(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 626 666**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04L 12/64 (2006.01)
H04W 36/12 (2009.01)
H04W 36/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.12.2008 PCT/CN2008/002116**

(87) Fecha y número de publicación internacional: **23.12.2009 WO09152656**

(96) Fecha de presentación y número de la solicitud europea: **29.12.2008 E 08874669 (8)**

(97) Fecha y número de publicación de la concesión europea: **01.03.2017 EP 2290875**

(54) Título: **Método y sistema de generación para identificador de identidad de claves durante la transferencia del dispositivo de usuario**

(30) Prioridad:

16.06.2008 CN 200810100472

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.07.2017

(73) Titular/es:

ZTE CORPORATION (100.0%)
ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District
Shenzhen, Guangdong 518057, CN

(72) Inventor/es:

ZHANG, XUWU;
GAN, LU y
HUANG, QING

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Método y sistema de generación para identificador de identidad de claves durante la transferencia del dispositivo de usuario

Campo técnico

La presente invención se refiere al campo de las telecomunicaciones móviles, particularmente a un método y sistema para la generación de un identificador de identidad de claves cuando se transfiere un equipo de usuario.

Antecedentes

Cuando un equipo de usuario (UE) se transfiere entre diferentes sistemas de acceso en un sistema de telecomunicaciones móviles, se requiere que se mapeen parámetros de seguridad de una red de servicios de origen a aquellos capaces de ser reconocidos y usados por una red de servicio objetivo, de modo que el UE pueda transferirse con éxito y desarrollar los servicios. Estos parámetros de seguridad incluyen una clave, un identificador de clave, un contador, un algoritmo de seguridad, etc.

Un sistema de paquetes evolucionado 3GPP (EPS) consiste en una red de acceso por radio terrestre UMTS evolucionada (EUTRAN) y una red del núcleo de paquetes evolucionado (EPC).

En el que la red EPC comprende una entidad de gestión de la movilidad (MME), que es la responsable de las tareas relacionadas con una superficie de control, por ejemplo, la gestión de la movilidad, procesamiento de una señalización del estrato de no acceso, y la gestión del modo de seguridad en el lado de usuario, etc.; en el que la MME almacena una clave raíz K_{ASME} (clave de la entidad de gestión de la seguridad de acceso) del EUTRAN, y genera una clave raíz K_{eNB} (clave del eNB) de un estrato de acceso para un nodo B (eNB) evolucionado basado en la K_{ASME} y un número de secuencia del estrato de no acceso (NAS SQN) del enlace ascendente. Un identificador de conjunto de claves para la entidad de gestión de la seguridad de acceso (KSI_{ASME}) es un identificador de identidad (o número de secuencia de clave) de la K_{ASME}, y el KSI_{ASME} tiene 3 bits de longitud y se usa para la identificación y recuperación de una clave entre una red y un equipo de usuario (UE). Cuando se conecta el UE con la red, de acuerdo con el KSI_{ASME}, puede notificarse a una parte opuesta para el uso de una clave especificada que se ha almacenado para establecer un contexto de seguridad sin necesidad de autenticación y asociación de clave (AKA), pueden ahorrarse así recursos de la red. Cuando se necesita borrar la clave debido a la finalización de su vida útil o por otras causas, el KSI_{ASME} se fija a “111” por el UE.

En el que el dispositivo de estación base en el EUTRAN es un nodo B evolucionado (eNB), y es responsable principalmente de las comunicaciones de radio, gestión de la comunicación de radio y gestión del contexto de movilidad.

En el sistema universal de telecomunicaciones móviles (UMTS) 3GPP, un nodo de soporte GPRS en servicio (SGSN) es un dispositivo responsable de la gestión del contexto de movilidad en el dominio de paquetes y/o la gestión del modo de seguridad en el lado del usuario. El SGSN es responsable también de la autenticación y gestión de la seguridad de una red de acceso por radio terrestre universal (UTRAN) en el UMTS, y del almacenamiento de una clave de integridad (IK) y una clave de cifrado (CK). Un identificador de identidad de claves de las CK/IK es un identificador del conjunto de claves (KSI) cuya función y uso son similares a los del KSI_{ASME} en el EPS, ambos se usan para identificación y recuperación de claves entre un UE y una red, y el KSI tiene 3 bits de longitud. Cuando el KSI es igual a 111, significa que no hay clave utilizable y el KSI no es válido. Cuando es necesario que el UE y el SGSN establezcan una conexión de seguridad UMTS a través de la asociación de claves, si se ha almacenado una clave utilizable en el UE, entonces el UE envía el KSI almacenado al SGSN que verifica si el KSI almacenado es idéntico al KSI almacenado en el UE, si es así, entonces se usa un conjunto de claves almacenado para establecer un contexto de seguridad a través de la asociación de claves y el KSI es enviado de vuelta al UE para confirmar la clave que usa el UE; si no hay clave utilizable almacenada en el UE, entonces el KSI se establece en 111 y se envía al SGSN, y el SGSN, tras detectar que el KSI está a 111, envía una mensaje de solicitud de autenticación al registro de localización local (HLR)/servidor de abonado local (HSS), y el UE y la red realizan un AKA durante una segunda vez y generan un nuevo conjunto de claves.

El SGSN es también un dispositivo responsable de la gestión del contexto de movilidad en el dominio de paquetes y/o gestión del modo de seguridad en el lado usuario en un sistema del servicio general de paquetes vía radio (GPRS)/ tasas de datos mejoradas para la evolución del GSM (EDGE). El SGSN es el responsable de la autenticación y gestión de la seguridad de una red de acceso por radio GPRS/EDGE (GERAN), y para el almacenamiento de una clave de cifrado (Kc) del GERAN; un identificador de identidad (o identificador de identidad de claves) del Kc es un número de secuencia de clave de cifrado (CKSN) cuya función y uso son las mismas que las del KSI.

Cuando un UE se transfiere desde EUTRAN a un UTRAN, una MME genera una CK y una IK para una red de servicio objetivo basándose en una K_{ASME}, y envía la CK y la IK a un SGSN, a continuación el UE y el SGSN usan la

CK y la IK para establecer un contexto de seguridad UTRAN mediante la negociación de los algoritmos de seguridad correspondientes; hay dos tipos de transferencias, que incluyen la transferencia cuando el RRC (control de recursos de radio) está en un estado activo y una transferencia cuando el UE está en un estado inactivo, en el que el primero incluye conmutación, etc., y el último incluye una solicitud de actualización del área de ruta, solicitud de adición del área de ruta, etc.

Cuando el UE se transfiere a GERAN desde el EUTRAN, la MME genera una CK y una IK basándose en la K_{ASME} (cuyo método es el mismo que el de la transferencia a UMTS), y envía la CK y la IK a un SGSN. El SGSN genera una Kc del GERAN basándose en la IK y la CK.

En la técnica anterior, un KSI_{ASME}, un KSI y un CKSN se generan todos por un lado de red durante la autenticación, y se envían a un UE a través de un mensaje de solicitud de autenticación. En un proceso de transferencia desde un EUTRAN a un UTRAN o un GERAN, aunque una MME genere una IK y una CK necesarias por el UTRAN o el GERAN para una red de servicio objetivo, no se genera ningún identificador de identidad correspondiente al par de claves, después de la finalización de la transferencia el UE y el SGSN no son capaces de recuperar las claves generadas durante la transferencia y, por lo tanto, no puede usar el par de claves. Cuando el UE y la red necesitan restablecer un control de recursos de radio (RRC) u otras conexiones, han de ser generadas nuevas claves a través de un AKA antes de establecer una conexión de radio, debido a que no pueden usarse esas claves almacenadas. Esto incrementa indudablemente la sobrecarga de señalización tanto de la red como del UE y retarda el tiempo de comunicación normal entre el UE y la red, dando como resultado un deterioro de la satisfacción del usuario.

El documento EP 1 841 267 A2 explica un sistema y método para la optimización de un procedimiento de autenticación durante traspasos del sistema entre accesos.

El documento 3GPP TS 33.401 v2.0.0 (2008-05) explica una evolución de la arquitectura del sistema (SAE) 3GPP.

Sumario

La presente invención se dirige principalmente a proporcionar un método y sistema para la generación de un identificador de identidad de claves cuando se transfiere un equipo de usuario, que sea capaz de resolver el problema de la técnica anterior en la que una clave mapeada desde una K_{ASME} en un proceso de transferencia no tiene identificador de identidad después de que un equipo de usuario se transfiera desde un EUTRAN a un UTRAN o un GERAN.

La presente invención se dirige a una materia objeto tal como se divulga en las reivindicaciones adjuntas.

El esquema técnico de la presente invención puede proporcionar una clave con un identificador de identidad en un proceso de transferencia, para reutilizar una clave generada a partir de una K_{ASME}, resolviendo de ese modo el problema de que la clave generada a partir de la K_{ASME} no puede reutilizarse debido a una carencia de un identificador de identidad cuando un UE se transfiere desde un EUTRAN a otro sistema, reduciendo así la señalización interactiva entre el UE y la red.

Breve descripción de los dibujos

Los dibujos a ser descritos en el presente documento se usan para facilitar una comprensión adicional y constituyen parte de la presente solicitud. Los ejemplos de implementación de la presente invención y la descripción de la misma se usan para explicación de la presente invención, y no deberán interpretarse como una limitación inapropiada de la presente invención. En los dibujos,

La Fig. 1 es un diagrama esquemático que ilustra un método para la generación de un KSI cuando un UE se transfiere desde un EUTRAN a un UTRAN en la presente invención;

La Fig. 2 es un diagrama esquemático que ilustra un método para la generación de un KSI cuando un UE se transfiere desde un EUTRAN a un GERAN en la presente invención;

La Fig. 3 es un diagrama de flujo de señalización de la realización del Ejemplo de Aplicación Uno del método en la presente invención;

La Fig. 4 es un diagrama de flujo de señalización de la realización del Ejemplo de Aplicación Dos del método en la presente invención;

La Fig. 5 es un diagrama de flujo de señalización de la realización del Ejemplo de Aplicación Tres del método en la presente invención;

La Fig. 6 es un diagrama de flujo de señalización de la realización del Ejemplo de Aplicación Cuatro del método en la presente invención;

La Fig. 7 es un diagrama de flujo de señalización de la realización del Ejemplo de Aplicación Cinco del método en la presente invención;

La Fig. 8 es un diagrama de flujo de señalización de la realización del Ejemplo de Aplicación Seis del método en la presente invención;

Descripción detallada

El esquema técnico de la invención se describirá adicionalmente en detalle basándose en los dibujos y realizaciones.

Un método para la generación de un identificador de identidad de claves cuando un UE se transfiere en la presente invención incluye las siguientes etapas:

cuando un UE se transfiere desde un EUTRAN a un sistema objetivo, una MME envía un identificador de identidad de una K_{ASME} (KSI_{ASME}) a un SGSN, y tanto el SGSN como el UE mapean el KSI_{ASME} en un identificador de identidad de claves del sistema objetivo.

En el que el método de mapeado puede incluir las siguientes etapas: asignar directamente del KSI_{ASME} al identificador de identidad de claves del sistema objetivo, asignar directamente de la suma del KSI_{ASME} y una constante al identificador de identidad de claves del sistema objetivo; y

el SGSN y el UE acuerdan sobre el método de mapeado y la constante.

