltiples células de E-UTRAN.

La funcionalidad para manejar movilidad de usuario es un componente fundamental en las redes de telefonía móvil. Desde la perspectiva de la calidad de un servicio, tal funcionalidad debe asegurar que se mantiene la continuidad del servicio mientras los usuarios de dispositivos de comunicación inalámbricos se desplazan de una célula a otra durante una sesión activa, y que cada nueva sesión es establecida en un entorno de radio suficientemente bueno. Desde una perspectiva de eficiencia espectral, tal funcionalidad debe asegurar que un usuario activo es siempre servido por la unidad o unidades de radio remotas apropiadas, tal como un eNodoB para la E-UTRAN o un RNC (Controlador de Red de Radio – Radio Network Controller, en inglés) en la UTRAN, lo que a menudo significa la unidad de radio remota más cercana, en un sentido de radio. Así una transferencia puede tener que ser llevada a cabo de vez en cuando, por ejemplo, cuando un dispositivo de comunicación inalámbrico se mueve entre diferentes células con el fin de evitar la terminación de la llamada cuando el dispositivo de comunicación inalámbrica sale del alcance de la primera célula.

Un procedimiento de transferencia Inter RAT de UTRAN a E-UTRAN tiene lugar cuando la red decide llevar a cabo una transferencia. La decisión de llevar a cabo transferencia de PS desde la UTRAN a la E-UTRAN es tomada por el RNC que sirve a la UTRAN (SRNC – Serving RNC, en inglés) y esta decisión podría estar basada en mediciones de condición de radio reportadas por un Equipo de Usuario, UE (User Equipment, en inglés), al SRNC.

El documento 3GPP TS 23.401, capítulo 5.5.2.2, proporciona una visión global de la preparación de una transferencia y de la señalización de la ejecución de la transferencia en la transferencia de UTRAN a E-UTRAN.

Antes de decidir sobre la transferencia a la E-UTRAN, el SRNC comprobará que el UE es capaz de E-UTRA. Además, tal UE puede ser configurado por el SRNC para llevar a cabo mediciones en células de E-UTRA, y con ese propósito el modo comprimido (dependiendo de la capacidad del UE) podría tener que ser configurado. El modo comprimido es necesario cuando se realizan mediciones en otra frecuencia (inter-frecuencias) o en una tecnología de radio diferente (Inter RAT). En el Modo Comprimido la transmisión y la recepción se detienen durante un corto espacio de tiempo mientras que se llevan a cabo las mediciones en otra frecuencia o RAT en ese momento. Después de que las mediciones se han terminado la transmisión y la recepción finalizan. Para estar seguros de que los datos no se han perdido, los datos son comprimidos en la trama creando un espacio vacío donde pueden llevarse a cabo mediciones.

Esto implica que cuando se inicia una transferencia, ésta ha sido precedida por un número de etapas tomadas, tales como las reconfiguraciones de recurso de radio, reconfiguraciones de medición, mediciones y reportes de medición. Si la transferencia a la E-UTRA no está permitida por alguna razón, esas etapas se perderían. Por el contrario, otras etapas alternativas (por ejemplo, medición en otras tecnologías de radio, otras frecuencias de UTRA) podrían haber sido inhibidas mientras el UE está configurado para realizar mediciones en células de E-UTRA. Debido a posibles limitaciones del UE y/o a limitaciones de la UTRAN, el SRNC tiene que seleccionar qué acción tomar cuando el resultado de la medición del UE recibido desde el UE indica por ejemplo malas condiciones de radio en la célula / frecuencia de UTRA actual. Además, cuando se inicia una transferencia para razones de condición de radio la transferencia debe tener una alta probabilidad de éxito; si no, la llamada podría caer.

Un usuario que opera en un sistema de acceso UTRA puede por ejemplo tener una suscripción de GSM con una Tarjeta de Circuitos Integrados de UMTS, UICC (UMTS Integrated Circuit Card, en inglés), de tipo SIM (Módulo de Identidad de Abonado Universal – Universal Subscriber Identity Module, en inglés). Dependiendo del tipo de UICC, se utilizan diferentes algoritmos de Autenticación y de Acuerdo de Clave, AKA (Authentication and Key Agreement, en inglés). El procedimiento de AKA se ejecuta entre el Nodo de Soporte de GPRS de Servicio, SGSN (Serving GPRS Support Node, en inglés), y la UICC en el UE. Es el SGSN el que inicia el procedimiento de AKA y es normalmente realizado en cada ataque, es decir, cada primer registro en la red de servicio, por ejemplo, durante el encendido. Un procedimiento de AKA podría ser también llevado a cabo cuando el UE está conectado. Un caso típico es en la actualización del Área de Encaminamiento en un nuevo SGSN. El tipo de AKA llevado a cabo depende de la información de seguridad que el SGSN está recibiendo del HLR / AuC (Registro de Ubicación de abonados Locales / Centro de Autenticación (Home Location Register / Authentication Center, en inglés) del Entorno

Local del usuario. La información de seguridad recibida del HLR / AuC contiene una clave de cifrado Kc (Ciphering Key, en inglés) si el usuario tiene una suscripción de GSM, mientras que contiene una clave de cifrado CK (Ciphering Key, en inglés) y una clave de protección de Integridad IK (Integrity protection Key, en inglés) si el usuario tiene una suscripción de UMTS. En el AKA de GSM, que es soportado por la UICC de tipo SIM, la clave de cifrado Kc (64 bits) es generada por el SIM. En el correspondiente AKA de UMTS, que está soportado por la UICC de tipo USIM, la clave de cifrado CK (128 bits) y la clave de protección de integridad IK (128 bits) son generadas por el USIM.

Los diferentes algoritmos de AKA, por ejemplo, las diferentes claves generadas y la longitud de las claves de seguridad, proporciona el que el nivel de seguridad para un UE equipado con una UICC de tipo SIM sea considerado más bajo que cuando se equipa con una UICC del tipo USIM.

El SGSN inicia la AKA relevante hacia el UE sobre la base de la información recibida del HLR /AuC (Registro de Ubicación de abonados Locales / Centro de Autenticación – Home Location Register / Authentication Center, en inglés) del usuario. El procedimiento de AKA es ejecutado con señalización entre el UE y el SGSN y es a transparente a través de la UTRAN.

El cifrado y la protección de integridad del usuario y de los datos de control es llevado a cabo entre el UE y el SRNC, es decir, los algoritmos de cifrado y protección de integridad están asignados al UE y al SRNC.

Los algoritmos de cifrado y de protección de integridad, definidos para acceso UTRA, utilizan claves de seguridad de 128 bits de longitud. Para proporcionar soporte a un usuario que tiene una subscripción de GSM (SIM) para obtener servicios también en UTRAN, existen dos funciones de conversión definidas en el 3GPP que obtienen las claves de cifrado y de protección de integridad de UMTS (CK e IK) a partir de la clave de cifrado de GSM (Kc) de 64 bits de acuerdo con lo que sigue, donde c4 es la función de conversión para obtener CK y c5 es la función de conversión para obtener IK:

CK [UMTS] = Kc | | Kc; (c4)

IK [UMTS] = Kc1 xor Kc2 | | Kc | | Kc1 xor Kc2; (c5)

por lo que en c5, Kc1 y Kc2 tienen las dos 32 bits de longitud y Kc = Kc1 | | Kc2.

