(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 615 956**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.06.2009 PCT/CN2009/072292**

(87) Fecha y número de publicación internacional: **23.12.2009 WO2009152759**

(96) Fecha de presentación y número de la solicitud europea: **16.06.2009 E 09765398 (4)**

(97) Fecha y número de publicación de la concesión europea: **30.11.2016 EP 2293610**

(54) Título: **Método y dispositivo de prevención de pérdida de sincronización de seguridad de red**

(30) Prioridad:

16.06.2008 CN 200810039233
25.08.2008 CN 200810146831

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.06.2017

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian Longgang District , Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

CHEN, JING;
YANG, YANMEI;
XU, YIXIAN;
WONG, MARCUS y
ZHANG, AIQIN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y dispositivo de prevención de pérdida de sincronización de seguridad de red

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo de la tecnología de las comunicaciones y en particular, a una tecnología de seguridad de red.

ANTECEDENTES DE LA INVENCIÓN

Actualmente, las comunicaciones móviles han sido ampliamente desarrolladas y se hicieron muy populares. El proceso de las comunicaciones móviles implica un problema de una transferencia de un terminal entre diferentes sistemas de acceso.

Las redes de acceso de radio de una estación base incluyen un sistema de comunicaciones móviles de la Segunda Generación (2G), un sistema de comunicaciones móviles de la Tercera Generación (3G) y un sistema de Evolución a Largo Plazo (LTE) futura. Los niveles de protección de seguridad y las medidas protectoras entre un terminal y las redes de acceso de radio son diferentes. Las redes de acceso heterogéneo implican diferentes tecnologías de acceso, y las estructuras de los parámetros de seguridad no son completamente las mismas. Cuando el terminal es objeto de transferencia entre las diferentes redes de acceso, la reutilización de los parámetros del contexto de seguridad en un sistema original se considera también en algunas circunstancias.

La Figura 1 es una vista de una estructura de red de una Red de Acceso de Radio Terrestre Universal (UTRAN). La red UTRAN incluye uno o más Subsistemas de Red de Radio (RNSs). Un subsistema RNS está constituido por un Controlador de Red de Radio (RNC) y una o más estaciones base (Node Bs). La interfaz entre el controlador RNC y una Red Base (CN) es una interfaz Iu. El nodo Node B está conectado al controlador RNC por intermedio de una interfaz Iub. En la red UTRAN, los controladores RNCs están interconectados por intermedio de una interfaz Iur. Las interfaces Iurs pueden conectarse por intermedio de una conexión física directa entre los controladores RNCs o por intermedio de una red de transporte. El controlador RNC está configurado para asignar y controlar recursos de radio del nodo Node B conectado o relacionado con el controlador RNC. El nodo Node B realiza una conversión de flujos de datos entre la interfaz Iub y la interfaz Iu, y al mismo tiempo, participa en una parte de gestión de recursos de radio. El subsistema RNS está conectado a la red CN por intermedio de la interfaz Iu entre el controlador RNC y un Nodo de Soporte (SGSN) de Servicio de Radio General en Paquetes de Servicio (GPRS).

Un Equipo de Usuario (UE) accede a la red UTRAN, y después del Acuerdo de Autenticación y Clave (AKA), el equipo de usuario UE y la red generan juntos una clave de Cifrado (CK) y una clave de Integridad (IK).

Una longitud de un Identificador de Conjunto de Claves (KSI) es 3 bits, y el identificador KSI se utiliza para identificar la clave CK y la clave IK. El valor de KSI varía desde 0 a 111. Sin embargo, si el valor de KSI es 111, lo que indica que las claves CK e IK están indisponibles, cuando el equipo de usuario UE alcanza el tiempo siguiente, el lado de la red, a modo de ejemplo, el nodo SGSN, detecta que el identificador KSI es 111 y a continuación, se inicia operativamente el proceso de una nueva autenticación (AKA).

En conformidad con los diferentes tipos de dominio (un dominio de paquetes conmutados o un dominio de circuitos conmutados), las claves CKs e IKs se dividen, además, en dos conjuntos de claves: CK_{ps} e IK_{ps} del dominio de paquetes conmutados y CK_{cs} e IK_{cs} del dominio de circuitos conmutados.

Las claves CK e IK tienen una duración, que se identifica por un valor denominado START. El valor START varía desde 0 a un valor umbral. Cuando se genera una clave CK y una clave IK en el proceso AKA original, el valor START es 0. Con el uso de las claves CK e IK, el valor de START aumenta continuamente hasta que se alcanza el valor umbral. Cuando el valor START alcanza el valor umbral, se inicia operativamente un nuevo proceso AKA.

Cuando se desactiva el Equipo Móvil (ME), una clave raíz Kasme memorizada en el equipo ME, un valor START y un identificador KSIasme son eliminados en su totalidad. Cuando se activa de nuevo el equipo ME, los parámetros de seguridad (tales como las claves CK_{ps}, IK_{ps}, KSI y el valor START) memorizados en un Módulo de Identidad Universal de Abonado (USIM) se envían al equipo ME, de modo que las claves CK_{ps} e IK_{ps} puedan reutilizarse también con normalidad, y no se requiere un nuevo proceso AKA.

La Figura 2 es una vista de una estructura de red de una red UTRAN evolucionada (EUTRAN), que incluye nodos NodeBs de EUTRAN (eNBs). El intercambio de datos y la señalización entre los nodos eNBs se realiza por intermedio de una interfaz X2. Un nodo eNB está conectado a una Entidad de Gestión de Movilidad (MME) de una red de Núcleo de Paquetes Evolucionado (EPC) por intermedio de una interfaz S1. Un nodo eNB está conectado a una Pasarela de Servicio (S-GW) por intermedio de una interfaz S1. Solamente existen dominios de paquetes conmutados en la red EUTRAN, y por lo tanto, solamente existen las claves CK_{ps} e IK_{ps}. Más adelante, si no se indica específicamente, ambas claves CK e IK representan las claves de dominios de paquetes conmutados.

En un primer escenario operativo, un equipo de usuario UE accede a la red EUTRAN. Después de la autenticación, el equipo UE y la red generan juntos una clave CK_{ps} y una clave IK_{ps}, que se memorizan en un módulo USIM en el equipo UE. Una clave raíz Kasme de la Entidad de Gestión de Seguridad de Acceso (ASME) se deriva, además, a partir de las claves CK_{ps} e IK_{ps}, y se memoriza en una parte del equipo ME en el UE. La entidad ASME en la red EUTRAN es una entidad MME.

Cuando el equipo UE se desplaza desde la red EUTRAN a una UTRAN (incluyendo una transferencia en un estado activo y la movilidad en un estado inactivo), pueden derivarse una nueva clave CK_{ps}' y una nueva clave IK_{ps}' a partir de la clave raíz K_{asme} (los valores CK_{ps}' y de IK_{ps}' no son iguales a los CK_{ps} e IK_{ps}). En consecuencia, cuando el equipo UE se desplaza desde la red UTRAN a la red EUTRAN, la clave raíz K_{asme} puede derivarse también a partir de las claves CK e IK.