En el que el método de mapeado incluye también la siguiente etapa: el UE y el SGSN almacenan el identificador de identidad de claves del sistema objetivo adquirido a partir del mapeado conjunto con la clave del sistema objetivo generada a partir de la K_{ASME}.

En el que la suma del KSI_{ASME} y la constante no puede ser 111, en caso contrario, se alterará de acuerdo con el acuerdo entre el UE y el SGSN, por ejemplo mediante su sustitución con un siguiente valor 000 u otro valor.

En el que si el UE y el SGSN han acordado acerca de una clave antes de la transferencia y el identificador de identidad de claves almacenado en el sistema objetivo es el mismo que el identificador de identidad de claves del sistema objetivo mapeado desde el KSI_{ASME} durante la transferencia, entonces se borra la clave almacenada antes de la transferencia.

En el que la transferencia del UE desde el EUTRAN a otros sistemas de acceso por radio significa la transferencia del UE a un sistema UTRAN o un sistema GERAN; y hay dos tipos de transferencia: transferencia inactiva y conmutación.

Cuando un UE se transfiere en un estado inactivo desde el EUTRAN a un UTRAN, el método de generación, tal como se muestra en la Fig. 1, comprende las siguientes etapas específicas:

A1: después de recibir un mensaje de solicitud de contexto o un mensaje de solicitud de identificación, una MME genera una IK y una CK basándose en la K_{ASME} y envía el KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN a través de un mensaje de respuesta de contexto o un mensaje de respuesta de identificación;

A2: después de la recepción del KSI_{ASME}, la IK y la CK desde la MME, el SGSN mapea el KSI_{ASME} en un KSI, y almacena el KSI, la IK y la CK conjuntamente; y el SGSN envía un mensaje de indicación de finalización del mapeado del KSI al UE; y

A3: el UE mapea el KSI_{ASME} en un KSI, es decir, asignando el valor del KSI_{ASME} al KSI: KSI = KSI_{ASME}, y almacena el KSI junto con la IK y la CK que se generan a partir de la K_{ASME}.

Adicionalmente, se incluye la siguiente etapa antes de la etapa A1:

A0: el UE decide transferirse a un UTRAN en un estado inactivo, y envía al SGSN un mensaje de solicitud de transferencia inactiva al UTRAN, en el que el mensaje de solicitud es un mensaje de solicitud de actualización del área de ruta o un mensaje de solicitud de adición del área de ruta; después de la recepción del mensaje de solicitud de transferencia inactiva al UTRAN que se envía desde el UE, el SGSN envía un mensaje de solicitud correspondiente a la MME.

Adicionalmente, en correspondencia, en la etapa A2, el mensaje de indicación de finalización del mapeado del KSI enviado por el SGSN es un mensaje de aceptación de actualización del área de ruta o un mensaje de aceptación de adición del área de ruta.

Adicionalmente, la etapa A3 puede tener lugar en cualquier etapa después de que el UE decida transferirse al UTRAN en un estado inactivo y antes de que el UE envíe un mensaje de finalización de actualización del área de ruta o mensaje de finalización de adición del área de ruta correspondiente al SGSN.

Cuando el UE conmuta desde el EUTRAN a un UTRAN, las etapas específicas del método de generación son como sigue:

a1: después de la recepción de un mensaje de solicitud de conmutación, la MME genera una IK y una CK basándose en la K_{ASME}, y envía el KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN a través de un mensaje de solicitud de envío y redirección;

a2: tras la recepción del KSI_{ASME}, la IK y la CK desde la MME, el SGSN mapea el KSI_{ASME} en un KSI, y almacena el KSI, la IK y la CK juntas; el SGSN envía un mensaje de respuesta de envío y redirección de indicación de finalización del mapeado del KSI a la MME; y la MME envía una orden de conmutación para dar instrucciones al UE para conmutar; y

a3: después de la recepción de la orden de conmutación desde la red, el UE mapea el KSI_{ASME} en un KSI, y almacena el KSI junto con la IK y la CK que se generan a partir de la K_{ASME}.

El método mencionado anteriormente para la generación de un KSI mapea un valor de un KSI_{ASME} en el EUTRAN en un valor de un KSI en el UTRAN, y garantiza que el KSI adquirido a través de mapeado y un número de secuencia de clave previamente almacenado no se repiten, resolviendo así el problema de la técnica anterior en la que una IK y una CK adquiridas a través de un mapeado no pueden reutilizarse debido a una carencia de identificadores de identidad cuando un UE se transfiere desde un EUTRAN a un UTRAN.

Cuando el UE se transfiere en un estado inactivo desde el EUTRAN a un GERAN, el método de generación, tal como se muestra en la Fig. 2, comprende las etapas específicas como sigue:

B1: después de recibir un mensaje de solicitud de contexto o de solicitud de identificación, la MME genera una IK y una CK basándose en la K_{ASME} y envía el KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN a través de un mensaje de respuesta de contexto o un mensaje de respuesta de identificación;

B2: después de la recepción del KSI_{ASME}, la IK y la CK desde la MME, el SGSN genera una Kc basándose en la IK y la CK, mapea el KSI_{ASME} en un CKSN, y almacena el CKSN junto con la Kc generada a partir de la IK y la CK; y el SGSN envía al UE un mensaje de indicación de finalización del mapeado del CKSN; y

B3: el UE mapea el KSI_{ASME} en un CKSN, y almacena el CKSN junto con la Kc generada a partir de la K_{ASME}.

Adicionalmente, se incluye la siguiente etapa antes de la etapa B1:

B0: el UE decide transferir a un GERAN en un estado inactivo, y envía al SGSN un mensaje de solicitud de transferencia inactiva al UTRAN, en el que el mensaje de solicitud es un mensaje de solicitud de actualización del área de ruta o un mensaje de solicitud de adición del área de ruta; después de la recepción del mensaje de solicitud de transferencia inactiva al UTRAN que se envía desde el UE, el SGSN envía un mensaje de solicitud correspondiente a la MME.

En correspondencia, en la etapa B2, el mensaje de indicación de finalización del mapeado del CKSN enviado por el SGSN es un mensaje de aceptación de actualización del área de ruta o un mensaje de aceptación de adición del área de ruta.

Adicionalmente, la etapa B3 puede tener lugar en cualquier paso después de que el UE decida transferirse al GERAN en un estado inactivo y antes de que el UE envíe un mensaje de conmutación correspondiente al lado de red.

Cuando el UE conmuta desde el EUTRAN a un GERAN, las etapas específicas del método de generación son como sigue:

b1: tras la recepción de un mensaje de solicitud de conmutación, la MME genera una IK y una CK basándose en la K_{ASME}, y envía el KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN a través de un mensaje de solicitud de envío y redirección;

b2: tras la recepción del KSI, la IK y la CK desde la MME, el SGSN genera una Kc basándose en la IK y la CK, mapea el KSI_{ASME} en un CKSN, y almacena el CKSN junto con la Kc generada a partir de la IK y la CK; el SGSN envía un mensaje de indicación de finalización del mapeado del CKSN a la MME; y la MME envía una orden de conmutación para dar instrucciones al UE para conmutar; y

b3: después de la recepción de la orden de conmutación desde la red, el UE mapea el KSI_{ASME} en un CKSN, y almacena el CKSN junto con la Kc generada a partir de la K_{ASME}.

El método mencionado anteriormente para la generación de un KSI mapea un valor de un KSI_{ASME} en un valor de un CKSN, y garantiza que el CKSN y un número de secuencia de clave previamente almacenado no se repiten, resolviendo así el problema de la técnica anterior en la que una Kc adquirida a través de un mapeado no puede reutilizarse debido a una carencia de identificadores de identidad cuando un UE se transfiere desde un EUTRAN a un GERAN.

Un sistema para la generación de un identificador de identidad de claves cuando un UE transfiere en la presente invención incluye un UE, una MME y un SGSN;

la MME se usa para el envío de un KSI_{ASME} al SGSN cuando el UE se transfiere desde un EUTRAN a un sistema objetivo; y
tanto el SGSN como el UE se usan para mapeado del KSI_{ASME} en un identificador de identidad de claves del sistema objetivo;
en el que el SGSN/UE puede realizar el mapeado en el siguiente método: asignar directamente del KSI_{ASME} al identificador de identidad de claves del sistema objetivo, o asignar directamente de la suma del KSI_{ASME} y una constante al identificador de identidad de claves del sistema objetivo;
el SGSN y el UE acuerdan sobre el método de mapeado y la constante.

En el que el SGSN y el UE se usan también para almacenamiento del identificador de identidad de claves del sistema objetivo generado durante el mapeado junto con la clave del sistema objetivo generada a partir de la K_{ASME}.

En el que la suma del KSI_{ASME} y la constante no puede ser 111, en caso contrario, puede alterarse en consonancia con el acuerdo entre el UE y el SGSN, por ejemplo sustituyéndole con un siguiente valor 000 u otro valor.

El UE y el SGSN se usan también para borrar una clave almacenada antes de la transferencia cuando el UE y el SGSN han acordado acerca de una clave antes de la transferencia y el identificador de identidad de claves del sistema objetivo almacenado es el mismo que el identificador de identidad de claves del sistema objetivo mapeado desde el KSI_{ASME} durante la transferencia.

En el que la transferencia del UE desde el EUTRAN a otro sistema de acceso por radio significa la transferencia del UE a un sistema UTRAN o un sistema GERAN; y hay dos tipos de transferencia: transferencia inactiva y conmutación.

En el que el UE consiste en una unidad de interacción del mensaje, una unidad de mapeado del identificador de clave y una unidad de almacenamiento de claves e identificador de claves;

la unidad de interacción del mensaje se usa para la recepción de un mensaje desde un lado de red;
la unidad de mapeado del identificador de claves se usa para mapeado del KSI_{ASME} en el identificador de identidad de claves del sistema objetivo cuando la unidad de interacción del mensaje recibe una orden de conmutación, un mensaje de aceptación de actualización del área de ruta o un mensaje de aceptación de adición del área de ruta, el mapeado del KSI_{ASME} en un KSI cuando el sistema objetivo es un UTRAN, y el mapeado del KSI_{ASME} en un CKSN cuando el sistema objetivo es un GERAN; y
la unidad de almacenamiento de claves e identificador de claves se usa para almacenar una clave de un sistema objetivo y un identificador de identidad de claves del sistema objetivo conjuntamente.

La MME consiste en una unidad de recepción del mensaje de solicitud y una unidad de procesamiento del parámetro de seguridad;

la unidad de recepción del mensaje de solicitud se usa para la recepción de mensajes de solicitud de transferencia desde otras entidades de red e instruir a la unidad de procesamiento del parámetro de seguridad para procesar estos mensajes; si el mensaje de solicitud de transferencia es un mensaje de solicitud de contexto o un mensaje de solicitud de identificación, entonces la unidad de recepción del mensaje de solicitud envía una primera instrucción de procesamiento a la unidad de procesamiento del parámetro de seguridad; si el mensaje de solicitud de transferencia es un mensaje de solicitud de conmutación, entonces la unidad de recepción del mensaje de solicitud envía una segunda instrucción de procesamiento a la unidad de procesamiento del parámetro de seguridad; y
la unidad de procesamiento del parámetro de seguridad se usa para generar una CK y una IK basándose en la K_{ASME} y el envío del KSI_{ASME} junto con la IK y la CK que se han generado a partir de la K_{ASME} al SGSN después de la recepción de una instrucción desde la unidad de recepción del mensaje de solicitud; si la instrucción es la primera instrucción de procesamiento, entonces la unidad de procesamiento del parámetro de seguridad envía el KSI_{ASME} junto con la IK y la CK que se han generado a partir de la K_{ASME} al SGSN a través de un mensaje de respuesta de contexto o un mensaje de respuesta de identificación; y si la instrucción es la segunda instrucción de procesamiento, entonces la unidad de procesamiento del parámetro de seguridad envía el KSI_{ASME} junto con

la IK y la CK que se han generado a partir de la K_{ASME} al SGSN a través de un mensaje de solicitud de envío y redirección.