Así, cuando un usuario / UE con suscripción de GSM, es decir, que contiene una UICC de tipo SIM, es conectada a una UTRAN, el UE obtiene las claves de cifrado y de protección de integridad del UMTS CK e IK que son válidas para acceso UTRA a partir de la clave cifrada Kc utilizando las funciones de conversión c4 y c5. Las claves de seguridad son utilizadas para el cifrado y la protección de integridad de los datos de usuario y de la señalización de control enviados entre el UE y el SRNC.

Las mismas funciones de conversión son utilizadas por el SGSN. Para un UE en modo de conexión, estas CK e IK obtenidas son enviadas desde el SGSN al SRNC cuando para solicitar el inicio del cifrado y de la protección de integridad entre el UE y el SRNC.

El documento 3GPP TS 33.102 proporciona información más detallada acerca de las funciones de seguridad en el UMTS. Información acerca del manejo de las claves se encuentra asimismo en el documento del 3GPP TR 33.821, V9.0.0 (2009-06); "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE) (Release 9)".

El 3GPP de Versión 8 no soporta ningún servicio en E-UTRA a los UE que no están equipados con una UICC de tipo USIM. Así, si un UE que tiene capacidad de E-UTRAN, pero que no está equipado con un USIM, no indicará ningún soporte para E-UTRA en su información de capacidad que es enviada a la red de UTRA. Como consecuencia, la UTRAN no solicitará al UE que realice ninguna medición de E-UTRA y no solicitará al UE que realice ninguna transferencia a la E-UTRA. Así, en el 3GPP de Versión 8, un UE sin USIM no puede realizar ninguna transferencia desde la UTRAN a la E-UTRAN debido a que el UE deshabilita su capacidad de E-UTRAN tal como se ha descrito anteriormente. Esta deshabilitación implica que, aunque el UE es capaz de acceso E-UTRA, cuando está equipado con una UICC de tipo SIM informará ya en la conexión a la red de que no tiene capacidad de E-UTRA. Entonces esto no cambiará mientras el UE está conectado.

No obstante, en el 3GPP de Versión 9, servicios de portadora de emergencia de IMS son soportados tanto para un UE de modo de servicio normal como para un UE de modo de servicio limitado, es decir, independientemente de con qué tipo de UICC esté equipado el UE, o si el UE no tiene una UICC en absoluto. El documento del 3GPP SA WG1 LS R2-094143 Reply LS a R2-094107 sobre “UICCless UE Access for IMS emergency call in Rel-9”, establece que, a un UE sin USIM que haga una llamada de emergencia de IMS, debe permitírsele la transferencia desde la UTRAN a la E-UTRAN.

Se han explicado diferentes soluciones para conseguir tal transferencia (véase R2-094569 “IMS emergency call handover from UTRAN to EUTRAN for USIMless UE”), como sigue:

La alternativa#1 es una solución basada en la red en la que el SGSN informa al RNC de si el UE tiene una UICC válida, es decir, un USIM que permite transferencia a la E-UTRAN para llamadas que no son de emergencia o no. El RNC utiliza esta información para decidir si hacer una transferencia a la E-UTRAN para un UE sin USIM de manera que, si el UE sin USIM está implicado en una llamada de emergencia de IMS, permitirá la transferencia.

No obstante, la alternativa#1 requiere la actualización del protocolo de señalización (RANAP, 3GPP TS 25.413) entre el SGSN y el RNC. Las especificaciones de la versión 8 están congeladas, pero un RNC basado en las especificaciones del protocolo de versión 8 debe, de cualquier modo, ser capaz de soportar los UE con capacidad de E-UTRA de versión 9.

La alternativa#2 es una solución basada en UE en la que un UE sin USIM deshabilita los elementos de Información, IEs, “Support of Inter-RAT PS Handover to E-UTRA FDD” y “Support of Inter RAT PS Handover to E-UTRA TDD”, que forman parte de la información de capacidad del UE enviada desde el UE al SRNC, y sólo los habilita cuando se establece una llamada de emergencia pero los deshabilita de nuevo cuando la llamada de emergencia ha terminado. Así, el UE sin USIM conmuta sus capacidades de E-UTRAN sobre la base de los estados del RRC en los que se encuentra y si existe una llamada de emergencia.

La alternativa#2 podría no obstante provocar mucha señalización entre el UE y la red debido al hecho de que el UE necesita enviar nuevas capacidades del UE a la red cada vez que lleve a cabo una llamada de emergencia y una vez más al final de la llamada de emergencia. Esto podría llevar a una incoherencia, pero también será una solución inflexible puesto que en el futuro podría haber otros servicios distintos a sólo llamadas de emergencia en las que la transferencia a la E-UTRAN puede hacerse autorizarse. Así, podría haber otras necesidades y otros tipos de restricciones en el futuro para las que la red (UTRAN) necesita conocer el tipo de UICC.

De este modo, se prefiere una solución de red y, si es posible, una solución que no requiera ningún cambio de protocolos de señalización entre nodos de red.

Compendio

La presente invención proporciona un método según la reivindicación 1 que está dirigido a resolver o mitigar los inconvenientes descritos anteriormente de las soluciones conocidas. Se describe asimismo un aparato correspondiente para uso en un RNC según la reivindicación 8.

En UTRAN es el SRNC el que inicia las mediciones en las células de E-UTRA y también toma la decisión acerca de la transferencia. El SRNC tiene conocimiento acerca del tipo de llamadas / portadoras que están establecidas para un UE, por ejemplo, el SRNC tiene conocimiento acerca de cuándo se establece una llamada de emergencia o no para un UE.

Con el fin de impedir que el SRNC inicie mediciones de E-UTRA en un UE, al que no se le permite llevar a cabo una transferencia a la E-UTRAN, es decir, no tiene una UICC válida para E-UTRA tal como un USIM, y para impedir el inicio de la señalización de asignación del recurso de transferencia en la red para tal UE, existe una necesidad de que el SRNC conozca qué tipo de UICC tiene el UE, por ejemplo, si hay una USIM o no en el UE.

Actualmente no existe información acerca de cómo puede el RNC identificar el tipo de UICC en el UE, y por lo tanto las realizaciones de la presente invención se dirigen a proporcionar una solución a este problema.

Un primer aspecto de las realizaciones de la presente invención se refiere a un método en un Controlador de Red de Radio de servicio, SRNC (Serving Radio Network Controller, en inglés), para controlar las transferencias Inter RAT a la E-UTRAN de un UE con capacidad de E-UTRA que opera en una red de servicio que comprende al citado SRNC, donde el SRNC recibe, desde el Nodo de Soporte del GPRS de Servicio, SGSN (Serving GPRS Support Node, en inglés), claves de seguridad generadas durante la autenticación y el acuerdo de claves, AKA (Authentication and Key Agreement, en inglés). El método comprende las etapas de

- determinar qué suscripción ha sido proporcionada al UE por el UICC mediante el análisis de las claves de seguridad recibidas desde el SGSN, utilizando propiedades de las funciones de conversión de claves conocidas para el SRNC;

- utilizar, por parte del SRNC, el conocimiento de qué suscripción es proporcionada al UE por la UICC, con la que el UE está equipado, para basar una decisión acerca de si permitir la transferencia del UE a la E-UTRAN.