En un segundo escenario operativo, un equipo UE accede a una red UTRAN. Después de la autenticación, el equipo UE y la red generan juntos una clave CK_{ps} y una clave IK_{ps}, que se memorizan en un módulo USIM en el equipo UE. Las claves CK_{ps} e IK_{ps} se memorizan en una parte del ME en el equipo UE.

Cuando el equipo UE se desplaza desde la red UTRAN a una red EUTRAN, una clave raíz K_{asme} puede derivarse también a partir de las claves CK e IK.

Cuando el equipo UE se desplaza desde la red EUTRAN a la red UTRAN (incluyendo una transferencia en un estado activo y una movilidad en un estado inactivo), puede derivarse una nueva CK_{ps}' y una IK_{ps}' a partir de la clave raíz K_{asme} (los valores de CK_{ps}' e IK_{ps}', en este caso, no son iguales a los de CK_{ps} e IK_{ps}).

En los dos escenarios operativos precedentes, el mismo KSI identifica diferentes pares de claves {CK_{ps}, IK_{ps} } y {CK_{ps}', IK_{ps}'}, y cuando se reutiliza el parámetro de seguridad en un terminal, es decir, el contexto de seguridad, puede presentarse el problema precedente de la desincronización del contexto de seguridad, que causa el fallo operativo del terminal para acceder a una red.

La publicación de la solicitud de patente de los Estados Unidos US 2008/0096530 A1 da a conocer la utilización de un valor START para controlar la duración de CK/IK. En el momento del establecimiento de cada conexión de RRC, el equipo UE iniciará operativamente la generación de un nuevo conjunto de claves de enlace de acceso (una nueva CK y una nueva IK) si el valor START actual ha alcanzado el valor umbral THRESHOLD, para los dominios de redes bases correspondientes.

SUMARIO DE LA INVENCIÓN

En consecuencia, la presente invención da a conocer un método y un dispositivo para evitar la desincronización de seguridad de red, con lo que se evita el fallo operativo de un usuario para acceder a una red debido a la desincronización de parámetros de seguridad de red. La solución técnica, según la presente invención, se realiza como se da a conocer en las reivindicaciones independientes.

Para conseguir los objetivos de la presente invención, se dan a conocer las soluciones técnicas siguientes.

En conformidad con un primer aspecto de la idea inventiva de la presente invención, un método para evitar la desincronización de seguridad de una red incluye en su primera forma de puesta en práctica:

realizar, por un terminal de usuario, una transferencia de red y generar una nueva clave derivada mediante la derivación de claves en una nueva red; y

modificar un parámetro de seguridad memorizado en un módulo USIM en el terminal de usuario.

En conformidad con el segundo aspecto de la idea inventiva de la presente invención, un dispositivo para evitar la desincronización de seguridad de una red, está situado en un lado del terminal de usuario, en donde el dispositivo incluye:

una unidad de transferencia, configurada para realizar una transferencia de red de un terminal de usuario y para generar una nueva clave derivada mediante una derivación de claves en una nueva red; y

una unidad de modificación, configurada para modificar un parámetro de seguridad en un módulo USIM en el equipo UE después de que se complete la transferencia de red del terminal de usuario.

En conformidad con el tercer aspecto de la idea inventiva de la presente invención, se da a conocer un terminal para evitar la desincronización de seguridad de red. El terminal incluye el dispositivo precedente para evitar la desincronización de seguridad de red.

Dicho método para evitar la desincronización de seguridad de red incluye en su segunda forma de puesta en práctica:

obtener un nuevo KSI en conformidad con un KSI de una red original cuando se realiza una transferencia de red; y

utilizar el nuevo KSI como un KSI de una red objetivo.

La obtención del nuevo KSI incluye:

recibir el KSI transferido por la red original; y

obtener el nuevo KSI modificando el KSI.

La obtención del nuevo KSI incluye:

recibir el nuevo KSI que se envía por la red original y se obtiene modificando el KSI de la red original.

La transferencia de red incluye:

una transferencia del terminal de usuario en un estado activo entre diferentes redes; o

la movilidad del terminal de usuario en un estado inactivo entre diferentes redes.

El método incluye, además:

notificar al terminal de usuario el nuevo KSI; o

notificar al terminal de usuario de la generación de un nuevo KSI que es el mismo que el de una red basada en una regla preestablecida.

El KSI de la red original se modifica utilizando el método siguiente:

la obtención de un nuevo KSI realizando el cálculo en conformidad con un KSI de la red original y/o asignando un nuevo valor de un nuevo KSI al KSI;

o demandar un nuevo KSI desde una entidad de red;

u obtener un nuevo KSI realizando un cálculo en conformidad con un algoritmo preestablecido;

o añadir un campo al KSI de la red original para identificar un tipo de red.

En conformidad con el cuarto aspecto de la idea inventiva de la presente invención, un dispositivo para evitar la desincronización de seguridad de red está situado en una red. El dispositivo incluye:

una unidad de recepción, configurada para recibir un KSI durante una transferencia de red;

una unidad de modificación, configurada para modificar el KSI; y

una unidad de notificación, configurada para enviar información de notificación para notificar un nuevo identificador de red.

La unidad de modificación incluye, además: un módulo de algoritmo, en donde el módulo de algoritmo está configurado para obtener un nuevo KSI realizando un cálculo en conformidad con un KSI de una red original; y/o configurado para asignar un nuevo nombre de un nuevo KSI al KSI; o

configurada para demandar un nuevo KSI desde una entidad de red; o

configurada para obtener un nuevo KSI realizando un cálculo en conformidad con un algoritmo preestablecido.

El equipo de red para evitar la desincronización de seguridad de red incluye cualquiera de los dispositivos precedentes en la red para evitar la desincronización de seguridad de red.

En conformidad con el quinto aspecto de la idea inventiva de la presente invención, un método para resolver el problema de desincronización de seguridad de red incluye:

adaptar, por una red, un parámetro de seguridad;

enviar, por la red, una información de orden de iniciar el modo de seguridad a un terminal;

recibir, por la red, ningún mensaje de respuesta desde el terminal dentro de un periodo de tiempo predeterminado; y

iniciar, por la red, un proceso de reautenticación.

En conformidad con el sexto aspecto de la idea inventiva de la presente invención, un dispositivo para resolver el problema de la desincronización de seguridad de red incluye:

una unidad de recepción, configurada para recibir un parámetro de seguridad enviado por un terminal de usuario;

una unidad de adaptación, configurada para adaptar el parámetro de seguridad recibido con su propio parámetro de seguridad;

una unidad de envío, configurada para enviar información de seguridad al terminal de usuario; y

una unidad de iniciación, configurada para reiniciar el proceso AKA si no se recibe ningún mensaje de respuesta desde el terminal de usuario dentro de un periodo de tiempo predeterminado.