El SGSN consiste en una unidad de procesamiento del parámetro de seguridad, una unidad de interacción del mensaje, una unidad de mapeado del identificador de claves, y una unidad de generación de claves;

la unidad de recepción del parámetro de seguridad se usa para la recepción de las claves y del KSI_{ASME} desde la MME, el envío del KSI_{ASME} a la unidad de mapeado del identificador de claves, generación de una clave de un sistema objetivo basándose en las claves enviadas por la MME y su envío a la unidad de almacenamiento de claves e identificador de claves: si se juzga que el sistema objetivo es un UTRAN, entonces la unidad de recepción del parámetro de seguridad envía las claves enviadas por la MME a la unidad de almacenamiento de claves e identificador de claves; y si el sistema objetivo es un GERAN, entonces la unidad de recepción del parámetro de seguridad genera una Kc basándose en las claves enviadas por la MME y envía la Kc a la unidad de almacenamiento de claves e identificador de claves;
la unidad de mapeado del identificador de claves se usa para mapeado del KSI_{ASME} en un identificador de identidad de claves de un sistema objetivo después de la recepción del KSI_{ASME}: si se juzga que el sistema objetivo es un UTRAN, entonces la unidad de mapeado del identificador de claves mapea el KSI_{ASME} en un KSI; y si el sistema objetivo es un GERAN, entonces la unidad de mapeado del identificador de claves mapea el KSI_{ASME} en un CKSN; y envía el identificador de identidad de claves adquirido a través del mapeado a la unidad de almacenamiento de claves e identificador de claves;
la unidad de almacenamiento de claves e identificador de claves se usa para almacenamiento tanto de la clave del sistema objetivo enviada por la unidad de recepción del parámetro de seguridad como el identificador de identidad de claves del sistema objetivo enviada por la unidad de mapeado del identificador de claves, y para notificación a la unidad de interacción del mensaje de la finalización del mapeado después del almacenamiento; y
la unidad de interacción del mensaje se usa para el envío de una notificación de éxito del mapeado del identificador de claves en el lado de red después de la recepción del mensaje de finalización de mapeado.

En el que la unidad de interacción del mensaje en el UE se usa también para el envío de un mensaje de solicitud de actualización del área de ruta o un mensaje de solicitud de adición del área de ruta al SGSN cuando el UE decide transferirse en un estado inactivo; y

la unidad de interacción del mensaje en el SGSN se usa también para el envío de un mensaje de solicitud de contexto o un mensaje de solicitud de identificación correspondientes a la MME después de haber recibido el mensaje de solicitud de actualización del área de ruta o el mensaje de solicitud de adición del área de ruta.

En el que la unidad de mapeado del identificador de claves en el UE se usa también para mapeado del KSI_{ASME} en el identificador de identidad de claves del sistema objetivo cuando el UE decide transferirse en un estado inactivo.

En el que la unidad interacción del mensaje en el SGSN envía una notificación de éxito de mapeado del identificador de claves del lado de red, es decir: si el mensaje de envío de la clave y del identificador de claves por la MME es un mensaje de respuesta de contexto o un mensaje de respuesta de identificación, entonces la unidad de interacción del mensaje envía en consecuencia un mensaje de aceptación de actualización del área de ruta o un mensaje de aceptación de adición del área de ruta al UE para indicar el éxito del mapeado del identificador de claves del lado de red; y si el mensaje de envío de la clave y el identificador de claves por la MME es un mensaje de solicitud de envío y redirección, entonces la unidad de interacción del mensaje envía un mensaje de respuesta de envío y redirección a la MME para indicar el éxito del mapeado del identificador de claves del lado de red.

El sistema para la generación de un identificador de identidad de claves mapea un valor de un KSI_{ASME} en un valor de un KSI o un valor de un CKSN, y garantiza que el KSI o CKSN adquiridos a través del mapeado y un número de secuencia clave previamente almacenado en un SGSN no se repiten, resolviendo así el problema en la técnica anterior de que una IK y una CK o una Kc mapeadas a partir de la K_{ASME} no pueden reutilizarse debido a la carencia de identificadores de identidad cuando el UE se transfiere desde un EUTRAN a un UTRAN, y reduciendo la señalización interactiva entre el UE y la red, y mejorando la satisfacción del usuario.

La siguiente parte describe adicionalmente la invención con seis ejemplos de aplicación.

La Fig. 3 es el Ejemplo de Aplicación Uno del método de la presente invención, que ilustra un diagrama de flujo del método para la generación de un identificador de claves cuando un UE se transfiere en un estado inactivo desde un EUTRAN a un UTRAN, lo que incluye las siguientes etapas:

etapa S301: un UE decide transferirse a un UTRAN en un estado inactivo y envía a un SGSN objetivo un mensaje de solicitud de transferencia inactiva al UTRAN, en el que el mensaje de solicitud puede ser un mensaje de solicitud de actualización del área de ruta o un mensaje de solicitud de adición del área de ruta;

etapa S302: tras la recepción del mensaje de solicitud de transferencia inactiva al UTRAN enviada desde el UE,

el SGSN objetivo envía a una MME de origen un mensaje de solicitud, en el que el tipo de mensaje de solicitud se corresponde al de un mensaje de solicitud de transferencia, es decir, puede ser un mensaje de solicitud de contexto o un mensaje de solicitud de identificación;

etapa S303: tras la recepción del mensaje de solicitud desde el SGSN objetivo, la MME de origen genera una CK y una IK basándose en una K_{ASME};

etapa S304: la MME de origen responde en correspondencia con un mensaje de respuesta de contexto o un mensaje de respuesta de identificación, y envía la CK, la IK y un KSI_{ASME} al SGSN objetivo;

etapa S305: tras la recepción de la CK, la IK y un KSI_{ASME} desde la MME de origen, el SGSN objetivo asigna el valor del KSI_{ASME} a un KSI, es decir, KSI = KSI_{ASME}, y almacena el KSI junto con la CK y la IK;

etapa S306: el SGSN objetivo envía al UE un mensaje de aceptación de transferencia inactiva al UTRAN (en correspondencia, un mensaje de aceptación de actualización del área de ruta o un mensaje de aceptación de adición del área de ruta) para notificar al UE el éxito del mapeado del identificador de claves del lado de red;

etapa S307: el UE asigna el valor del KSI_{ASME} a un KSI, es decir, KSI = KSI_{ASME}, y almacena el KSI junto con la CK y la IK que se generaron a partir de la K_{ASME}; y

etapa S308: el UE envía un mensaje de finalización de actualización del área de ruta o un mensaje de finalización de adición del área de ruta correspondiente al SGSN objetivo.

La Fig. 4 es el Ejemplo de Aplicación Dos del método de la presente invención, que ilustra un diagrama de flujo del método para la generación de un identificador de claves cuando un UE se transfiere en un estado inactivo desde un EUTRAN a un UTRAN, lo que incluye las siguientes etapas:

etapa S401: un UE decide transferirse a un UTRAN en un estado inactivo, asigna un valor de un KSI_{ASME} a un KSI, es decir, KSI = KSI_{ASME}, y almacena el KSI junto con una CK y una IK que se generaron a partir de una K_{ASME};

etapa S402: el UE envía a un SGSN objetivo un mensaje de solicitud de transferencia inactiva al UTRAN, en el que el mensaje de solicitud puede ser un mensaje de solicitud de actualización del área de ruta o un mensaje de solicitud de adición del área de ruta;

etapa S403: tras la recepción del mensaje de solicitud de transferencia inactiva al UTRAN enviada desde el UE, el SGSN objetivo envía a una MME de origen un mensaje de solicitud, en el que el tipo de mensaje de solicitud se corresponde al de un mensaje de solicitud de transferencia, es decir, puede ser un mensaje de solicitud de contexto o un mensaje de solicitud de identificación;

etapa S404: tras la recepción del mensaje de solicitud desde el SGSN, la MME de origen genera una CK y una IK basándose en la K_{ASME};

etapa S405: la MME responde en correspondencia con un mensaje de respuesta de contexto o un mensaje de respuesta de identificación, y envía la CK, la IK y el KSI_{ASME} al SGSN;

etapa S406: tras la recepción del KSI_{ASME}, de la CK y la IK desde la MME de origen, el SGSN objetivo asigna el valor del KSI_{ASME} a un KSI, es decir, KSI = KSI_{ASME}, y almacena el KSI junto con la CK y la IK;

etapa S407: el SGSN objetivo envía al UE un mensaje de aceptación de transferencia inactiva al UTRAN (en correspondencia, un mensaje de aceptación de actualización del área de ruta o un mensaje de aceptación de adición del área de ruta) para notificar al UE el éxito del mapeado del identificador de claves del lado de red; y

etapa S408: el UE envía un mensaje de finalización de actualización del área de ruta o un mensaje de finalización de adición del área de ruta correspondiente al SGSN objetivo.

La Fig. 5 es el Ejemplo de Aplicación Tres del método de la presente invención, que ilustra un diagrama de flujo del método para la generación de un identificador de claves cuando un UE conmuta en un estado inactivo desde un EUTRAN a un UTRAN, lo que incluye las siguientes etapas:

etapa S501: un eNB de origen decide iniciar una conmutación basándose o bien en un informe de consulta enviado desde un UE al eNB o bien por otras razones;

etapa S502: el eNB de origen envía a una MME de origen un mensaje de solicitud de conmutación;

etapa S503: la MME de origen genera una IK y una CK basándose en una K_{ASME};

etapa S504: la MME de origen envía a un SGSN objetivo una solicitud de envío y redirección, y transmite un KSI_{ASME} junto con la IK y la CK al SGSN objetivo;

etapa S505: el SGSN objetivo asigna el valor del KSI_{ASME} a un KSI, es decir, KSI = KSI_{ASME}, y almacena el KSI junto con la IK y la CK;

etapa S506: el SGSN objetivo envía a la MME de origen un mensaje de respuesta de envío y redirección para notificar a la MME de origen que la red de servicio objetivo se ha preparado para conmutación;

etapa S507: la MME de origen envía al eNB una orden de conmutación;

etapa S508: el eNB de origen envía al UE una orden de conmutación EUTRAN;

etapa S509: el UE asigna el valor del KSI_{ASME} a un KSI, es decir, KSI = KSI_{ASME}, genera una IK y una CK basándose en la K_{ASME}, y almacena el KSI junto con la CK y la IK; y

etapa S510: el UE envía un mensaje de éxito de conmutación a un RNC objetivo para notificarle el éxito del mapeado del KSI de red.