De acuerdo con una realización específica, el método comprende la etapa de permitir la transferencia del UE a la E-UTRAN para que sea iniciada si el UE tiene una UICC que proporciona una suscripción válida para la E-UTRAN o si al menos se cumple una condición relativa al tipo de servicio en curso del citado UE.

En una realización específica, el método comprende las etapas de

- permitir que la transferencia del UE a la E-UTRAN sea iniciada si al menos se cumple una de las siguientes condiciones:

- el UE tiene una UICC que proporciona una suscripción válida para la E-UTRAN, o
- el UE tiene una llamada de emergencia en curso,

o si no,

- no permitir transferencia Inter RAT del UE a la E-UTRAN.

Así, de acuerdo con las realizaciones específicas, si el UE no tiene una UICC válida para E-UTRAN, el SRNC comprueba si el UE tiene un servicio en curso para el cual la transferencia a la E-UTRAN está permitida, por ejemplo, una llamada de emergencia.

De acuerdo con una realización específica, las claves de seguridad recibidas desde el SGSN son analizadas aplicando funciones de conversión conocidas para el SRNC, estando las citadas funciones de conversión definidas para obtener claves de seguridad que son válidas para acceder a la red de servicio a partir de una clave de seguridad no válida.

En una realización específica, la transferencia Inter RAT es una transferencia desde la UTRAN a la E-UTRAN, y en la que las claves de seguridad definidas para acceso UTRA, generadas por una UICC que proporciona una suscripción de UMTS, son una clave de cifrado (CK) de 128 bits y una clave de protección de integridad (IK) de 128 bits, por lo que una clave de cifrado (Kc) generada por un UICC que proporciona una suscripción de GSM puede ser convertida a dichas claves de seguridad definidas para acceso UTRA mediante las siguientes funciones de conversión:

CK = Kc | | Kc;

IK = Kc1 xor Kc2 | | Kc | | Kc1 xor Kc2

En una realización específica, la etapa de determinar qué suscripción es proporcionada por la UICC, con la que el UE con capacidad de E-UTRA está equipado, comprende

- comprobar si la CK recibida desde el SGSN consiste en dos Kc de 64 bits idénticas de acuerdo con la ecuación c4,

- si no, concluir que el UE está equipado con una UICC que proporciona una suscripción de UMTS; o si no,

- calcular un valor de prueba a partir de la ecuación c5, en la que Kc = Kc1 | | Kc2 es una de las dos Kc de 64 bits idénticas, y Kc1 y Kc2 tienen ambas una longitud de 32 bits, de tal manera que si el valor de prueba es igual a la IK recibida del SGSN, entonces concluir que el UE está equipado con una UICC que proporciona una suscripción de GSM, o si no, concluir que el UE está equipado con una UICC que proporciona una suscripción de UMTS.

Un segundo aspecto de las realizaciones de la invención se refiere a un aparato para su uso en un Controlador de Red de Radio, RNC (Radio Network Controller, en inglés), capaz de controlar una transferencia Inter RAT a la E-UTRAN de un UE con capacidad de E-UTRA que opera en una red de servicio que comprende el citado RNC, que comprende una interfaz para comunicación con un Nodo de Soporte de GPRS de Servicio, SGSN (Serving GPRS Support Node, en inglés), estando la citada interfaz adaptada para recibir, desde el SGSN, claves de seguridad generadas durante la autenticación y el acuerdo de claves, AKA (Authentication and Key Agreement, en inglés). La citada disposición comprende una unidad de procesamiento configurada para:

- determinar qué suscripción es proporcionada al UE por la UICC con la que el UE está equipado analizando las claves de seguridad recibidas desde el SGSN;

- utilizar el conocimiento de qué suscripción es proporcionada al UE por la UICC con la que el UE está equipado para basar una decisión acerca de si permitir la transferencia del UE a la E-UTRAN.

Así, una realización particular proporciona un método en un Controlador de Red de Radio de Servicio, SRNC (Serving Radio Network Controller, en inglés) para determinar el tipo de UICC, Tarjeta de Circuitos Integrados de UMTS (UMTS Integrated Circuit Card, en inglés) en un UE utilizando claves de seguridad tales como CK e IK y funciones de conversión especificadas que son aplicadas cuando una autenticación y acuerdo de claves, AKA (Authentication and Key Agreement, en inglés), tal como AKA de GSM, han sido llevados a cabo, para determinar qué tipo de UICC tiene el UE, por ejemplo un USIM o un SIM.

En realizaciones particulares de la presente invención se asume que un UE con SIM en uso está autorizado para indicar la capacidad de E-UTRA en acceso UTRA.

La información relativa al tipo de UICC, es decir, la suscripción proporcionada por la UICC, puede ser utilizada por el SRNC para decidir si un UE con capacidad de E-UTRAN estará configurado para llevar a cabo mediciones de célula de E-UTRA y si puede iniciarse una transferencia a una célula de E-UTRA. Esto proporciona una posibilidad de que el SRNC limite la configuración de las mediciones de célula de E-UTRA y la transferencia de UTRA a E-UTRA para aquellos UE que tienen capacidad de E-UTRA y bien tienen un servicio en curso de un tipo para el cual la

transferencia a la E-UTRAN está permitida, tal como una llamada de emergencia tal como la especificada para la E-UTRA de versión 9, o bien aquellos UE que tienen un servicio en curso de cualquiera tipo, tal como una llamada que no es de emergencia, y tienen un USIM. Así, a los UE que, por ejemplo, contienen una UICC del tipo de SIM puede impedírseles preparar e iniciar una transferencia Inter RAT a la E-UTRAN, o alternativamente, en caso de que por ejemplo haya una llamada de emergencia en curso, puede permitírseles preparar e iniciar la transferencia Inter RAT a la E-UTRAN.

Otros objetos, ventajas y nuevas características de la invención resultarán evidentes a partir de la siguiente descripción detallada de la invención cuando se considera junto con los dibujos que se acompañan.

Breve descripción de los dibujos

La Fig. 1 ilustra un flujo de señalización en relación con qué realizaciones de la invención pueden ser aplicadas,

la Fig. 2 muestra un diagrama de flujo que ilustra un método de acuerdo con una realización de la invención;

la Fig. 3 muestra esquemáticamente una disposición en un RNC de acuerdo con una realización de la invención.

Descripción detallada

La presente invención puede ser ejemplificada en la siguiente descripción no limitativa de una realización de la invención. En la siguiente descripción, se hace referencia a un escenario relativo a una transferencia de la UTRAN a la E-UTRAN, donde el cifrado y las claves de protección de integridad de UMTS, CK, IK, son recibidas por un RNC de servicio del nodo de soporte de GPRS de servicio. Debe observarse, no obstante, que la invención no debe ser considerada como limitada a estas claves específicas. En otro escenario el principio de acuerdo con las realizaciones particulares de las invenciones puede ser aplicado para otras claves generadas durante la autenticación y el acuerdo de clave en la conexión del UE a una red de servicio.

La Fig. 1 ilustra un esquema de señalización al que se hará referencia en la siguiente descripción detallada de realizaciones particulares de la invención.