Considerando lo que antecede, un parámetro de seguridad en un terminal de usuario (la parte de USIM) se procesa en un tiempo adecuado, o un parámetro de seguridad en el terminal de usuario (la parte de ME) y la red se procesa cuando el terminal de usuario realiza una transferencia de red. En conformidad con la presente invención, modificando un parámetro de seguridad en un momento adecuado, se evita efectivamente el fallo operativo de un terminal para acceder a una red debido a la desincronización del parámetro de seguridad y se mejora la disponibilidad de la red y la seguridad en los escenarios operativos relacionados con la transferencia.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para describir las soluciones técnicas en conformidad con las formas de realización de la presente invención o en la técnica anterior con mayor claridad, se introducen brevemente, a continuación, los dibujos adjuntos para describir las formas de realización o la técnica anterior.

La Figura 1 es un diagrama esquemático de una estructura de red de una red UTRAN en la técnica anterior;

La Figura 2 es un diagrama esquemático de una estructura de red de una red EUTRAN en la técnica anterior;

La Figura 3 es un diagrama esquemático de un proceso intermedio de una transferencia de red en la técnica anterior;

La Figura 4 es un diagrama esquemático de un proceso intermedio de una transferencia de red en la técnica anterior;

La Figura 5 es un diagrama esquemático de un proceso intermedio de una transferencia de red en la técnica anterior;

La Figura 6 es un diagrama esquemático de un proceso intermedio de una transferencia de red en la técnica anterior;

La Figura 7 es un diagrama de flujo de un método en conformidad con una primera forma de realización de la presente invención;

La Figura 8 es un diagrama de flujo de un método en conformidad con una segunda forma de realización de la presente invención;

La Figura 9 es un diagrama de flujo de un método en conformidad con una tercera forma de realización de la presente invención;

La Figura 10 es una vista de señalización de un método en conformidad con la tercera forma de realización de la presente invención;

La Figura 11 es un diagrama de flujo de un método en conformidad con una cuarta forma de realización de la presente invención;

La Figura 12 es una vista de señalización de un método en conformidad con la cuarta forma de realización de la presente invención;

La Figura 13 es un diagrama de flujo de un método en conformidad con una quinta forma de realización de la presente invención;

La Figura 14 es un diagrama de flujo de un método en conformidad con una sexta forma de realización de la presente invención;

La Figura 15 es una vista de señalización del método en conformidad con la sexta forma de realización de la presente invención;

La Figura 16 es un diagrama de flujo de un método en conformidad con una séptima forma de realización de la presente invención;

La Figura 17 es una vista de señalización de un método en conformidad con la séptima forma de realización de la presente invención;

La Figura 18 es un diagrama de flujo de un método en conformidad con una octava forma de realización de la presente invención;

La Figura 19 es una vista de señalización del método en conformidad con la octava forma de realización de la presente invención;

La Figura 20 es una vista estructural esquemática de un dispositivo en conformidad con una forma de realización de la presente invención;

La Figura 21 es una vista estructural esquemática de un dispositivo en conformidad con otra forma de realización de la presente invención;

La Figura 22 es una vista estructural esquemática de un dispositivo en conformidad con otra forma de realización de la presente invención;

La Figura 23 es una vista de señalización de un método en conformidad con una novena forma de realización de la presente invención;

La Figura 24 es una vista de señalización de un método en conformidad con una décima forma de realización de la presente invención; y

La Figura 25 es una vista de señalización de un método en conformidad con una undécima forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

Para hacer más comprensibles los objetivos, las soluciones técnicas y las ventajas de las formas de realización de la presente invención, dichas formas de realización de la presente invención se describen con más detalle a continuación.

La transferencia mencionada en las formas de realización de la presente invención incluye la movilidad de un equipo UE en un estado inactivo (movilidad inactiva) y una transferencia de un equipo UE en un estado activo (transferencia activa).

A continuación, se proporcionan dos ejemplos típicos para describir los escenarios operativos de la desincronización del parámetro de seguridad entre un equipo de usuario UE y una red.

En un primer escenario operativo, un equipo UE realiza, al principio, un proceso AKA inicial en una red EUTRAN. Cuando el equipo UE se desplaza desde la red EUTRAN a una red UTRAN, una clave CK y una clave IK utilizadas en la red UTRAN se derivan de una clave raíz Kasme utilizada en la red EUTRAN.

En primer lugar, el equipo UE está en la red EUTRAN. Después del proceso AKA inicial, una clave CK_{ps}, una IK_{ps} y un identificador KSIasme, es decir, un identificador de conjunto de claves de una clave raíz Kasme se genera a este respecto. Una entidad ME memoriza también el identificador KSIasme y la clave Kasme, según se ilustra en la Figura 3.

En conformidad con la técnica anterior, si un equipo UE está en una red UTRAN, después del proceso AKA, la situación en la que la clave CK_{ps} y la clave IK_{ps} se memorizan en un módulo USIM, que es similar al ilustrado en la Figura 3, puede producirse también, o, otras claves CK_{ps} e IK_{ps}, tales como las derivadas durante una transferencia de red pueden memorizarse también en el módulo USIM.

Cuando el equipo UE se desplaza desde una red basada en paquetes de la EUTRAN a una red basada en paquetes de la UTRAN, la clave Kasme memorizada en el ME necesita utilizarse para generar un nueva clave CK_{ps}' y una nueva clave IK_{ps}', y el equipo ME memoriza también el KSI, en donde KSI = KSIasme, según se ilustra en la Figura 4.

Después de que el equipo UE se desplace desde la red EUTRAN a la red UTRAN, si el equipo ME se desactiva repentinamente (lo que similar a la retirada de una batería desde un teléfono móvil), en el momento, un nodo SGSN en la red todavía memoriza temporalmente los antiguos parámetros de claves de seguridad en el equipo ME, es decir, el KSI, la clave CK_{ps}' y la clave IK_{ps}'. La clave de seguridad memorizada en el equipo ME ha sido completamente suprimida debido a la desactivación, mientras que los antiguos valores de KSIasme, CK_{ps} e IK_{ps} se memorizan todavía en el módulo USIM, según se ilustra en la Figura 5.

Cuando el usuario pasa de nuevo a la condición activa, y también lo hace el equipo UE, el equipo ME efectúa la lectura de los parámetros de seguridad memorizados en el módulo USIM, que incluyen las claves CK_{ps}, IK_{ps} y el KSI. En ese momento, el nodo SGSN en la red memoriza todavía los antiguos parámetros de seguridad en el equipo ME, es decir, las claves CK_{ps}', IK_{ps}', y el identificador KSI, según se ilustra en la Figura 6.