La Fig. 6 es el Ejemplo de Aplicación Cuatro del método de la presente invención, que ilustra un diagrama de flujo del método para la generación de un identificador de claves cuando un UE se transfiere en un estado inactivo desde un EUTRAN a un GERAN, lo que incluye las siguientes etapas:

etapa S601: un UE decide transferirse a un GERAN en un estado inactivo, y envía a un SGSN objetivo un mensaje de solicitud de transferencia inactiva al GERAN, en el que el mensaje de solicitud puede ser un mensaje de solicitud de actualización del área de ruta o un mensaje de solicitud de adición del área de ruta;

etapa S602: tras la recepción del mensaje de solicitud de transferencia inactiva al GERAN enviada desde el UE, el SGSN objetivo envía a una MME de origen un mensaje de solicitud, en el que el tipo de mensaje de solicitud se corresponde al de un mensaje de solicitud de transferencia recibido, es decir, puede ser un mensaje de solicitud de contexto o un mensaje de solicitud de identificación;

etapa S603: tras la recepción del mensaje de solicitud desde el SGSN objetivo, la MME de origen genera una CK y una IK basándose en una K_{ASME};

etapa S604: la MME de origen responde en correspondencia con un mensaje de respuesta de contexto o un mensaje de respuesta de identificación, y envía la CK, la IK y un KSI_{ASME} al SGSN objetivo;

etapa S605: tras la recepción del KSI_{ASME}, la CK y la IK desde la MME de origen, el SGSN objetivo asigna el valor del KSI_{ASME} a un CKSN, es decir, CKSN = KSI_{ASME}, y almacena el CKSN junto con una Kc generada a partir de la CK y la IK;

etapa S606: el SGSN objetivo envía al UE un mensaje de aceptación de transferencia inactiva correspondiente al UTRAN (en correspondencia, un mensaje de aceptación de actualización del área de ruta o un mensaje de aceptación de adición del área de ruta) para notificar al UE el éxito del mapeado del identificador de claves del lado de red;

etapa S607: el UE asigna el valor del KSI_{ASME} a un CKSN, es decir, CKSN = KSI_{ASME}, y almacena el CKSN junto con una Kc generada a partir de la K_{ASME}; y

etapa S608: el UE envía un mensaje de finalización de actualización del área de ruta o un mensaje de finalización de adición del área de ruta correspondiente al SGSN objetivo.

La Fig. 7 es el Ejemplo de Aplicación Cinco del método de la presente invención, que ilustra un diagrama de flujo del método para la generación de un identificador de claves cuando un UE se transfiere en un estado inactivo desde un EUTRAN a un GERAN, lo que incluye las siguientes etapas:

etapa S701: un UE decide transferirse a un GERAN en un estado inactivo, asigna un valor de un KSI_{ASME} a un CKSN, es decir, CKSN = KSI_{ASME}, y almacena el CKSN junto con una Kc generada a partir de una K_{ASME};

etapa S702: el UE envía a un SGSN objetivo un mensaje de solicitud de transferencia inactiva al GERAN, en el que el mensaje de solicitud puede ser un mensaje de solicitud de actualización del área de ruta o un mensaje de solicitud de adición del área de ruta;

etapa S703: tras la recepción del mensaje de solicitud de transferencia inactiva al GERAN enviada desde el UE, el SGSN objetivo envía a una MME de origen un mensaje de solicitud, en el que el tipo de mensaje de solicitud

se corresponde al de un mensaje de solicitud de transferencia, es decir, puede ser un mensaje de solicitud de contexto o un mensaje de solicitud de identificación;

etapa S704: tras la recepción del mensaje de solicitud desde el SGSN, la MME de origen genera una CK y una IK basándose en la K_{ASME};

etapa S705: la MME de origen responde en correspondencia con un mensaje de respuesta de contexto o un mensaje de respuesta de identificación, y envía la CK, la IK y el KSI_{ASME} al SGSN objetivo;

etapa S706: tras la recepción del KSI_{ASME}, de la CK y la IK desde la MME de origen, el SGSN objetivo asigna el valor del KSI_{ASME} a un CKSN, es decir, CKSN = KSI_{ASME}, y almacena el CKSN junto con una Kc generada a partir de la CK y la IK;

etapa S707: el SGSN objetivo envía al UE un mensaje de aceptación de transferencia inactiva al GERAN (en correspondencia, un mensaje de aceptación de actualización del área de ruta o un mensaje de aceptación de adición del área de ruta) para notificar al UE el éxito del mapeado del identificador de claves del lado de red; y

etapa S708: el UE envía un mensaje de finalización de actualización del área de ruta o un mensaje de finalización de adición del área de ruta correspondiente al SGSN objetivo.

La Fig. 8 es el Ejemplo de Aplicación Seis del método de la presente invención, que ilustra un diagrama de flujo del método para la generación de un identificador de claves cuando un UE conmuta en un estado inactivo desde un EUTRAN a un GERAN, lo que incluye las siguientes etapas:

etapa S801: un eNB de origen decide iniciar una conmutación basándose o bien en un informe de consulta enviado desde un UE al eNB o bien por otras razones;

etapa S802: el eNB de origen envía a una MME de origen un mensaje de solicitud de conmutación;

etapa S803: la MME de origen genera una IK y una CK basándose en una K_{ASME};

etapa S804: la MME de origen envía a un SGSN objetivo una solicitud de envío y redirección, y transmite un KSI_{ASME} junto con la IK y la CK al SGSN objetivo;

etapa S805: el SGSN objetivo asigna el valor del KSI_{ASME} a un CKSN, es decir, CKSN = KSI_{ASME}, y almacena el CKSN junto con una Kc generada a partir de la IK y la CK;

etapa S806: el SGSN objetivo envía a la MME de origen un mensaje de respuesta de envío y redirección para notificar a la MME de origen que la red de servicio objetivo se ha preparado para conmutación;

etapa S807: la MME de origen envía al eNB una orden de conmutación;

etapa S808: el eNB de origen envía al UE una orden de conmutación EUTRAN;

etapa S809: el UE asigna el valor del KSI_{ASME} a un CKSN, es decir, CKSN = KSI_{ASME}, genera una Kc basándose en la K_{ASME}, y almacena el CKSN junto con la Kc; y

etapa S810: el UE envía un mensaje de éxito de conmutación a un RNC objetivo para notificarle el éxito del mapeado del CKSN de red.

En los seis ejemplos de aplicación anteriormente mencionados, el UE y el SGSN pueden asignar también la suma del KSI_{ASME} y una constante al identificador de identidad de claves del sistema objetivo; la constante se acuerda por el UE y la red, en el que la suma del KSI_{ASME} y la constante no pueden ser 111, en caso contrario, puede alterarse en consonancia con el acuerdo entre el UE y el SGSN, por ejemplo mediante su sustitución con un valor siguiente 000 u otro valor.

Obviamente, los expertos en la materia deberían entender que varios módulos o etapas de la presente invención pueden implementarse mediante dispositivos de cálculo universal, pueden estar integrados en un único dispositivo de cálculo, o pueden distribuirse en una red que consiste en múltiples dispositivos de cálculo; alternativamente, pueden implementarse mediante códigos ejecutables por dispositivos de cálculo. Por lo tanto, pueden almacenarse en un dispositivo de almacenamiento para ser ejecutados mediante un dispositivo de cálculo, o pueden realizarse en varios módulos de circuitos integrados, o múltiples módulos o etapas de los mismos pueden realizarse en un único módulo de circuito integrado. Por ello, la presente invención no está limitada a ninguna combinación específica de hardware y software.

Los ejemplos anteriores son solo realizaciones preferidas de la presente invención, y no constituyen limitación a la

presente invención. Para los expertos en la materia, la presente invención puede tener una variedad de modificaciones y cambios.

REIVINDICACIONES

1. Un método para la generación de un identificador de identidad de claves cuando un equipo de usuario, UE, se transfiere, que incluye las siguientes etapas:

cuando un UE se transfiere desde una red de acceso por radio terrestre, EUTRAN, de un sistema universal de telecomunicaciones móviles evolucionado, UMTS, a un sistema objetivo, una entidad de gestión de la movilidad, MME, del EUTRAN, enviar un identificador de identidad de una clave de la entidad de la gestión de seguridad de acceso, K_{ASME}, KSI_{ASME}, a un nodo de soporte, SGSN, del servicio general de paquetes vía radio, GPRS, en servicio, del sistema objetivo (A1, B1), y mapear tanto el SGSN como el UE el KSI_{ASME} en un identificador de identidad de claves del sistema objetivo; en el que el mapeado del KSI_{ASME} en un identificador de conjunto de claves, KSI, cuando el sistema objetivo es una red de acceso por radio terrestre UMTS, UTRAN (A2, A3) y el mapeado del KSI_{ASME} en un número de secuencia de clave de cifrado, CKSN, cuando el sistema objetivo es una red de acceso por radio GERAN (B2, B3), GPRS/tasas de datos mejoradas para la evolución de GSM, EDGE, en el que, la MME del EUTRAN que envía el KSI_{ASME}, al SGSN del sistema objetivo, comprende:

generar la MME una clave de integridad, IK, y una clave de cifrado, CK, basándose en la K_{ASME} y enviar el KSI_{ASME} junto con la IK y la CK que se generaron a partir de la K_{ASME} al SGSN (A1, B1).

2. El método de generación de acuerdo con la reivindicación 1, en el que el mapeado incluye las siguientes etapas: asignar directamente el KSI_{ASME} al identificador de identidad de claves del sistema objetivo, o asignar directamente la suma del KSI_{ASME} y una constante que es acordada por el UE y la red al identificador de identidad de claves del sistema objetivo.

3. El método de generación de acuerdo con cualquiera de las reivindicaciones 1 a 2, en el que las etapas específicas son como sigue cuando el UE se transfiere en un estado inactivo desde el EUTRAN al UTRAN:

A1: después de recibir un mensaje de solicitud de contexto o un mensaje de solicitud de identificación, la MME genera la IK y la CK basándose en la K_{ASME} y envía el KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN a través de un mensaje de respuesta de contexto o un mensaje de respuesta de identificación;
A2: después de la recepción del KSI_{ASME}, la IK y la CK desde la MME, el SGSN mapea el KSI_{ASME} en el KSI, y almacena el KSI, la IK y la CK; y el SGSN envía un mensaje de indicación de finalización del mapeado del KSI al UE; y
A3: el UE mapea el KSI_{ASME} en el KSI, y almacena el KSI junto con la IK y la CK que se generan a partir de la K_{ASME}.

4. El método de generación de acuerdo con la reivindicación 3, en el que la etapa A3 tiene lugar en cualquier etapa después de que el UE decida transferirse al UTRAN en un estado inactivo y antes de que el UE envíe un mensaje de finalización de actualización del área de ruta o mensaje de finalización de adición del área de ruta correspondientes al SGSN.