El procedimiento de autenticación, representado mediante la etapa 6 de la Fig. 1, está precedido por las etapas 1 – 5 conocidas relativas al establecimiento de la conexión del UE a la red. Estas etapas precedentes no son directamente relevantes para la presente invención y por lo tanto no serán explicadas con más detalle en esta memoria.

De acuerdo con la técnica anterior representada por ejemplo por el documento 3GPP TS 33.102, al inicio de la funcionalidad de seguridad, es decir, el cifrado de los datos de usuario y de control y la protección de integridad de los datos de control entre el UE y el SRNC, para una conexión del UE, el SGSN envía la clave de cifrado de UMTS CK y la clave de protección de integridad de UMTS IK al SRNC en una Orden de Modo de Seguridad, véase la etapa 7.1 de la Fig. 1. El inicio de la funcionalidad de seguridad se realiza una vez que el UE tiene una conexión de señalización entre el UE y el SGSN tras un nuevo procedimiento de AKA. Las dos claves CK, IK, tienen 128 bits cada una. Los algoritmos de cifrado y de integridad están asignados en el SRNC y el UE. Junto con el CK y el IK, el SRNC recibe además, del SGSN, información acerca de los algoritmos de seguridad que se permite utilizar. De acuerdo con la técnica anterior, no se proporciona ninguna información desde el SGSN al SRNC acerca de qué tipo de UICC contiene el UE.

De acuerdo con realizaciones particulares de la presente invención, el SRNC, tras recibir las claves CK, IK desde el SGSN, identifica el tipo de UICC del UE para una conexión del UE mediante el uso de las claves de seguridad CK e IK recibidas desde el SGSN en el mensaje de ORDEN DE MODO DE SEGURIDAD. Esto puede ser realizado utilizando propiedades de las funciones de conversión de clave conocidas para el SRNC, pudiendo las citadas funciones de conversión haber sido utilizadas por el SGSN y el UE para obtener claves que son válidas para la red de servicio. Las funciones de conversión de clave pueden ser funciones de conversión de clave de GSM a UMTS especificadas en el 3GPP TS 33.102.

De acuerdo con realizaciones particulares de la invención, el SRNC utiliza el conocimiento acerca de si el UE tiene un USIM o no, junto con otro tipo de información tal como la capacidad del UE y los tipos de llamada en curso, para basar su decisión en si configurar el UE para hacer las mediciones de célula de E-UTRA, véase la etapa 11 – 12 de la Fig. 1, y/o para iniciar una transferencia hacia la E-UTRAN, véase la etapa 13 de la Fig. 1, sobre la base de los reportes de medición que indican una mala calidad, véase la etapa 9 de la Fig. 1. Debe observarse que puede no ser obligatorio llevar a cabo mediciones de célula de E-UTRA antes de que se inicie la transferencia a la E-UTRA. Tal decisión de transferencia podría también ser tomada sobre la base de mediciones de célula de UTRA por ejemplo en caso de que la cobertura de la célula de UTRA y de la célula de E-UTRA se superpongan.

Un método de acuerdo con una realización de la invención llevado a cabo por un RNC de Servicio, SRNC (Serving RNC, en inglés), se describirá ahora con referencia a la Fig. 2. Debe observarse que las etapas del método pueden ser llevadas a cabo en un orden cronológico de alguna manera diferente de las sugerencias de enumeración y que algunas de ellas, por ejemplo, las etapas 202 y 203 pueden ser llevadas a cabo en un orden cronológico nuevamente dispuesto.

En la etapa 201, el SRNC recibe la clave de cifrado de UMTS CK y la clave de protección de integridad de UMTS CK desde el SGSN en una Orden de Control de Seguridad, las citadas claves deben ser utilizadas para el cifrado y la protección de integridad de los datos de usuario y de la señalización de control enviados entre un UE y el SRNC.

En la etapa 202, el SRNC determina qué tipo de UICC contiene el UE, es decir, qué suscripción es proporcionada al UE por la UICC, analizando las claves de seguridad recibidas desde el SGSN. Esto puede ser realizado utilizando propiedades de funciones de conversión de clave conocidas para el SRNC.

De acuerdo con el documento TS 33.103, sección 6.8.2.4, un R99+ VLR / SGSN (R99+ se refiere a un nodo de red o UE que está de acuerdo con el 3GPP de Versión 99 ó posteriores especificaciones) y un UE con SIM insertado obtendrá las claves de cifrado / protección de integridad de UMTS CK e IK a partir de la clave de cifrado de GSM utilizando las siguientes funciones de conversión:

CK [UMTS] = Kc | | Kc; (ecuación c4)

IK [UMTS] = Kc1 xor Kc2 | | Kc | | Kc1 xor Kc2 (ecuación c5);

por lo que en c5, Kc1 y Kc2 son las dos de 32 bits de longitud y Kc = Kc1 | | Kc2.

Para la introducción de una identificación del tipo de UICC el SRNC realiza la siguiente comprobación:

- ¿Consiste la CK tal como se recibe desde el SGSN en dos Kc de 64 – bits idénticas (de acuerdo con la ecuación c4), es decir, son los al menos 64 bits significativos de la CK idénticos a los 64 bits más significativos de la CK?

Si la respuesta es No: El UE utiliza un USIM.

Si la respuesta es Sí: Calcular un valor de prueba según la fórmula para calcular una IK a partir de una Kc, es decir, la función c5, como sigue: valor de prueba = Kc1 xor Kc2 | | Kc | | Kc1 xor Kc2

donde Kc = Kc1 | | Kc2 es una de las dos Kc de 64 bits idénticas anteriores y Kc1 y Kc2 son ambos de 32 bits de longitud.

- Si el valor de prueba es igual al IK recibido desde el SGSN, entonces
    - el UE utiliza un SIM,
- si no
    - el UE utiliza un USIM.

El USIM es como se ha mencionado previamente una UICC que es válida para la E-UTRAN.

En la etapa 203, el SRNC recibe información del UE, por ejemplo, en un reporte de medición, de que el UE experimenta una mala calidad de radio, indicando que puede ser necesaria una transferencia.

Si la transferencia a la E-UTRAN es la alternativa más apropiada, y el UE tiene capacidad de E-UTRA, el SRNC comprobará, en la etapa 204, si el UE contiene una UICC que es válida para la E-UTRAN. Esto se realiza analizando las claves de seguridad recibidas desde el SGSN, por ejemplo, utilizando las funciones de conversión c4 y c5 tal como se describen en lo anterior.

Si el UE contiene una UICC que es válida para la E-UTRAN, el SRNC puede iniciar una transferencia a la E-UTRAN de acuerdo con la etapa 205.

Si el UE no contiene una UICC válida para la E-UTRAN, el SRNC puede, de acuerdo con realizaciones particulares, comprobar de nuevo, en la etapa 206, si el servicio en curso del UE es de un tipo para el cual la transferencia a la E-UTRAN está permitida independientemente de qué tipo de UICC contiene el UE. Tal servicio puede por ejemplo ser una llamada de emergencia.

Si el servicio que el UE está utilizando es de un tipo para el cual la transferencia a la E-UTRAN está permitida independientemente de qué tipo de UICC contiene el UE, el SRNC puede iniciar transferencia a la E-UTRAN de acuerdo con la etapa 205.

Si no, el SRNC no iniciará de acuerdo con la etapa 207 una transferencia a la E-UTRAN para el citado UE, ahorrando por ello recursos que de otro modo habrían sido gastados por el UE en las mediciones de la E-UTRA.