En la técnica anterior, cuando el equipo de usuario UE se activa de nuevo y se conecta a la red UTRAN durante el establecimiento del contexto de seguridad, el equipo ME envía el KSI al nodo SGSN y el nodo SGSN compara el KSI recibido con el KSI memorizado por el nodo SGSN, y si son los mismos, se considera que el equipo ME y el nodo SGSN memorizan las mismas claves CK e IK. No se requiere ningún nuevo proceso AKA. Durante la investigación, los inventores encontraron que, de hecho, en la situación ilustrada en la Figura 6, las claves CK_{ps} e IK_{ps} utilizadas por el equipo UE en un sistema de red EUTRAN se memorizan en el equipo ME y las claves CK_{ps}' e IK_{ps}' derivadas de la clave raíz Kasme en una entidad MME, cuando se realiza la transferencia desde la red EUTRAN a la red UTRAN, se memorizan en el nodo SGSN, lo que hace que el mismo KSI identifique realmente los diferentes pares de claves {CK_{ps}, IK_{ps}} y {CK_{ps}', IK_{ps}'} en el equipo ME y en la red. Puesto que las claves IKs y CKs memorizadas en el equipo ME y en el nodo SGSN son diferentes, la desincronización de parámetros de seguridad puede dar lugar al fallo operativo del equipo UE para acceder a la red.

En un segundo escenario operativo, un equipo UE se desplaza desde una red original a una red EUTRAN, y luego, se desplaza desde la red EUTRAN a una red UTRAN. La red original puede ser una red de Sistema Global para Comunicaciones Móviles (GSM) o una red UTRAN. Cuando se realiza el proceso de autenticación inicial (AKA) en el equipo UE en primer lugar en la red UTRAN, un módulo USIM memoriza el contexto de seguridad del equipo UE en la red UTRAN, el contexto de seguridad incluye una clave CK_{ps}, una clave IK_{ps} y un KSI.

Cuando el equipo UE se desplaza desde la red UTRAN a la red EUTRAN, necesita derivarse una clave raíz Kasme del equipo UE en la red EUTRAN en conformidad con las claves CK_{ps} e IK_{ps} memorizadas en el módulo USIM. En este momento, el módulo USIM memoriza la clave CK_{ps}, la clave IK_{ps} y el identificador KSI, y el equipo ME memoriza el identificador KSI y la clave raíz Kasme, que es similar al resultado de realizar el proceso AKA en el equipo UE directamente en la red EUTRAN en el primer escenario operativo según se ilustra en la Figura 3.

Después de que el equipo UE se desplace desde la red EUTRAN a la red UTRAN, las claves CK_{ps}' e IK_{ps}' se derivan además a partir de la clave raíz Kasme y el identificador KSI no cambia. Si se desactiva repentinamente el equipo ME (de modo similar a la retirada de una batería), en ese momento operativo, un nodo SGSN en la red sigue memorizando temporalmente los parámetros de clave de seguridad antiguos en el equipo ME, es decir, el identificador KSI, la clave CK_{ps}' y la clave IK_{ps}'. La clave de seguridad memorizada en el equipo ME ha sido completamente eliminada al producirse la desactivación, mientras que el antiguo identificador KSIasme así como las claves CK_{ps} e IK_{ps} se siguen memorizando en el módulo USIM. El proceso es similar al del primer escenario operativo, y el resultado se ilustra en la Figura 5.

Cuando el usuario se activa de nuevo, se activa también el equipo UE y en ese momento operativo, el equipo ME efectúa la lectura de los parámetros de seguridad memorizados en el módulo USIM, que incluyen la clave CK_{ps}, la clave IK_{ps} y el identificador KSI. En ese momento operativo, el nodo SGSN en la red memoriza todavía los antiguos parámetros de seguridad en el equipo ME, es decir, la clave CK_{ps}', la clave IK_{ps}' y el identificador KSI, según se ilustra en la Figura 6.

En la misma situación que en la del primer escenario operativo, cuando el equipo UE se activa de nuevo y se conecta a la red UTRAN, durante el establecimiento del contexto de seguridad, el equipo ME envía el identificador KSI de seguridad al nodo SGSN, el nodo SGSN compara el KSI recibido con el identificador KSI memorizado por el nodo SGSN, y si son los mismos, se considera que el equipo ME y el nodo SGSN memorizan las mismas claves CK e IK. No se requiere ningún nuevo proceso AKA. De hecho, en la situación ilustrada en la Figura 6, las claves CK_{ps} e IK_{ps} se memorizan en el equipo ME y las claves CK_{ps}' e IK_{ps}' derivadas de la clave raíz Kasme en una entidad MME cuando se realiza una transferencia desde la red EUTRAN a la red UTRAN se memorizan en el nodo SGSN. Las claves IKs y CKs memorizadas en el equipo ME en el nodo SGSN son diferentes, de modo que la desincronización del parámetro de seguridad de red puede dar lugar al fallo operativo del equipo UE para acceder a la red.

De modo similar, después de que se realice el proceso AKA inicial en el equipo UE en primer lugar en una red GSM, el módulo USIM memoriza el parámetro de seguridad del proceso AKA inicial de la red GSM. A continuación, el equipo UE se desplaza a la red EUTRAN, y se realiza la derivación de claves. Cuando el equipo UE se desplaza de nuevo desde la red EUTRAN a la red UTRAN o la red GSM, se desactiva el equipo ME y luego, el equipo UE se activa de nuevo. El principio de que la desincronización de parámetros de seguridad de la red da lugar al fallo operativo del equipo UE para acceder a la red es el mismo que lo era en el segundo escenario operativo.

Los escenarios operativos dados a conocer con anterioridad están previstos para ilustrar lo siguiente: cuando un terminal está en la red, el mismo KSI identifica diferentes pares de claves {CK_{ps}, IK_{ps}} y {CK_{ps}', IK_{ps}'}, cuando el parámetro de seguridad en el terminal, es decir, el contexto de seguridad, se reutiliza, puede producirse el problema precedente de la desincronización del contexto de seguridad, lo que da lugar al fallo operativo del terminal para acceder a la red. Además de los escenarios operativos anteriores, todos los escenarios que potencialmente hacen que el mismo KSI identifique los diferentes pares de claves {CK_{ps}, IK_{ps}} y {CK_{ps}', IK_{ps}'} pueden dar lugar también a la desincronización del contexto de seguridad y por ello no se describirán aquí uno por uno.

La Figura 7 ilustra una primera forma de realización de la presente invención. En la forma de realización, la puesta en práctica de un método para evitar la desincronización de seguridad de la red en conformidad con la forma de realización incluye las etapas siguientes:

En la etapa 701, un equipo de usuario realiza un proceso AKA en una red original (tal como una red EUTRAN).

La red original es la red EUTRAN. Después del proceso AKA, se generan una clave CK_{ps}, una clave IK_{ps}, una clave raíz Kasme y un identificador KSIasme. Las claves CK_{ps}, IK_{ps} y el identificador KSIasme se memorizan en un módulo USIM. Un equipo ME memoriza el mismo identificador KSIasme que en el módulo USIM.

En la etapa 702, se modifica un parámetro de seguridad.

Preferentemente, después de la etapa 702, el método incluye, además, la etapa siguiente:

Reiniciar el proceso AKA y generar una nueva información de parámetro de seguridad.