5. El método de generación de acuerdo con cualquiera de las reivindicaciones 1 a 2, en el que las etapas específicas son como sigue cuando el UE conmuta desde el EUTRAN al UTRAN:

a1: después de la recepción de un mensaje de solicitud de conmutación, la MME genera la IK y la CK basándose en la K_{ASME}, y envía el KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN a través de un mensaje de solicitud de envío y redirección;
a2: tras la recepción del KSI_{ASME}, junto con la IK y la CK desde la MME, el SGSN mapea el KSI_{ASME} en el KSI, y almacena el KSI, la IK y la CK juntas; el SGSN envía un mensaje de respuesta de envío y redirección de indicación de finalización del mapeado del KSI a la MME; y la MME envía una orden de conmutación para dar instrucciones al UE para conmutar; y
a3: después de la recepción de la orden de conmutación desde la red, el UE mapea el KSI_{ASME} en el KSI, y almacena el KSI junto con la IK y la CK que se generan a partir de la K_{ASME}.

6. El método de generación de acuerdo con cualquiera de las reivindicaciones 1 a 2, en el que las etapas específicas son como sigue cuando el UE se transfiere en un estado inactivo desde el EUTRAN al GERAN:

B1: después de recibir un mensaje de solicitud de contexto o un mensaje de solicitud de identificación, la MME genera la IK y la CK basándose en la K_{ASME} y envía el KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN a través de un mensaje de respuesta de contexto o un mensaje de respuesta de identificación;
B2: después de la recepción del KSI_{ASME}, la IK y la CK desde la MME, el SGSN genera una clave de cifrado, Kc, del GERAN basándose en la IK y la CK, mapea el KSI_{ASME} en el CKSN del GERAN, y almacena el CKSN del GERAN junto con la Kc del GERAN; y el SGSN envía al UE un mensaje de indicación de finalización del mapeado del CKSN del GERAN; y
B3: el UE mapea el KSI_{ASME} en el CKSN del GERAN, y almacena el CKSN del GERAN junto con la Kc del GERAN generada a partir de la K_{ASME}.

7. El método de generación de acuerdo con la reivindicación 6, en el que la etapa B3 tiene lugar en cualquier etapa después de que el UE decida transferirse al GERAN en un estado inactivo y antes de que el UE envíe un mensaje de conmutación a la red.

8. El método de generación de acuerdo con cualquiera de las reivindicaciones 1 a 2, en el que las etapas específicas son como sigue cuando el UE conmuta desde el EUTRAN al GERAN:

b1: tras la recepción de un mensaje de solicitud de conmutación, la MME genera la IK y la CK basándose en la K_{ASME}, y envía el KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN a través de un mensaje de solicitud de envío y redirección;
b2: tras la recepción del KSI_{ASME} junto con la IK y la CK desde la MME, el SGSN genera una Kc del GERAN basándose en la IK y la CK, asigna el valor del KSI_{ASME} al CKSN del GERAN, y almacena el CKSN del GERAN junto con la Kc del GERAN; el SGSN envía un mensaje de indicación de finalización del mapeado del CKSN del GERAN a la MME; y la MME envía una orden de conmutación para dar instrucciones al UE para conmutar; y
b3: después de la recepción de la orden de conmutación desde la red, el UE mapea el KSI_{ASME} en el CKSN del GERAN, y almacena el CKSN del GERAN junto con la Kc del GERAN generada a partir de la K_{ASME}.

9. Un sistema para la generación de un identificador de identidad de claves cuando un UE se transfiere, que incluye un equipo de usuario, UE, una entidad de gestión de la movilidad, MME, y un nodo de soporte, SGSN, del servicio general de paquetes vía radio, GPRS, en servicio;

estando adaptada la MME para el envío de un identificador de identidad de una clave de entidad de gestión de seguridad de acceso, K_{ASME}, KSI_{ASME}, al SGSN cuando el UE se transfiere desde una red de acceso por radio terrestre, EUTRAN, del sistema universal de telecomunicaciones móviles evolucionado, UMTS, a un sistema objetivo (A1, B1); y
estando adaptados tanto el SGSN como el UE para mapeado del KSI_{ASME} en un identificador de identidad de claves del sistema objetivo;
en el que el mapeado del KSI_{ASME} en un identificador del conjunto de claves, KSI, cuando el sistema objetivo es una red de acceso por radio terrestre UMTS, UTRAN (A2, A3) y el mapeado del KSI_{ASME} en un número de secuencia de clave de cifrado, CKSN, cuando el sistema objetivo es una red de acceso por radio GERAN (B2, B3), GPRS/tasas de datos mejoradas para evolución de GSM, EDGE,;
en el que, estando adaptada la MME para la generación de una clave de integridad, IK, y una clave de cifrado, CK, basándose en la K_{ASME} y el envío del KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN (A1, B1).

10. El sistema de generación de acuerdo con la reivindicación 9, en el que el SGSN/UE está adaptado para la realización del mapeado asignando directamente el KSI_{ASME} al identificador de identidad de claves del sistema objetivo, o asignar directamente la suma del KSI_{ASME} y una constante, que se acuerda por el UE y la red al identificador de identidad de claves del sistema objetivo.

11. El sistema de generación de acuerdo con la reivindicación 9, en el que el UE y el SGSN están adaptados adicionalmente para borrar una clave almacenada antes de la transferencia cuando el UE y el SGSN han acordado acerca de una clave antes de la transferencia y el identificador de identidad de claves de un sistema objetivo es el mismo que el identificador de identidad de claves del sistema objetivo convertido desde el KSI_{ASME} durante la transferencia.

12. El sistema de generación de acuerdo con cualquiera de las reivindicaciones 9 a 11, en el que

el UE comprende una unidad de interacción del mensaje, una unidad de mapeado del identificador de claves y una unidad de almacenamiento de claves e identificador de claves;
la unidad de interacción del mensaje está adaptada para la recepción de un mensaje desde un lado de red;
la unidad de mapeado del identificador de claves está adaptada para mapeado del KSI_{ASME} en un identificador de identidad de claves de un sistema objetivo cuando la unidad de interacción del mensaje recibe una orden de conmutación, un mensaje de aceptación de actualización del área de ruta o un mensaje de aceptación de adición del área de ruta; y
la unidad de almacenamiento de claves e identificador de claves está adaptada para almacenar una clave de un sistema objetivo y un identificador de identidad de claves del sistema objetivo conjuntamente;
la MME comprende una unidad de recepción del mensaje de solicitud y una unidad de procesamiento del parámetro de seguridad;
la unidad de recepción del mensaje de solicitud está adaptada para la recepción de mensajes de solicitud de transferencia desde otras entidades de red e instruir a la unidad de procesamiento del parámetro de seguridad para procesar estos mensajes; y
la unidad de procesamiento del parámetro de seguridad está adaptada para generar la CK y la IK a partir de la K_{ASME} y el envío del KSI_{ASME} junto con la IK y la CK que se han generado a partir de la K_{ASME} al SGSN después de la recepción de la instrucción desde la unidad de recepción del mensaje de solicitud;

el SGSN comprende una unidad de procesamiento del parámetro de seguridad, una unidad de interacción del mensaje, una unidad de mapeado del identificador de claves, y una unidad de generación de claves;
la unidad de recepción del parámetro de seguridad está adaptada para la recepción de las claves y del KSI_{ASME} desde la MME, el envío del KSI_{ASME} a la unidad de mapeado del identificador de claves, adquirir la clave del sistema objetivo basándose en las claves enviadas por la MME y enviarlas a la unidad de almacenamiento de claves e identificador de claves;
la unidad de mapeado del identificador de claves está adaptada para mapeado del KSI_{ASME} en un identificador de identidad de claves del sistema objetivo tras la recepción del KSI_{ASME};
la unidad de almacenamiento de claves e identificador de claves está adaptada para almacenar tanto la clave del sistema objetivo enviada por la unidad de recepción del parámetro de seguridad como el identificador de identidad de claves del sistema objetivo enviado por la unidad de mapeado del identificador de claves, y para notificar a la unidad de interacción del mensaje de la finalización del mapeado después del almacenamiento; y
la unidad de interacción del mensaje está adaptada para el envío de una notificación de éxito del mapeado del identificador de claves en el lado de red después de la recepción del mensaje de finalización de mapeado.

13. El sistema de generación de acuerdo con la reivindicación 12, en el que

la unidad de recepción del parámetro de seguridad en el SGSN está adaptada para la adquisición de la clave del sistema objetivo basándose en las claves enviadas por la MME y está adaptada para enviarlas a la unidad de almacenamiento de claves e identificador de claves, en el que
cuando el sistema objetivo es un UTRAN, las claves enviadas por la MME se envían a la unidad de almacenamiento de claves e identificador de claves; y cuando el sistema objetivo es un GERAN, las claves enviadas por la MME se usan para generar una Kc del GERAN que se envía a la unidad de almacenamiento de claves e identificador de claves.

14. El sistema de generación de acuerdo con la reivindicación 12, en el que la unidad de mapeado del identificador de claves en el UE está adaptada adicionalmente para mapeado del KSI_{ASME} en el identificador de identidad de claves del sistema objetivo cuando el UE decide transferirse en un estado inactivo.

15. El sistema de generación de acuerdo con la reivindicación 12, en el que

la unidad de interacción del mensaje en el UE está adaptada adicionalmente para el envío de un mensaje de solicitud de actualización del área de ruta o un mensaje de solicitud de adición del área de ruta al SGSN cuando el UE decide transferirse en un estado inactivo;
la unidad de interacción del mensaje en el SGSN está adaptada adicionalmente para envío de un mensaje de solicitud de contexto o mensaje de solicitud de identificación correspondiente a la MME tras la recepción del mensaje de solicitud de actualización del área de ruta o del mensaje de solicitud de adición del área de ruta;
la unidad de recepción del mensaje de solicitud en la MME está adaptada para el envío de una primera instrucción de procesamiento a la unidad de procesamiento del parámetro de seguridad si el mensaje de solicitud de transferencia es un mensaje de solicitud de contexto o un mensaje de solicitud de identificación, y la unidad de recepción del mensaje de solicitud está adaptada para el envío de una segunda instrucción de procesamiento a la unidad de procesamiento del parámetro de seguridad si el mensaje de solicitud de transferencia es un mensaje de solicitud de conmutación; y
la unidad de procesamiento del parámetro de seguridad en la MME está adaptada para el envío del KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN a través de un mensaje de respuesta de contexto o mensaje de respuesta de identificación después de la recepción de la primera instrucción de procesamiento, y la unidad de procesamiento del parámetro de seguridad está adaptada para el envío del KSI_{ASME} junto con la IK y la CK que se generan a partir de la K_{ASME} al SGSN a través de un mensaje de solicitud de envío y redirección después de la recepción de la segunda instrucción de procesamiento.

16. El sistema de generación de acuerdo con la reivindicación 15, en el que la unidad de interacción del mensaje en el SGSN está adaptada para el envío de una notificación de éxito de mapeado del identificador de claves del lado de red, en el que si el mensaje de envío de la clave y del identificador de claves por la MME es un mensaje de respuesta de contexto o un mensaje de respuesta de identificación, entonces la unidad de interacción del mensaje está adaptada para el envío de un mensaje de aceptación de actualización del área de ruta o un mensaje de aceptación de adición del área de ruta al UE para indicar el éxito del mapeado del identificador de claves del lado de red; y si el mensaje de envío de la clave y el identificador de claves por la MME es un mensaje de solicitud de envío y redirección, entonces la unidad de interacción del mensaje está adaptada para el envío de un mensaje de respuesta de envío y redirección a la MME para indicar el éxito del mapeado del identificador de claves del lado de red.