La Fig. 3 ilustra esquemáticamente una disposición 300 en un RNC de acuerdo con una realización particular de la invención, siendo el citado RNC capaz de actuar como RNC de servicio para un UE con capacidad de E-UTRA en una red de comunicaciones de telefonía móvil. El citado RNC es capaz de controlar una transferencia Inter RAT a la E-UTRAN del citado UE. Debe observarse que cualquier electrónica interna de la realización no necesaria para la

comprensión del método y disposición de acuerdo con las realizaciones de la invención ha sido omitida de la Fig. 3 en aras de la claridad. Debe observarse también que las unidades descritas comprendidas dentro de la realización 300 deben ser consideradas como entidades lógicas y no con necesidad como entidades físicas separadas.

La citada disposición 300 comprende una interfaz 301 para comunicarse con un Nodo de Soporte de GPRS de Servicio, SGSN (Serving GPRS Support Node, en inglés), estando la citada interfaz 301 adaptada para recibir, de SGSN, claves de seguridad generadas durante la autenticación y el acuerdo de clave, AKA (Authentication and Key Agreement, en inglés), durante la conexión del UE a la red de servicio. Las citadas claves de seguridad pueden ser la clave de cifrado de UMTS CK y la clave de protección de integridad de UMTS IK.

La disposición puede además comprender una unidad de cifrado y de protección de integridad 302 para el manejo del cifrado y de la protección de integridad, utilizando las claves de seguridad recibidas, de los datos de usuario y de la señalización de control enviados entre el RNC y el UE cuando el RNC está actuando como RNC de Servicio para el citado UE.

La disposición también comprende una unidad de procesamiento 303 capaz de determinar con qué tipo de UICC está equipado el UE analizando las claves de seguridad recibidas desde el SGSN, y utilizando el conocimiento de con qué tipo de UICC está equipado del UE para basar una decisión de si permitir la transferencia del UE a la E-UTRAN.

Como se ha descrito previamente para el método ilustrado en la Fig. 2, esto puede ser realizado utilizando propiedades de las funciones de conversión de clave conocidas para el SRNC tal como se describen en lo anterior.

Las realizaciones de la invención proporcionan así al SRNC la posibilidad de limitar la configuración de las mediciones de la célula de E-UTRA (etapa 11 – 12 de la Fig. 1) y la transferencia (la Fig. 1, etapa 13) de UTRA a E-UTRA para aquellos UE que tienen una llamada en curso de un cierto tipo, tal como una llamada de emergencia y tienen capacidad de E-UTRA, y para aquellos UE que tienen una llamada en curso de cualquier tipo, tal como una llamada que no es de emergencia, tienen capacidad de E-UTRA y tienen un USIM.

Las realizaciones la invención proporcionan así una solución para cómo puede la UTRAN identificar el tipo de UICC en el UE, y este conocimiento proporciona la flexibilidad para que la red inicie mediciones de UE y lleve a cabo transferencia de UTRAN a E-UTRAN para un UE con capacidad de E-UTRA sobre la base del tipo de llamada / servicios del UE en curso.

Esta posibilidad puede ser proporcionada sin cambio de señalización de la Capa 3, L3 (Layer 3, en inglés), es decir, sobre la base de los estándares del 3GPP de Versión 8.

La presente invención puede, por supuesto, ser llevada a cabo de otras maneras distintas de las específicamente establecidas en esta memoria sin separarse de las características esenciales de la invención. Las presentes realizaciones deben ser consideradas en todos los aspectos como ilustrativas y no restrictivas.

Abreviaturas

3GPP	Programa de Colaboración de Tercera Generación	Third Generation Partnership Program, en inglés
AKA	Autenticación y Acuerdo de Claves	Authentication and Key Agreement, en inglés
AUC	Centro de Autenticación	Authentication Center, en inglés
CK	Clave Cifrada	Cipher Key, en inglés
E-UTRA	UTRA Evolucionado	Evolved UTRA, en inglés
E-UTRAN	UTRAN Evolucionada	Evolved UTRAN, en inglés
GSM	Sistema Global para comunicaciones Móviles	Global System for Mobile communications
HLR	Registro de Ubicación de abonados Locales	Home Location Register
IK	Clave de Integridad	Integrity Key
Kc	Clave de Cifrado	Ciphering Key
MME	Entidad de Gestión de Móviles	Mobile Management Entity
PS	Servicios de Paquetes	Packet Services
RAT	Tecnología de Acceso por Radio	Radio Access Technology
RNC	Controlador de Red de Radio	Radio Network Controller
RRC	Control de Recurso de Radio	Radio Resource Control
SRNC	RNC de Servicio	Serving RNC
SGSN	Nodo de Soporte de GPRS de Servicio	Serving GPRS Support Node
SGW	Puerta de Enlace de Servicio	Serving Gateway
SIM	Módulo de Identidad de Abonados de GSM	GSM Subscriber Identity Module
UE	Equipo de Usuario	User Equipment
UICC	Tarjeta de Circuitos Integrados de UMTS	UMTS Integrated Circuit Card
UMTS	Sistema de Telecomunicaciones mediante telefonía Móvil Universal	Universal Mobile Telecommunications System
USIM	Módulo de Identidad de Abonados Universal	Universal Subscriber Identity Module
	(Cont.)	
UTRA	Acceso por Radio Terrestre de UMTS	UMTS Terrestrial Radio Access
UTRAN	Red de Acceso por Radio Terrestre de UMTS	UMTS Terrestrial Radio Access Network
VLR	Registro de Ubicación de Visitantes	Visitor Location Register

REIVINDICACIONES

1. Un método para su uso en un Controlador de Red de Radio de servicio, SRNC, para controlar la transferencia inter Tecnología de Acceso Por Radio, RAT, a la Red de Acceso Terrestre Universal Evolucionado, E-UTRAN, de un Equipo de Usuario, UE, con capacidad de Acceso Terrestre Universal Evolucionado, E-UTRA, que opera en una red de servicio que comprende el citado SRNC, donde el SRNC recibe, de un Nodo de Soporte de GPRS de Servicio, SGSN, claves de seguridad generadas durante la autenticación y el acuerdo de clave, AKA, caracterizado además por las etapas de:

- determinar (202) por parte del SRNC qué suscripción es proporcionada al UE por una Tarjeta de Circuitos Integrados de UMTS, UICC, con la que está equipado el UE analizando las claves de seguridad recibidas desde el SGSN, utilizando propiedades de las funciones de conversión de clave conocidas para el SRNC;

- utilizar el conocimiento de con qué tipo de UICC está equipado el UE para basar una decisión (204) sobre si permitir una transferencia del UE a la E-UTRAN.

2. El método de acuerdo con la reivindicación 1, que comprende la etapa de permitir que la transferencia del UE a la E-UTRAN sea iniciada si el UE tiene una UICC que proporciona una suscripción válida para la E-UTRAN o si se cumple al menos una condición relativa al tipo del servicio en curso del citado UE (206).