En diferentes formas de realización, el parámetro de seguridad puede modificarse en diferentes maneras. Las formas de realización de la presente invención se describen en detalle a continuación haciendo referencia a las diferentes maneras.

En una segunda forma de realización, el parámetro de seguridad se modifica estableciendo el parámetro de seguridad en un módulo USIM para un estado no disponible. El estado no disponible se refiere a que el parámetro de seguridad se hace indisponible modificando el parámetro de seguridad en el módulo USIM. Haciendo referencia a la Figura 8, la forma de realización incluye las etapas siguientes:

En la etapa 801, un terminal de usuario realiza un proceso AKA en una red original.

La red original es una red EUTRAN, una red UTRAN o una red GSM.

Cuando un equipo UE está en la red EUTRAN, después del proceso AKA en la red original, se generan una clave CK_{ps}, una clave IK_{ps}, una clave raíz Kasme y un KSI o un identificador KSIasme. Las claves CK_{ps}, IK_{ps}, Kasme y el identificador KSIasme se memorizan en un módulo USIM. Un equipo ME memoriza también los mismos valores de KSIasme y Kasme que los del módulo USIM.

Cuando el equipo UE está en una red UTRAN, después de un proceso AKA en la red UTRAN, se genera una clave CK_{ps}, una clave IK_{ps} y un identificador KSI, que se memorizan en un equipo ME. Cuando el equipo ME envía una instrucción al módulo USIM para demandar al módulo USIM que memorice el parámetro de seguridad, el módulo USIM puede memorizar los valores de CK_{ps}, IK_{ps} y KSI.

En la etapa 802, se establece el parámetro de seguridad en el módulo USIM a un estado no disponible.

El parámetro de seguridad en el módulo USIM puede establecerse al estado no disponible en numerosas maneras, que incluye utilizando el método de establecer un valor de START en el módulo USIM para un umbral, el método de establecer el KSI a 111, o utilizando el método de suprimir las clave CK e IK. La descripción detallada se proporciona a continuación mediante formas de realización para describir cada manera operativa.

En una tercera forma de realización, un módulo USIM se hace indisponible cambiando un valor de START en el módulo USIM. Haciendo referencia a la Figura 9, la forma de realización incluye las etapas siguientes:

En la etapa 901, un terminal de usuario realiza un proceso AKA en una red original.

En la etapa 902, se establece un valor START de un módulo USIM a un valor umbral.

O bien, se suprime una clave CK y una clave IK.

O bien, se establece un identificador KSI a 111.

La Figura 10 es un diagrama de flujo de señalización correspondiente a una realización ejemplo dada a conocer en esta forma de realización. En la Figura 10, un equipo UE está en una red UTRAN, y las etapas son como sigue:

En las etapas 1-2, el equipo UE está en la red EUTRAN, y el equipo UE envía un mensaje de demanda de servicio a una entidad MME por intermedio de un nodo eNB.

En la etapa 3, la entidad MME no tiene un parámetro de seguridad en el UE, se inicia operativamente un proceso AKA, y el equipo UE y la entidad MME generan una clave raíz K_{asme}.

En la etapa 4, en el equipo UE, un equipo ME establece un valor START en un módulo USIM a un valor umbral.

Cuando el valor START del módulo USIM se establece al valor umbral, las claves CK e IK ya no se pueden utilizar (o bien, las claves CK e IK se suprimen). Cuando un terminal de usuario (la parte de ME) se desactiva y activa de nuevo, el equipo ME efectúa la lectura del parámetro de seguridad a partir del módulo USIM. Cuando la red recibe una demanda de conexión (incluyendo un identificador KSI) desde el terminal de usuario, y comprueba que las claves CK e IK originales correspondientes al identificador KSI están indisponibles (o bien, puesto que se han suprimido las claves CK e IK, el terminal de usuario no puede incluir el identificador KSI en la demanda de conexión), la red realiza la determinación correspondiente e inicia un nuevo proceso de autenticación, y no se produce la situación de la desincronización de seguridad de la red.

En una cuarta forma de realización, cuando un terminal de usuario realiza una transferencia en redes, y después de que el terminal de usuario realice una derivación de claves, (a modo de ejemplo, el terminal de usuario realiza una transferencia desde una red EUTRAN a una red UTRAN, en una parte de ME del terminal de usuario y en la red, se derivan una clave CK_{ps}' y una clave IK_{ps}' a partir de una clave raíz Kasme, el parámetro de seguridad en un módulo USIM se hace indisponible estableciendo la clave en el módulo USIM para ser indisponible (incluyendo el establecimiento de un identificador KSI a 111 y/o estableciendo un valor START en el módulo USIM a un valor umbral y/o suprimiendo una clave CK_{ps} original y una clave IK_{ps} original en el módulo USIM). Haciendo referencia a la Figura 11, la forma de realización incluye las etapas siguientes:

En la etapa 1101, un terminal de usuario realiza un proceso AKA en una red original.

El proceso AKA es esencialmente el mismo que el de las formas de realización precedentes, y por lo tanto no se describe aquí de nuevo.

En la etapa 1102, el terminal de usuario realiza una transferencia de red, genera una clave derivada y se sincroniza con la red.

Después de que se realice satisfactoriamente la transferencia de red del usuario, la información en un nodo SGSN en la red se sincroniza con la información en un equipo ME. El nodo SGSN memoriza los parámetros de seguridad en el equipo ME, es decir, una clave CK_{ps}', una clave IK_{ps}' y un identificador KSI.

En la etapa 1103, se establece un identificador KSI en un módulo USIM a 111.

El identificador KSI puede ser un número, que ocupa 3 bits, es decir, se utilizan 7 valores para identificar el identificador KSI. El valor 111 puede utilizarse por un terminal para indicar que la clave raíz Kasme no es válida si un identificador KSIasme se establece a 111, o bien, el valor 111 puede utilizarse por un terminal para indicar que la clave CK y la clave IK no son válidas si el identificador KSI puede establecerse a 111.

El identificador KSI en el módulo USIM se establece a 111, lo que indica que actualmente ninguna clave CK_{ps}' o IK_{ps}' está disponible, de modo que en el proceso posterior (tal como un terminal de usuario se activa de nuevo o un terminal de usuario realiza una transferencia de red), se inicia operativamente un nuevo proceso AKA, y se establece un nuevo parámetro de seguridad.

La Figura 12 es un diagrama de flujo de señalización de una realización ejemplo dada a conocer en la forma de realización. En la Figura 12, un equipo UE es objeto de transferencia desde una red basada en paquetes de una red EUTRAN a una red basada en paquetes de una red UTRAN. Haciendo referencia a la Figura 12, se incluyen las etapas siguientes.

En la etapa 1, un equipo UE envía una demanda de actualización de área de enrutamiento (RAU) a un nodo SGSN

objetivo, en donde la demanda RAU incluye un identificador KSI y un identificador de identidad temporal, etc., que se memorizan por el equipo UE.

En la etapa 2, el nodo SGSN objetivo demanda un parámetro de seguridad desde una demanda MME original y la demanda incluye el identificador de identidad de abonado móvil temporal (TMSI) obtenido a partir del equipo UE.