Fig. 1

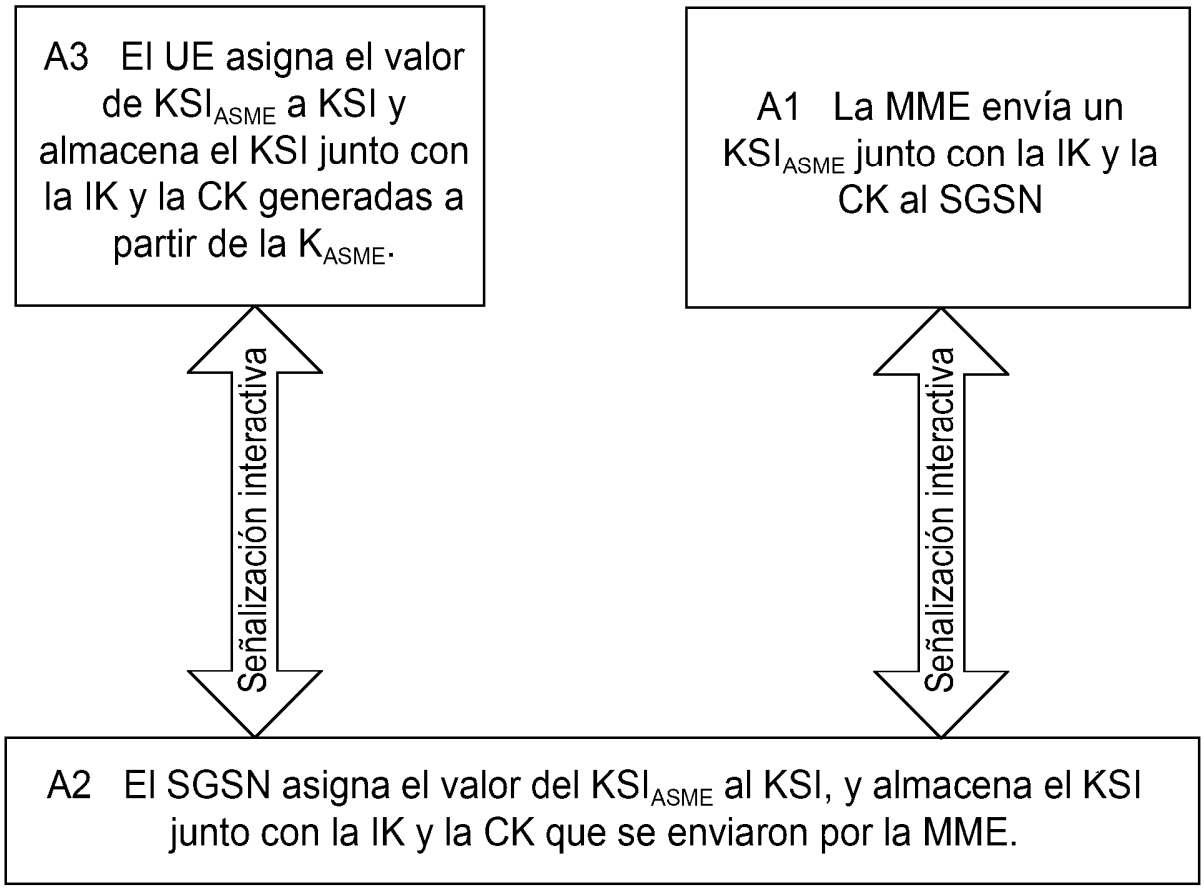

A3 El UE asigna el valor de KSI_{ASME} a KSI y almacena el KSI junto con la IK y la CK generadas a partir de la K_{ASME}.
A1 La MME envía un KSI_{ASME} junto con la IK y la CK al SGSN
Señalización interactiva
Señalización interactiva
A2 El SGSN asigna el valor del KSI_{ASME} al KSI, y almacena el KSI junto con la IK y la CK que se enviaron por la MME.

Fig. 2

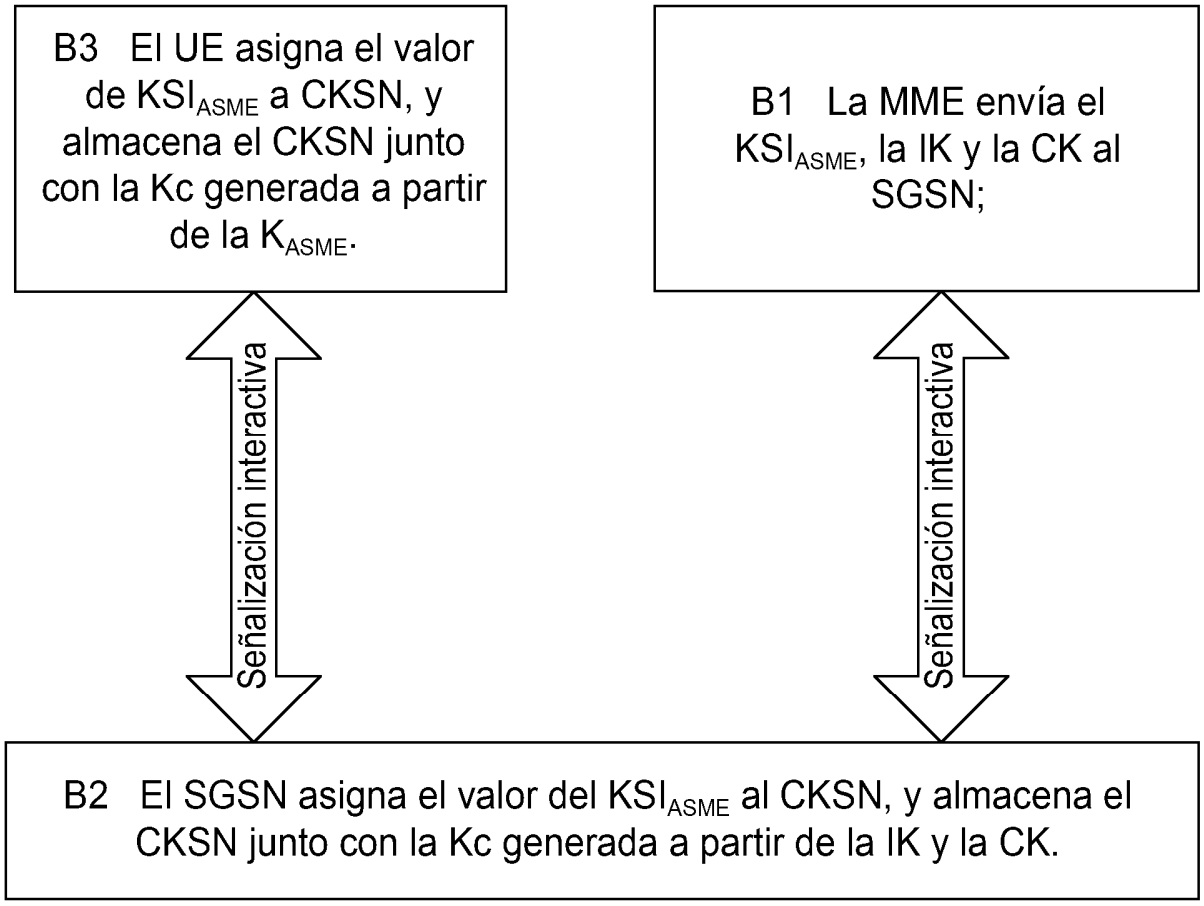

B3 El UE asigna el valor de KSI$_{ASME}$ a CKSN, y almacena el CKSN junto con la Kc generada a partir de la K$_{ASME}$.
B1 La MME envía el KSI$_{ASME}$, la IK y la CK al SGSN;
Señalización interactiva
Señalización interactiva
B2 El SGSN asigna el valor del KSI$_{ASME}$ al CKSN, y almacena el CKSN junto con la Kc generada a partir de la IK y la CK.

Fig. 3

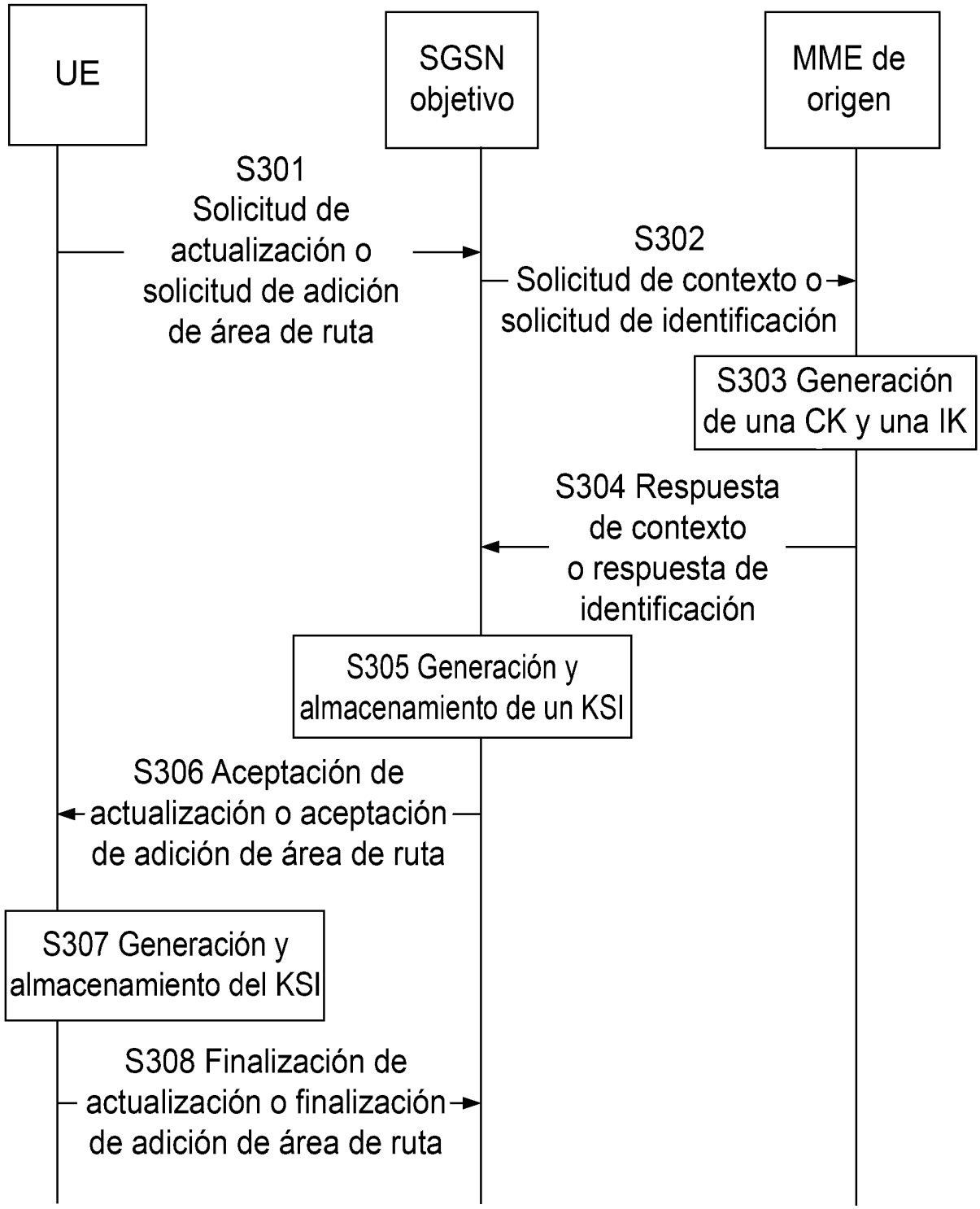

UE
SGSN objetivo
MME de origen
S301 Solicitud de actualización o solicitud de adición de área de ruta
S302 Solicitud de contexto o solicitud de identificación
S303 Generación de una CK y una IK
S304 Respuesta de contexto o respuesta de identificación
S305 Generación y almacenamiento de un KSI
S306 Aceptación de actualización o aceptación de adición de área de ruta
S307 Generación y almacenamiento del KSI
S308 Finalización de actualización o finalización de adición de área de ruta