3. El método de acuerdo con la reivindicación 1 ó 2, que comprende las etapas de

- permitir que una transferencia del UE a la E-UTRAN sea iniciada si se cumple al menos una de las siguientes condiciones:

  - el UE tiene una UICC que proporciona una suscripción válida para la E-UTRAN, o

  - el UE tiene una llamada de emergencia en curso,

o si no,

- no permitir una transferencia Inter RAT del UE a la E-UTRAN (207).

4. El método de acuerdo con cualquiera de las reivindicaciones 1 – 3, en el que las claves de seguridad recibidas desde el SGSN son analizadas aplicando funciones de conversión conocidas para el SRNC, estando las citadas funciones de conversión definidas para obtener las claves de seguridad que son válidas para acceder a la red de servicio a partir de una clave de seguridad no válida.

5. El método de acuerdo con cualquiera de las reivindicaciones 1 – 4, en el que la transferencia Inter RAT es una transferencia de la UTRAN a la E-UTRAN.

6. El método de acuerdo con la reivindicación 5, en el que las claves de seguridad definidas para el acceso UTRA, generadas por una UICC que proporciona una suscripción de UMTS, son una clave de cifrado, CK, de 128 bits y una clave de protección de integridad, IK, de 128 bits, por lo que una clave de cifrado, Kc, generada por una UICC que proporciona una suscripción de UMTS puede ser convertida a las citadas claves de seguridad definidas para acceso UTRA mediante las siguientes funciones de conversión:

CK = Kc | | Kc (ecuación c4)

IK = Kc1 xor Kc2 | | Kc | | Kc1 xor Kc2 (ecuación c5)

7. El método de acuerdo con la reivindicación 6, en el que la etapa de determinar qué suscripción es proporcionada al UE por la UICC con la que está equipado un UE con capacidad de E-UTRA comprende

- comprobar si la CK recibida del SGSN consiste en dos Kc de 64 bits idénticas de acuerdo con la ecuación c4,

- si no, concluir que el UE está equipado con una UICC de tipo USIM; o si no,

- calcular un valor de prueba que cumple la ecuación c5, donde Kc = Kc1 | | Kc2 es una de las dos Kc y Kc1 de 64 bits idénticas y Kc2 son ambas de 32 bits de longitud, de manera que si el valor de prueba es igual a la IK recibida del SGSN, entonces concluir que el UE está equipado con una UICC que proporciona una suscripción de GSM, o si no, concluir que el UE está equipado con una UICC que proporciona una suscripción de UMTS.

8. Un aparato (300) para su uso en un Controlador de Red de Radio, RNC, capaz de controlar una transferencia Inter Red de Acceso por Radio, RAT, a la Red de Acceso Terrestre Universal Evolucionado, E-UTRAN, de un UE con capacidad de Acceso Terrestre Universal, E-UTRA, que opera en una red de servicio que comprende el citado RNC, comprendiendo el aparato (300) una interfaz (301) para comunicarse con un Nodo de Soporte de GPRS de Servicio, SGSN, estando la citada interfaz adaptada para recibir, del SGSN, claves de seguridad generadas durante

la autenticación y el acuerdo de clave, AKA; caracterizado además por que comprende una unidad de procesamiento (303) configurada para:

- determinar qué suscripción es proporcionada al UE por una Tarjeta de Circuitos Integrados de UMTS, UICC, con la que está equipado el UE analizando las claves de seguridad recibidas desde el SGSN, utilizando propiedades de funciones de conversión de clave conocidas para el SRNC;

- utilizar el conocimiento de qué suscripción es proporcionada al UE por la UICC con la que está equipado el UE para basar una decisión de si permitir una transferencia del UE a la E-UTRAN.

9. El aparato (300) de acuerdo con la reivindicación 8, en el que la citada unidad de procesamiento (303) está configurada para permitir que una transferencia del UE a la E-UTRAN sea iniciada si el UE tiene una UICC válida para la E-UTRAN o si se cumple al menos una condición relativa a qué tipo de servicio en curso del citado UE se cumple.

10. El aparato (300) de acuerdo con la reivindicación 8 ó 9, en el que la citada unidad de procesamiento (303) está configurada para

- permitir que una transferencia del UE a la E-UTRAN sea iniciada si se cumple al menos una de las siguientes condiciones:

  - el UE tiene una UICC que proporciona una suscripción válida para la E-UTRAN, o

  - el UE tiene una llamada de emergencia en curso,

o si no,

- no permitir una transferencia Inter RAT del UE a la E-UTRAN.

11. El aparato (300) de acuerdo con cualquiera de las reivindicaciones 8 – 10, en el que la citada unidad de procesamiento (303) está configurada para analizar las claves de seguridad recibidas del SGSN aplicando funciones de conversión conocidas para el SRNC, estando las citadas funciones de conversión definidas para obtener claves de seguridad que son válidas para acceder a la red de servicio a partir de una clave de seguridad no válida.

12. El aparato (300) de acuerdo con cualquiera de las reivindicaciones 8 – 11, en el que la disposición es capaz de controlar una transferencia Inter RAT de la UTRAN a la E-UTRAN.

13. El aparato (300) de acuerdo con la reivindicación 12, en el que las claves de seguridad definidas para el acceso UTRA, generadas por una UICC que proporciona una suscripción de UMTS son una clave de cifrado (CK) de 128 bits y una clave de protección de integridad, IK, de 128 bits, por lo que una clave de cifrado, Kc, generada por una UICC de tipo SIM puede ser convertida a las citadas claves de seguridad definidas para el acceso UTRA mediante las siguientes funciones:

$$CK = Kc \,||\, Kc \qquad \text{(ecuación c4)}$$

$$IK = Kc1 \text{ xor } Kc2 \,||\, Kc \,||\, Kc1 \text{ xor } Kc2 \qquad \text{(ecuación c5)}$$

14. El aparato (300) de acuerdo con la reivindicación 13, en el que la unidad de procesamiento capaz de determinar qué suscripción es proporcionada por la UICC con la que está equipado un UE con capacidad de E-UTRA está configurada para

- comprobar si la CK recibida del SGSN consiste en dos Kc de 64 bits idénticas de acuerdo con la ecuación c4,

- si no, concluir que el UE está equipado con una UICC que proporciona una suscripción de UMTS; o si no,

- calcular un valor de prueba que cumple la ecuación c5, donde Kc = Kc1 | | Kc2 es una de las dos Kc de 64 bits idénticas y Kc1 y Kc2 son las dos de 32 bits de longitud, de manera que, si el valor de prueba es igual a la IK recibida del SGSN, entonces concluir que el UE está equipado con una UICC que proporciona una suscripción de UMTS, o si no, concluir que el UE está equipado con una UICC que proporciona una suscripción de UMTS.