En la etapa 2a, la entidad MME original realiza la derivación de claves, derivándose las claves CK_{ps}' e IK_{ps}' a partir de una clave raíz Kasme.

En la etapa 3, el nodo SGSN obtiene los parámetros de seguridad enviados por la entidad MME, en donde los parámetros de seguridad incluyen las claves CK_{ps}' e IK_{ps}' derivadas, y un nuevo identificador KSI.

En la etapa 4, de modo opcional, si el identificador KSI enviado desde el equipo UE en la etapa 1 es 111, o debido a otros requisitos operativos, se inicia un nuevo proceso AKA. Puede generarse también un nuevo identificador KSI.

En la etapa 5, el nodo SGSN envía una orden de modo de seguridad que incluye las claves CK_{ps}' e IK_{ps}' derivadas obtenidas a partir de la entidad MME original, y algoritmos de encriptación (UEAs) del Sistema Universal de Telecomunicaciones Móviles (UMTS) y algoritmos de integridad de UMTS (UIAs) permitidos por el nodo SGSN.

En la etapa 6, un controlador RNC selecciona un algoritmo UEA final y un algoritmo UIA final y envía la orden de modo de seguridad al equipo UE.

En la etapa 7, el equipo UE deriva las claves CK_{ps}' e IK_{ps}' a partir de la clave raíz Kasme.

En la etapa 8, el equipo UE envía un mensaje del modo de seguridad completo.

En la etapa 9, el controlador RNC transfiere el mensaje del modo de seguridad completo al nodo SGSN.

En la etapa 10, el nodo SGSN envía un mensaje de aceptación de RAU (con protección de integridad) al equipo UE, que incluye el nuevo identificador KSI obtenido en la etapa 2b.

En la etapa 11, el equipo UE recibe el mensaje de aceptación de RAU, y reenvía un mensaje de RAU completo al nodo SGSN.

En la etapa 12, después de que se complete la transferencia, se establece el KSI en el módulo USIM a 111.

Cuando el usuario se activa de nuevo, y la red detecta que el identificador KSI enviado por el equipo UE es 111, y/o el equipo UE no puede enviar el identificador KSI, se inicia un proceso AKA para generar una nueva clave, de modo que se evite la desincronización de seguridad de red.

En una quinta forma de realización, haciendo referencia a la Figura 13, se modifica un identificador KSI en un módulo USIM, y la forma de realización incluye las etapas siguientes:

En la etapa 1301, un terminal de usuario realiza un proceso AKA en una red original.

El proceso AKA es el mismo que en la totalidad de las formas de realización precedentes, y por lo tanto, no se describe aquí de nuevo.

En la etapa 1302, el terminal de usuario realiza una transferencia de red, genera una clave derivada y se sincroniza con la red.

Después de que la transferencia de red del terminal de usuario sea satisfactoria, la información en un nodo SGSN en la red se sincroniza con la información en un equipo ME. El nodo SGSN memoriza los parámetros de seguridad en el terminal de usuario, es decir, una clave CK_{ps}', una clave IK_{ps}' y un identificador KSI.

En la etapa 1303, se modifica el KSI en un módulo USIM.

El identificador KSI en el módulo USIM puede modificarse mediante múltiples métodos, tales como estableciendo KSI = KSI + 1.

Después de que el terminal de usuario sea objeto de transferencia desde una red EUTRAN a una red UTRAN, si el terminal de usuario se desactiva, cuando el terminal de usuario se active de nuevo, el equipo ME envía un identificador de usuario que incluye un identificador KSI a la red, y la red comprueba el KSI por comparación.

El nodo SGSN en la red memoriza el identificador KSI en el equipo ME cuando se realiza el interfuncionamiento de la red. Una vez terminado el interfuncionamiento de la red, se modifica el KSI en la red UTRAN. A modo de ejemplo,

el identificador KSI puede establecerse a KSI', en donde KSI' = KSI + 1. Si el equipo UE está desactivado, se pierde la clave de seguridad memorizada en el equipo ME debido a la desactivación. Cuando se activa un terminal de usuario, el equipo ME efectúa la lectura de la información en el módulo USIM, en donde la información es el identificador KSI'. Por lo tanto, el identificador KSI' enviado por el terminal de usuario es diferente del KSI en la red, y se considera que no existe ninguna clave CK o IK disponible y el módulo USIM está en un estado indisponible. A continuación, se reinicia un proceso AKA. El fallo operativo del terminal de usuario para acceder a la red debido a la desincronización del parámetro de seguridad se evita de esta manera.

En la aplicación real, el parámetro de seguridad puede modificarse también modificando un identificador KSI de la red, lo que incluye las etapas siguientes:

Un terminal de usuario realiza un proceso AKA en una red original.

Durante una transferencia de la red, se obtiene un nuevo KSI en conformidad con un KSI de la red original.

Utilizar el nuevo KSI como el KSI de una red objetivo.

La obtención del nuevo KSI en conformidad con el KSI de la red original incluye, además: recibir un identificador KSI transferido por la red original, y modificar el KSI, o bien, recibir un nuevo KSI obtenido mediante la modificación del KSI de la red original.

En una sexta forma de realización, haciendo referencia a la Figura 14, se evita una desincronización de seguridad de la red modificando un KSI de una red original. Esta forma de realización incluye las etapas siguientes:

En la etapa 1401, un terminal de usuario realiza un proceso AKA en la red original.

En la etapa 1402, cuando se realiza una transferencia de red, se modifica el KSI de la red original.

En la etapa 1403, se envía un nuevo KSI a una red objetivo.

En KSI en la red se modifica utilizando el método siguiente.

Un nuevo KSI se obtiene realizando un cálculo en conformidad con el identificador KSI.

Y/o, un nuevo nombre de un nuevo KSI se asigna al KSI.

O bien, un nuevo KSI se demanda desde una entidad de red.

O bien, un nuevo KSI se obtiene realizando un cálculo en conformidad con un algoritmo preestablecido.

La Figura 15 es un diagrama de flujo de señalización de un ejemplo dado a conocer en esta forma de realización. La red original es una red EUTRAN. La red objetivo es una red UTRAN. Las etapas son como sigue.

En la etapa 1, un equipo UE envía una demanda RAU a un nodo SGSN objetivo, la demanda RAU incluye un identificador KSI, un identificador de identidad temporal, y así sucesivamente., que se memorizan por el equipo UE.

En la etapa 2, el nodo SGSN objetivo demanda un parámetro de seguridad desde una pasarela MME original, y la demanda incluye el identificador TMSI obtenido a partir del equipo UE.

En la etapa 2a, la entidad MME original realiza una derivación de claves y se derivan una clave CK_{ps}' e IK_{ps}' desde una clave raíz Kasme.

En la etapa 2b, la entidad MME original obtiene un nuevo identificador KSI.