Fig. 4

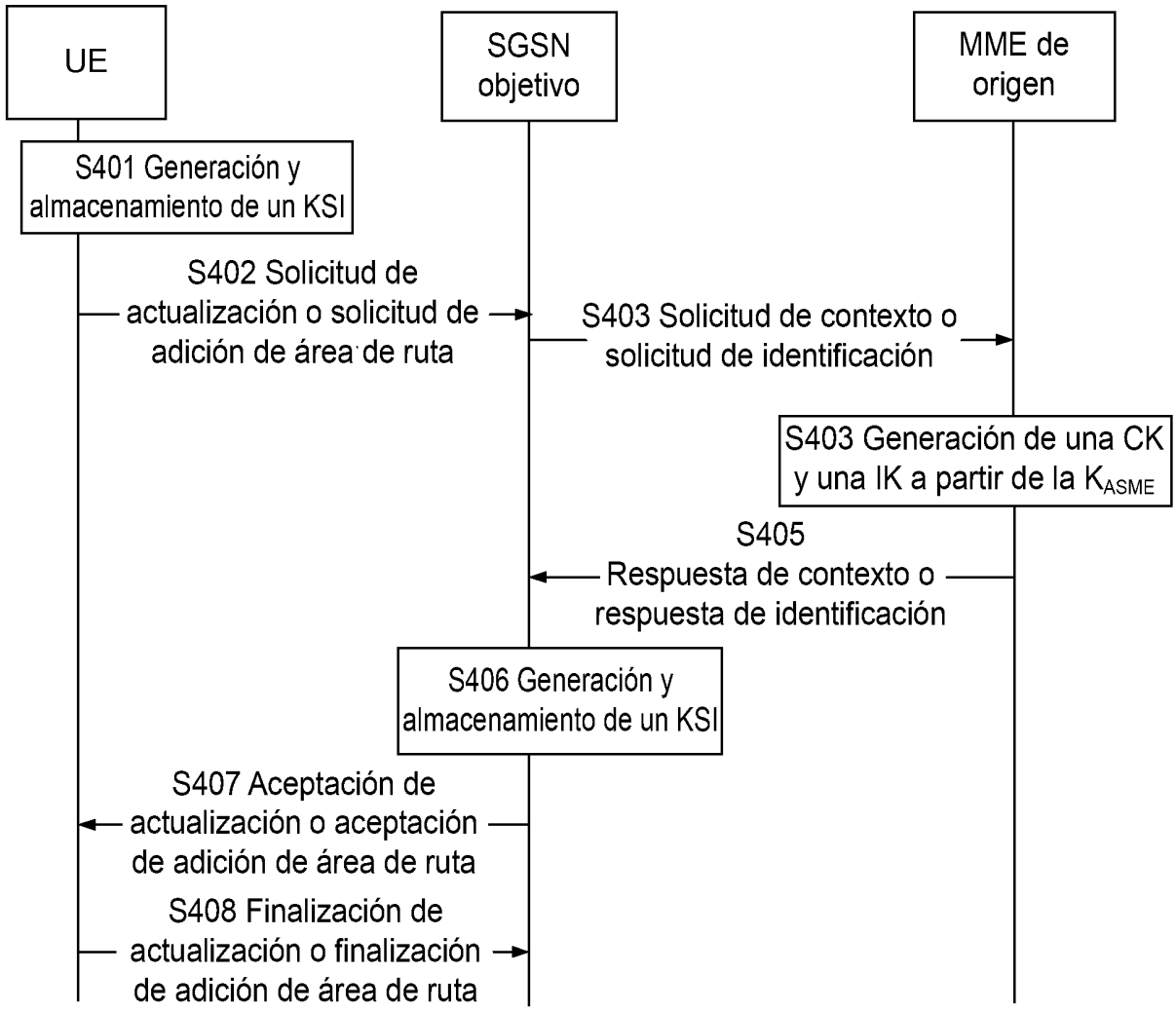

UE
SGSN objetivo
MME de origen
S401 Generación y almacenamiento de un KSI
S402 Solicitud de actualización o solicitud de adición de área de ruta
S403 Solicitud de contexto o solicitud de identificación
S403 Generación de una CK y una IK a partir de la K_{ASME}
S405 Respuesta de contexto o respuesta de identificación
S406 Generación y almacenamiento de un KSI
S407 Aceptación de actualización o aceptación de adición de área de ruta
S408 Finalización de actualización o finalización de adición de área de ruta

Fig. 5

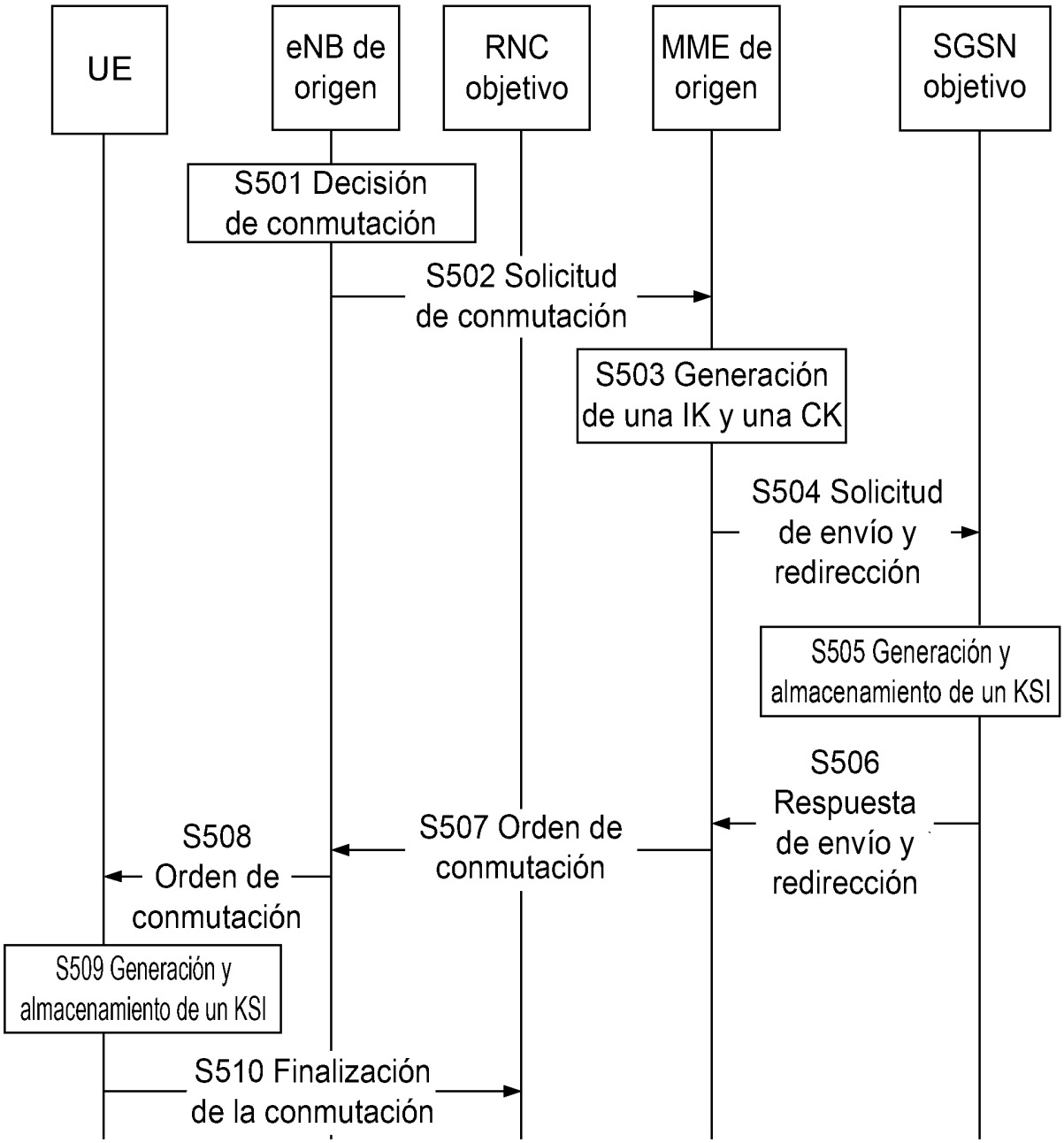

UE
eNB de origen
RNC objetivo
MME de origen
SGSN objetivo
S501 Decisión de conmutación
S502 Solicitud de conmutación
S503 Generación de una IK y una CK
S504 Solicitud de envío y redirección
S505 Generación y almacenamiento de un KSI
S506 Respuesta de envío y redirección
S507 Orden de conmutación
S508 Orden de conmutación
S509 Generación y almacenamiento de un KSI
S510 Finalización de la conmutación