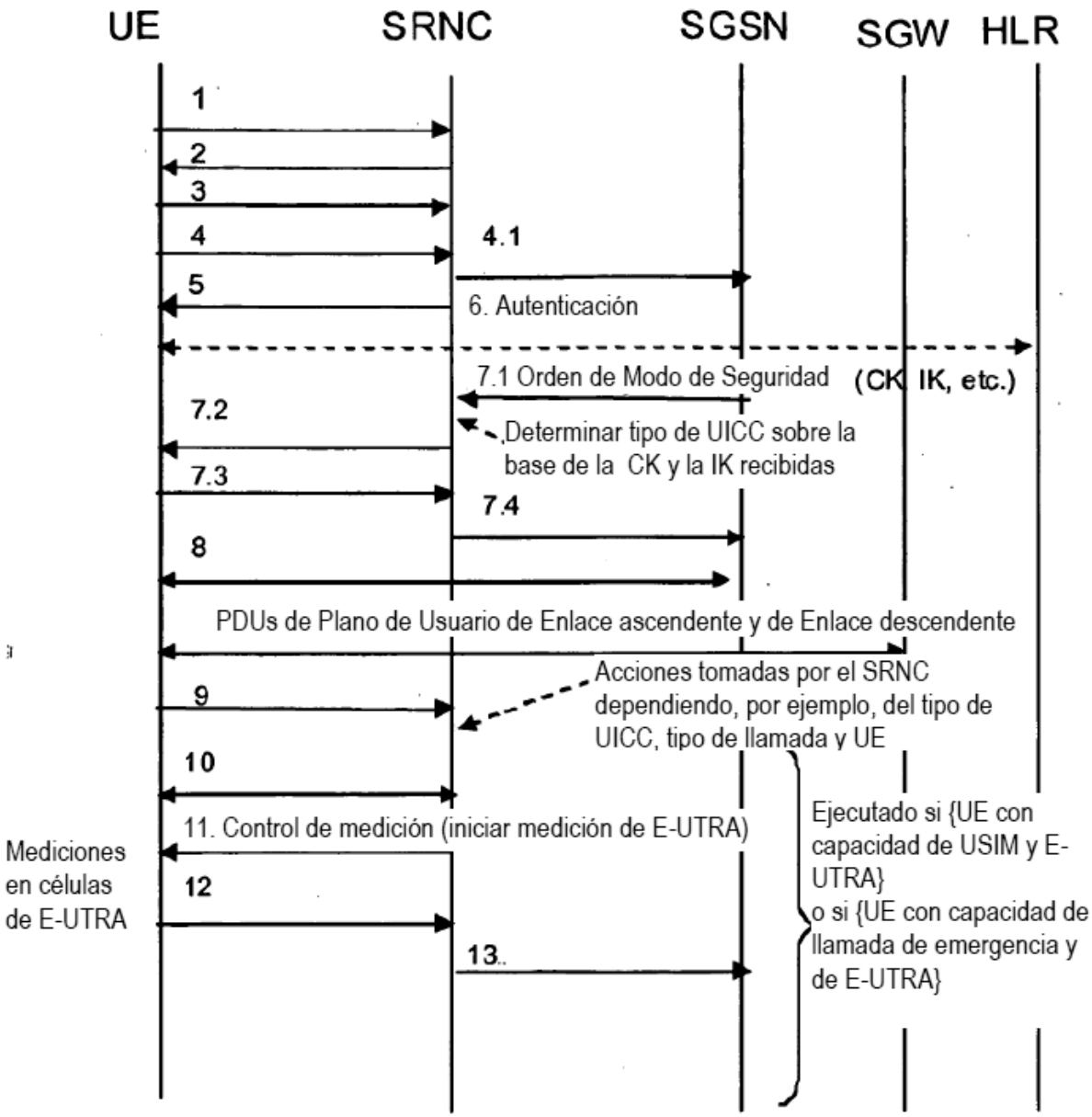
UE
SRNC
SGSN
SGW
HLR
1
2
3
4
4.1
5
6. Autenticación
7.1 Orden de Modo de Seguridad
(CK IK, etc.)
7.2
Determinar tipo de UICC sobre la base de la CK y la IK recibidas
7.3
7.4
8
PDUs de Plano de Usuario de Enlace ascendente y de Enlace descendente
Acciones tomadas por el SRNC dependiendo, por ejemplo, del tipo de UICC, tipo de llamada y UE
9
10
11. Control de medición (iniciar medición de E-UTRA)
Mediciones en células de E-UTRA
12
13
Ejecutado si {UE con capacidad de USIM y E-UTRA}
o si {UE con capacidad de llamada de emergencia y de E-UTRA}

Fig. 1

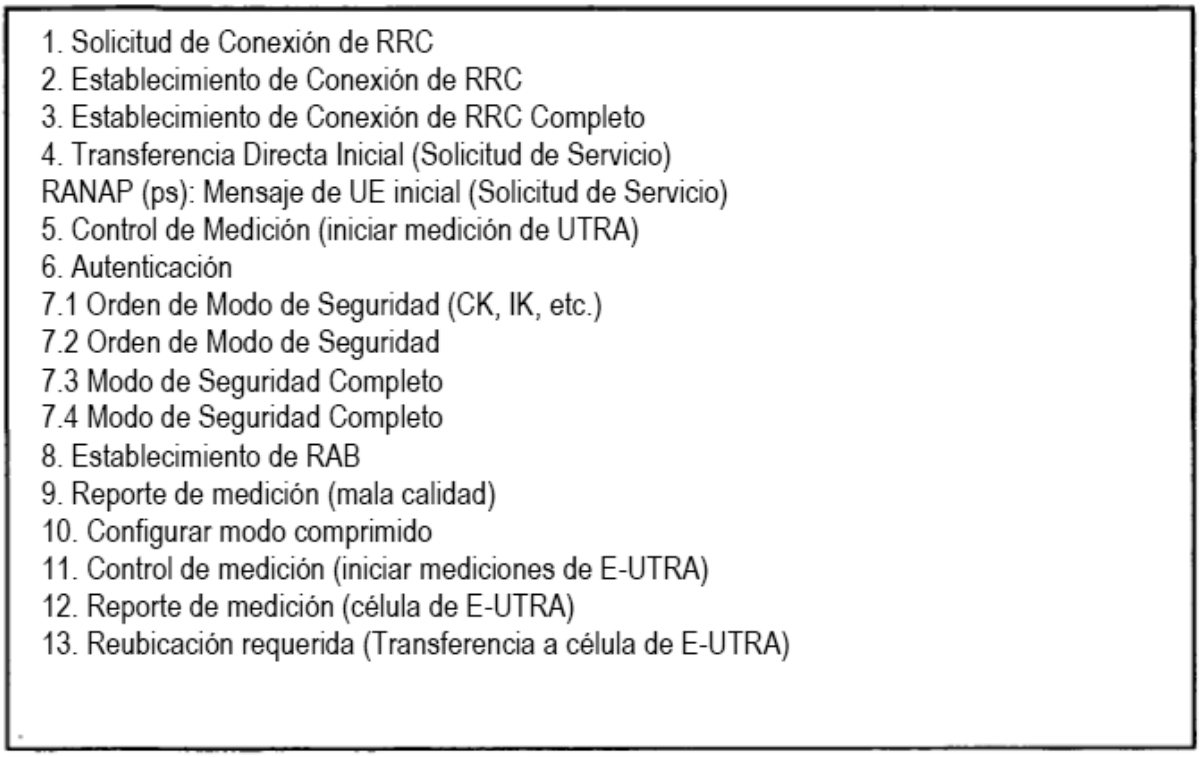

Fig. 1 (Continuación)