El nuevo identificador KSI se genera por la entidad MME original, de modo que el nuevo KSI pueda generarse sobre la base de un KSI antiguo en un mensaje 1, a modo de ejemplo, nuevo KSI = antiguo KSI + 1; o bien, el nuevo KSI puede generarse realizando el cálculo en conformidad con un algoritmo por defecto; o bien, el nuevo KSI puede generarse sobre la base de un proceso AKA normal.

En otras formas de realización, el nuevo KSI se demanda por la entidad MME original desde una entidad de red, tal como un Servidor Local de Abonado (HSS).

La entidad MME original puede asignar también un nuevo nombre, tal como un identificador KSI_{new} o $KSI_{UTRAN,}$ al nuevo identificador KSI. A diferencia del KSI utilizado en la red EUTRAN, es el KSI_{UTRA} el que se utiliza en la red objetivo, y el KSI_{new} del nuevo KSI puede ser igual o desigual respecto a un KSI_{old} del KSI del sistema original.

En otras formas de realización, se puede añadir también un campo a un identificador KSI para indicar a qué tipo de red pertenece el KSI del parámetro de seguridad. A modo de ejemplo, se añaden 2 bits para identificar el tipo de red correspondiente al KSI, con 01 identificando una red GSM, 10 para identificar una red UTRAN y 11 para identificar una EUTRAN. Por lo tanto, para un mismo KSI (3 bits), tal como 110, cuando se añade el tipo de red, los identificadores KSIs reales en la red GSM, la red UTRAN y una red del Sistema de Paquetes Evolucionado (EPS) son: 01110, 10110 y 11110. Durante una transferencia entre diferentes tipos de redes, el equipo UE y la red no modifican el KSI antiguo cuya longitud es 3 bits en conformidad con la información del tipo de red, y en cambio, añaden identificadores de tipo de red diferentes al identificador KSI antiguo.

Cuando un equipo UE inicia un mensaje de capa 3 (tal como un mensaje de conexión o un mensaje de demanda de servicio), en donde el mensaje de capa 3 incluye un identificador KSI con un identificador del tipo de red (que corresponde al escenario operativo ya descrito en el apartado de ANTECEDENTES DE LA INVENCIÓN, o la Figura 19), la red puede determinar que los identificadores KSIs (añadidos con el valor del tipo de red, y siendo de 5 bits) en los dos lados no son compatibles, y se inicia un nuevo proceso AKA para evitar la desincronización del contexto de seguridad de la red.

En la etapa 3, el nodo SGSN obtiene el parámetro de seguridad enviado por la entidad MME, que incluye las claves derivadas CK_{ps}' e IK_{ps}' y el nuevo identificador KSI.

En la etapa 4, de modo opcional, si el KSI enviado desde el equipo UE en la etapa 1 es 111 o debido a otros requisitos, se inicia un nuevo proceso AKA. Puede también generarse un nuevo identificador KSI.

En la etapa 5, el nodo SGSN envía una orden de modo de seguridad, que incluye las claves derivadas CK_{ps}' e IK_{ps}' obtenidas desde la entidad MME original y los algoritmos UEAs y UIAs permitidos por el nodo SGSN.

En la etapa 6, un controlador RNC selecciona un algoritmo UEA final y un algoritmo UIA final, y envía la orden de modo de seguridad al equipo UE.

En la etapa 7, el equipo UE deriva las claves CK_{ps}' e IK_{ps}' desde la clave raíz Kasme.

En la etapa 8, el equipo UE envía un mensaje de modo de seguridad completo.

En la etapa 9, el controlador RNC transfiere el mensaje de modo de seguridad completo al nodo SGSN.

En la etapa 10, el nodo SGSN envía un mensaje de aceptación de RAU (con protección de integridad) al equipo UE, incluyendo el anclaje de aceptación de RAU el nuevo KSI obtenido en la etapa 2b.

En la etapa 11, el equipo UE recibe el mensaje de aceptación RAU, y reenvía el mensaje RAU completo al nodo SGSN.

Sobre la base de la solución precedente, no importa si la clave utilizada en un sistema UTRAN después de la transferencia se deriva de la clave raíz K_{asme} del sistema original o la clave se obtiene a partir de un nuevo proceso AKA, generándose un nuevo identificador KSI.

Por lo tanto, después de la transferencia, el nuevo KSI no es igual a la clave K_{asme} memorizada en el módulo USIM del equipo UE. Si en el momento operativo, el equipo UE se desactiva en la red UTRAN, se suprime la clave en un equipo ME.

Cuando el equipo UE se activa de nuevo, el equipo ME efectúa la lectura de los valores CK, IK y K_{asme} a partir del módulo USIM. El nodo SGSN memoriza todavía los valores de CK_{ps}', IK_{ps}' y KSI después de la derivación de claves. No obstante, el KSI no es igual a K_{asme} y por lo tanto, no se produce la desincronización de seguridad. En cambio, se inicia un nuevo proceso AKA.

En una séptima forma de realización, se modifican los parámetros de seguridad modificando un KSI de una red. Haciendo referencia a la Figura 16, la forma de realización incluye las etapas siguientes:

En la etapa 1601, un terminal de usuario realiza un proceso AKA en una red original.

En la etapa 1602, cuando se realiza una transferencia de red, se modifica un identificador KSI de una red objetivo.

La entidad que realiza la generación de un nuevo KSI puede ser un elemento de red de la red original (tal como una entidad MME) o un elemento de red de la red objetivo (tal como un nodo SGSN).

El identificador KSI en la red se modifica utilizando el método siguiente.

Un nuevo KSI se obtiene realizando el cálculo en conformidad con el KSI.

Y/o, un nuevo nombre de un KSI se asigna al KSI.

O bien, un nuevo KSI se demanda desde una entidad de red.

O bien, un nuevo KSI se calcula sobre la base de un algoritmo preestablecido.

En la etapa 1603, el terminal de usuario obtiene el nuevo identificador KSI.

La red notifica al terminal de usuario del nuevo KSI, o el terminal de usuario calcula el nuevo KSI localmente basado en la misma estrategia de cálculo (a modo de ejemplo, el mismo algoritmo) que el de la red, y sobre la base del KSI.

La Figura 17 es un diagrama de flujo de señalización de un ejemplo dado a conocer en una forma de realización de la presente invención, que incluye las etapas siguientes:

En la etapa 1, un equipo UE envía una demanda RAU a un nodo SGSN objetivo, la demanda RAU incluye un KSI, un identificador de identidad temporal, y así sucesivamente, que se memorizan por el equipo UE.

En la etapa 2, el nodo SGSN objetivo demanda un parámetro de seguridad desde una entidad MME original, y la demanda incluye el identificador TMSI obtenido a partir del equipo UE.

En la etapa 2a, la entidad MME original realiza una derivación de claves, y se derivan las claves CK_{ps}' e IK_{ps}' a partir de una clave raíz Kasme.

En la etapa 3, el nodo SGSN obtiene los parámetros de seguridad enviados por la entidad MME, incluyendo los parámetros de seguridad las claves CK_{ps}' e IK_{ps}' derivadas y un identificador KSI.