Fig. 6

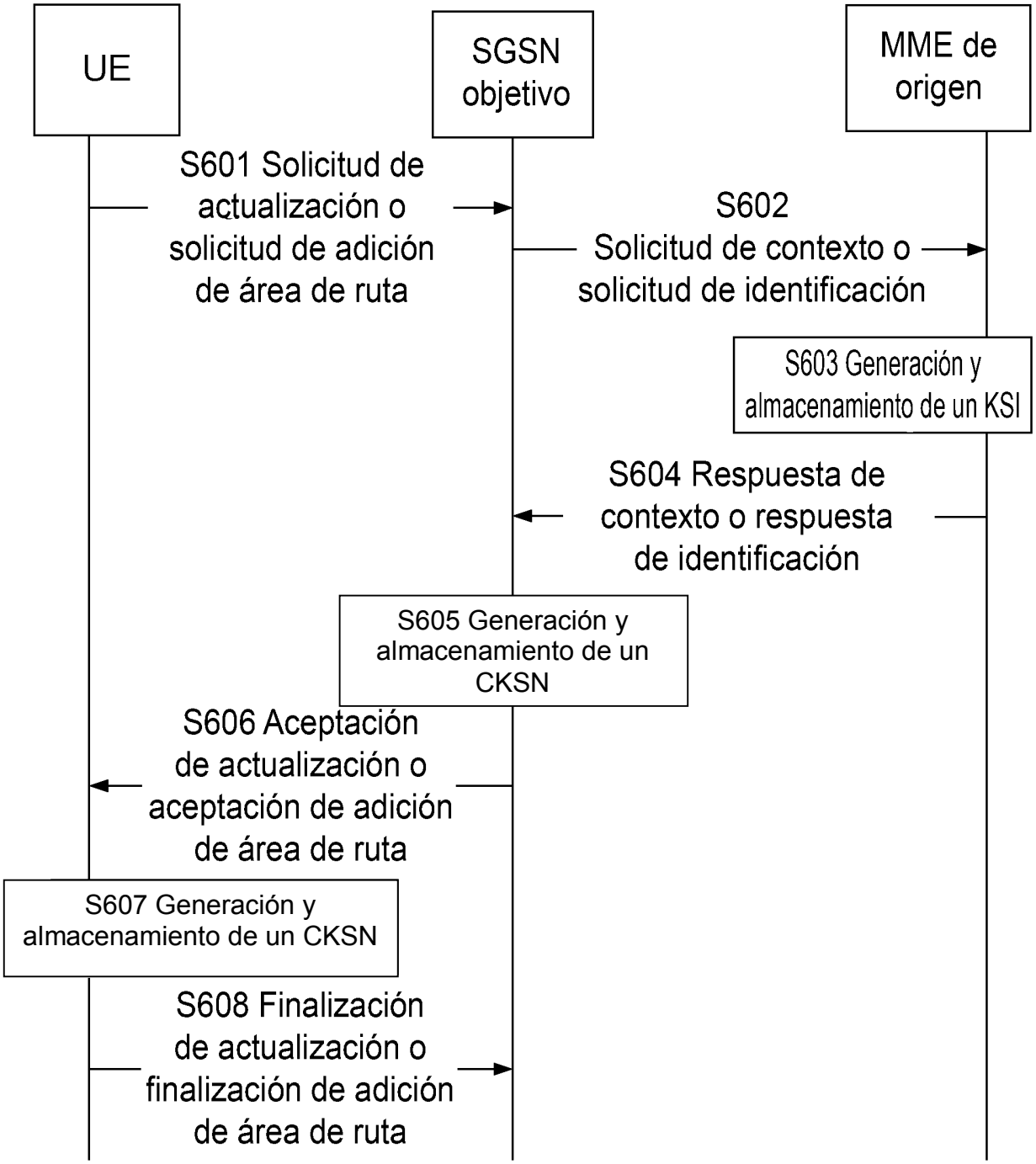

UE
SGSN objetivo
MME de origen
S601 Solicitud de actualización o solicitud de adición de área de ruta
S602 Solicitud de contexto o solicitud de identificación
S603 Generación y almacenamiento de un KSI
S604 Respuesta de contexto o respuesta de identificación
S605 Generación y almacenamiento de un CKSN
S606 Aceptación de actualización o aceptación de adición de área de ruta
S607 Generación y almacenamiento de un CKSN
S608 Finalización de actualización o finalización de adición de área de ruta

Fig. 7

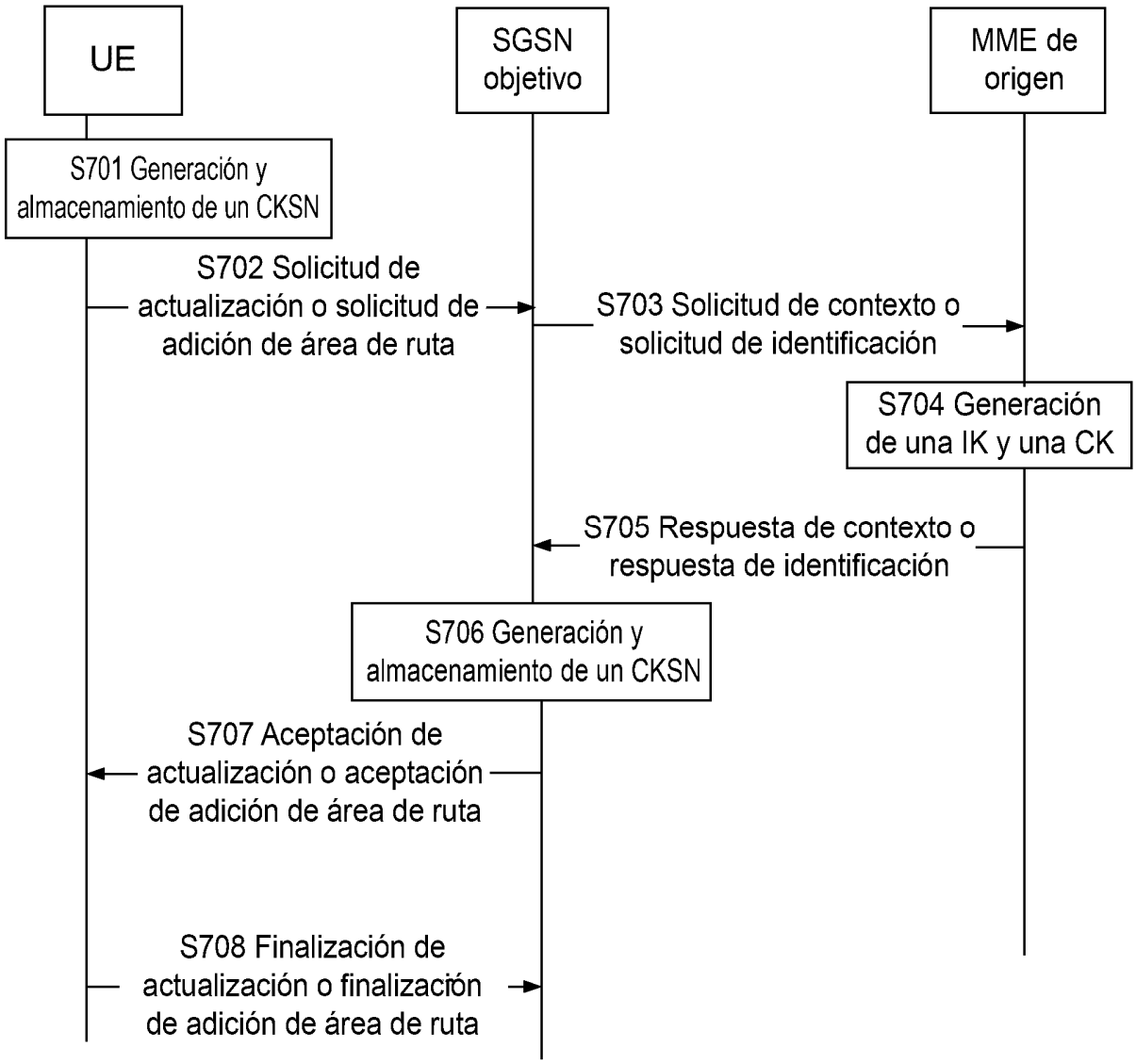
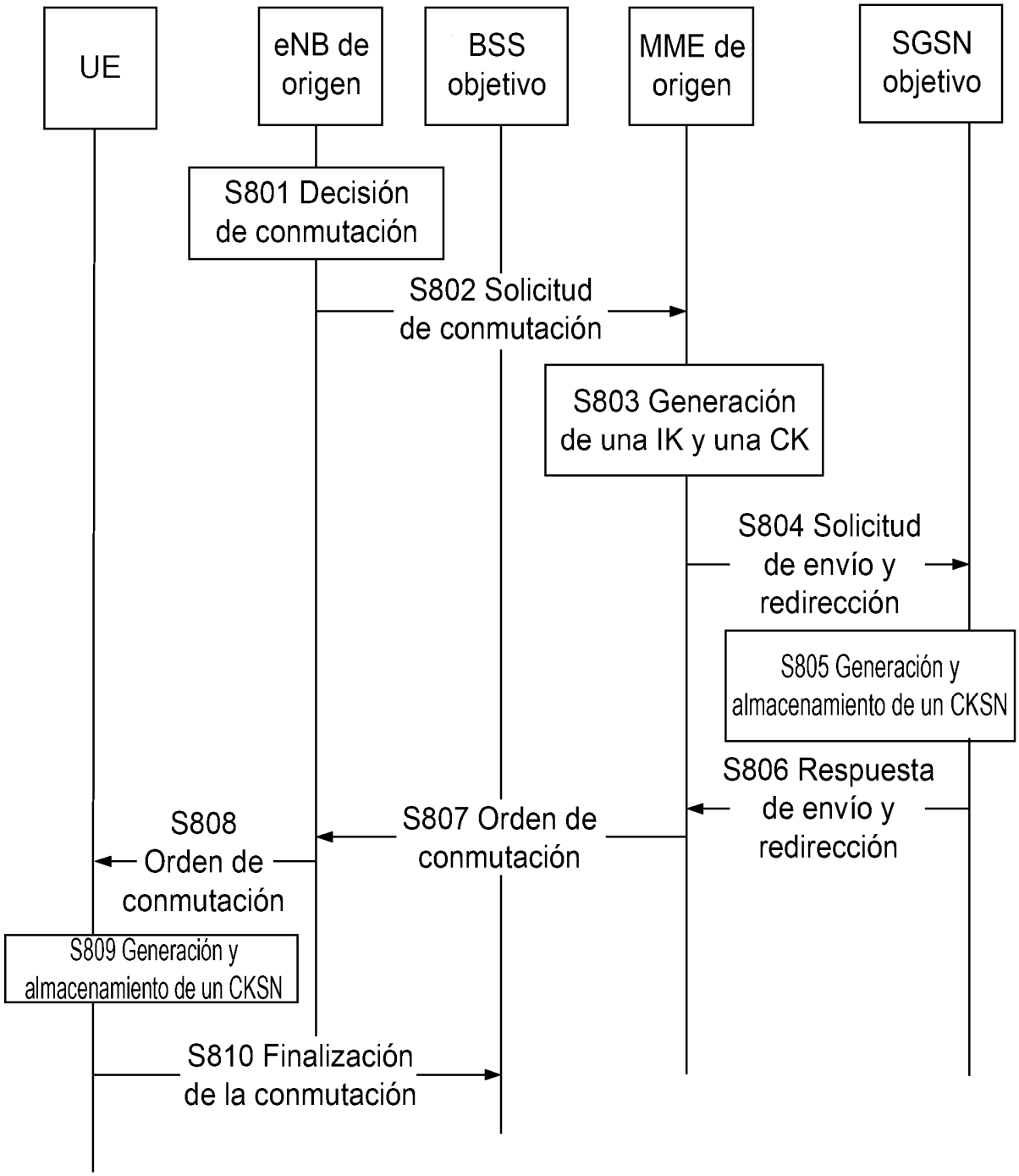

UE
SGSN objetivo
MME de origen
S701 Generación y almacenamiento de un CKSN
S702 Solicitud de actualización o solicitud de adición de área de ruta
S703 Solicitud de contexto o solicitud de identificación
S704 Generación de una IK y una CK
S705 Respuesta de contexto o respuesta de identificación
S706 Generación y almacenamiento de un CKSN
S707 Aceptación de actualización o aceptación de adición de área de ruta
S708 Finalización de actualización o finalización de adición de área de ruta

Fig. 8


UE
eNB de origen
BSS objetivo
MME de origen
SGSN objetivo
S801 Decisión de conmutación
S802 Solicitud de conmutación
S803 Generación de una IK y una CK
S804 Solicitud de envío y redirección
S805 Generación y almacenamiento de un CKSN
S806 Respuesta de envío y redirección
S807 Orden de conmutación
S808 Orden de conmutación
S809 Generación y almacenamiento de un CKSN
S810 Finalización de la conmutación