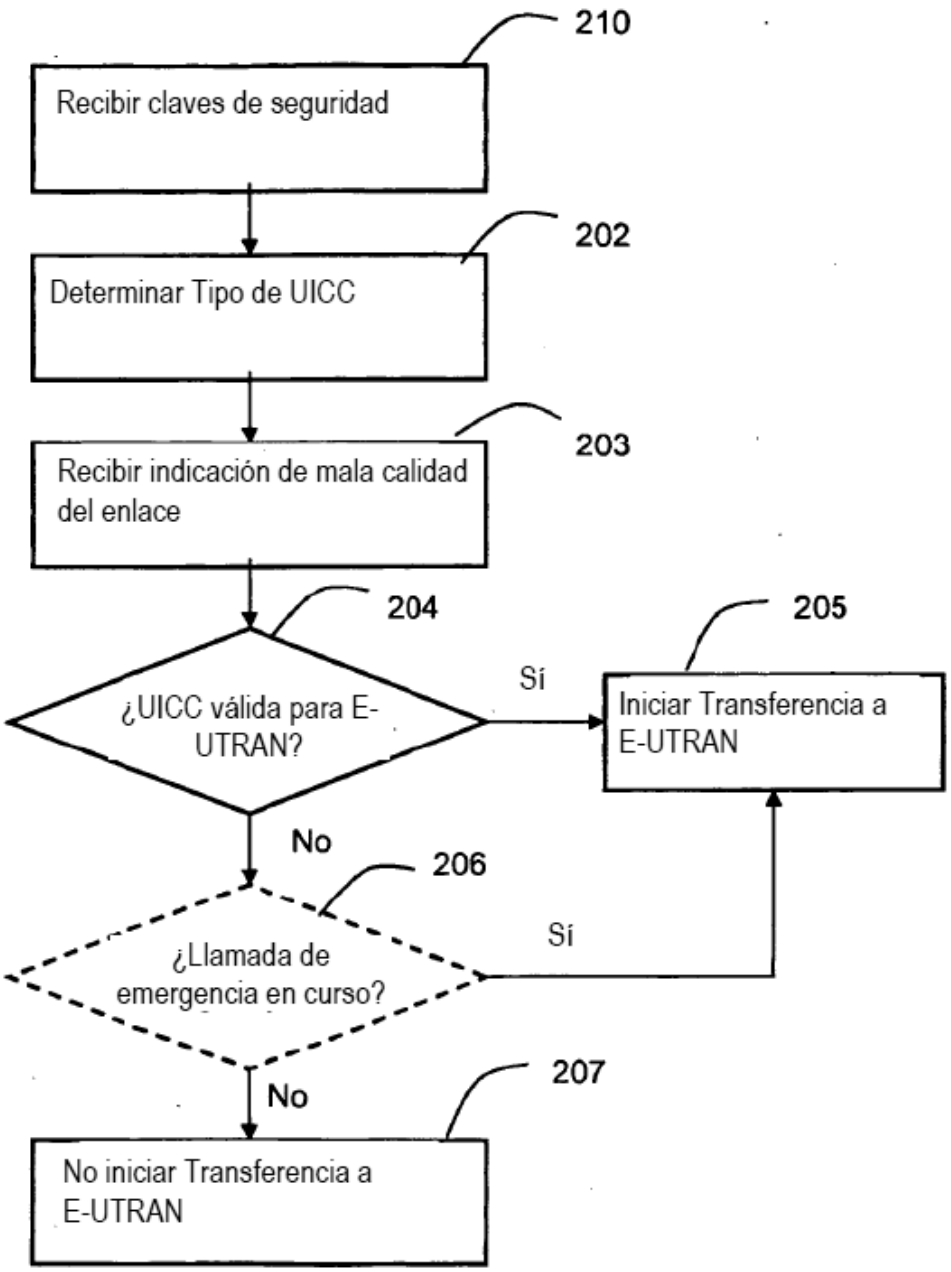
210
Recibir claves de seguridad
202
Determinar Tipo de UICC
203
Recibir indicación de mala calidad del enlace
204
¿UICC válida para E-UTRAN?
Sí
205
Iniciar Transferencia a E-UTRAN
No
206
¿Llamada de emergencia en curso?
Sí
No
207
No iniciar Transferencia a E-UTRAN

Fig. 2

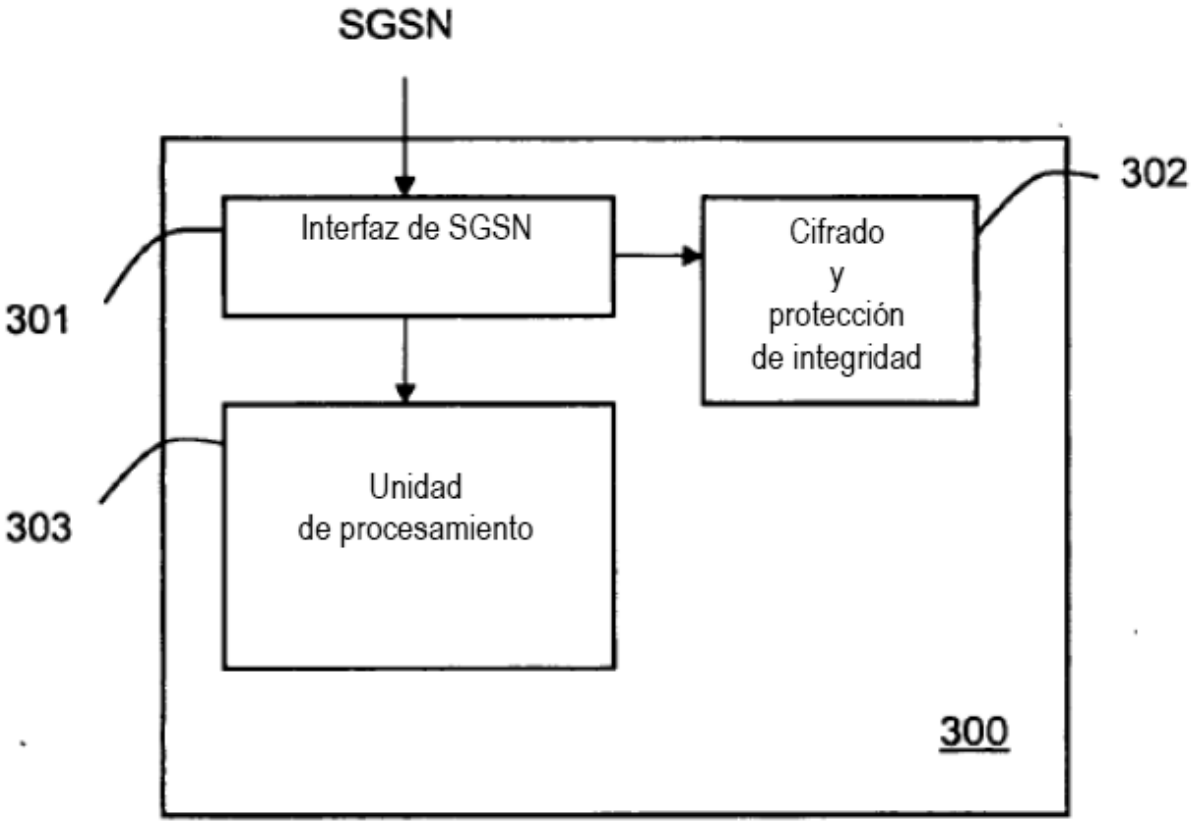
SGSN
Interfaz de SGSN
Cifrado
y
protección
de integridad
Unidad
de procesamiento
301
302
303
300

Fig. 3