En la etapa 3a, se genera un nuevo KSI sobre la base del antiguo KSI y un algoritmo por defecto. O el nodo SGSN objetivo puede asignar un nuevo nombre, tal como KSI_{new} o KSI_{UTRAN}, al nuevo KSI (el nuevo nombre es diferente de un nombre del antiguo KSI que se utiliza en una red EUTRAN, utilizándose KSI_{UTRAN} en la red objetivo).

En la etapa 4, de modo opcional, si el KSI enviado desde el equipo UE en la etapa 1 es 111 y debido a otros requisitos operativos, se inicia un nuevo proceso AKA. Puede generarse también un nuevo KSI.

En la etapa 5, el nodo SGSN envía una orden de modo de seguridad que incluye las claves CK_{ps}' e IK_{ps}' derivadas obtenidas desde la entidad MME original y los algoritmos UEAs y UIAs permitidos por el nodo SGSN.

En la etapa 6, un controlador RNC selecciona un algoritmo UEA final y un algoritmo UIA final, y envía la orden de módulo orden de control seguridad al equipo UE.

En la etapa 7, el equipo UE deriva las claves CK_{ps}' e IK_{ps}' desde la clave raíz Kasme.

En la etapa 7a, se genera un nuevo KSI sobre la base del KSI antiguo y un algoritmo por defecto.

En la etapa 8, el equipo UE envía un mensaje de modo de seguridad completo.

En la etapa 9, el controlador RNC transfiere el mensaje de modo de seguridad completo al nodo SGSN.

En la etapa 10, el nodo SGSN envía un mensaje de aceptación de RAU (con protección de integridad) al equipo UE, incluyendo el mensaje de aceptación de RAU el nuevo KSI obtenido en la etapa 2b.

En la etapa 11, el equipo UE recibe el mensaje de aceptación de RAU y reenvía un mensaje de RAU completo al nodo SGSN.

El efecto de la forma de realización del método es el mismo que el de la forma de realización ilustrada en la Figura 15 y por ello no se describe aquí de nuevo.

En las sexta y séptima formas de realización, los escenarios operativos de la “transferencia” de un terminal de usuario en el estado inactivo (movilidad inactiva) se ilustran a este respecto. El método para poner en práctica una transferencia de un terminal de usuario en un estado activo (una transferencia activa) puede realizarse de forma análoga y por ello no se describe aquí de nuevo.

En una octava forma de realización, para la desincronización de seguridad de red que ya se produce, se da a conocer un método de subsanamiento. Según se ilustra en la Figura 18, el método incluye las etapas siguientes:

En la etapa 1801, un parámetro de seguridad en un terminal no coincide con el parámetro de seguridad de una red,

y se produce una desincronización de seguridad de red.

En la etapa 1802, el terminal rechaza la información recibida.

En la etapa 1803, la red no recibe ningún mensaje de respuesta procedente del terminal dentro de un periodo de tiempo predeterminado.

En la etapa 1804, la red inicia un proceso de reautenticación.

La Figura 19 es un diagrama de flujo de señalización en conformidad con la forma de realización de la presente invención. Se incluyen las etapas siguientes:

En la etapa 1, una Estación Móvil (MS) de un usuario inicia una demanda de conexión y se establece una conexión de control de recursos de radio (RRC) entre la estación móvil MS y un controlador de red de radio de servicio (SRNC).

En la etapa 2, la estación MS envía un mensaje de demanda de conexión a un nodo SGSN, y el mensaje de demanda incluye un identificador KSI que ya existe en la estación móvil MS.

En la etapa 3, la red compara un identificador KSI' correspondiente a una clave CK y una clave IK localmente memorizadas con el KSI recibido, y comprueba que los dos identificadores KSIs son los mismos, y de este modo, se considera que la red y el terminal memorizan las mismas claves CK e IK. Puede utilizarse el antiguo parámetro de seguridad y no se requiere ningún nuevo proceso de autenticación AKA.

En la etapa 4, el nodo SGSN entrega una orden de modo de seguridad, estando la orden del modo de seguridad protegida en su integridad con la clave IK (la clave IK se memoriza por la red y la red garantiza que el terminal tenga la misma clave IK). La orden del modo de seguridad incluye la indicación de qué algoritmos de seguridad han de utilizarse, el tiempo de inicio de la encriptación y la protección de integridad y un valor del código de autenticación de mensaje (MAC) calculado de la protección de integridad.

En las etapas 5-6, cuando un equipo UE recibe la orden del modo de seguridad, una clave IK' en el terminal se utiliza primero para realizar un control de integridad sobre la orden del modo de seguridad. Sin embargo, debido al hecho de que la clave IK no es igual a la clave IK', un código MAC' calculado por el terminal con la clave IK' no es igual al valor MAC incluido en la orden del modo de seguridad. El terminal comprueba si ha fallado la integridad de la orden del modo de seguridad, y de este modo, el terminal rechaza la orden del modo de seguridad.

En las etapas 7-8, puesto que la red no recibe ninguna respuesta, la red envía repetidamente la orden del modo de seguridad dentro de un determinado periodo de tiempo hasta terminar el tiempo de espera.

En la etapa 9, se inicia un proceso AKA de reautenticación.

Con el método dado a conocer en esta forma de realización, se evita la desincronización de seguridad de red.

En una forma de realización, la presente invención da a conocer, además, un método para resolver el problema de la desincronización de seguridad de red, que incluye las etapas siguientes:

Una red realiza la coincidencia de los parámetros de seguridad.

La red envía la información de la orden del modo de seguridad inicial a un terminal.

La red no recibe ningún mensaje de respuesta desde el terminal dentro de un periodo de tiempo predeterminado.

La red inicia un proceso de reautenticación.

Con el método dado a conocer en la forma de realización de la presente invención, puede resolverse el problema de desincronización de seguridad de red.

En una novena forma de realización, en un estado inactivo, haciendo referencia a un diagrama de flujo de señalización ilustrado en la Figura 23, un equipo UE permanece primero en una red UTRAN y se completa un proceso AKA. Después de que se realice el proceso AKA en la red UTRAN, un módulo USIM memoriza una clave CK_{ps} y una clave IK_{ps} pertinentes para el contexto de seguridad de la red de UTRAN y un identificador KSI. Cuando el equipo UE se desplaza desde la red UTRAN a una red EUTRAN, el método incluye las etapas siguientes:

En la etapa 1, un equipo UE envía una demanda de TAU a una entidad MME objetivo, la demanda de TAU incluye un identificador KSI, un identificador de identidad temporal, y así sucesivamente, que se memorizan por el equipo UE.

En la etapa 2, la entidad MME objetivo demanda un parámetro de seguridad desde un nodo SGSN original, y la demanda incluye el identificador de identidad temporal obtenido por el equipo UE.

En la etapa 2a, la entidad MME obtiene los parámetros de seguridad enviados por el nodo SGSN. Los parámetros de seguridad incluyen una clave CK_{ps}, una clave IK_{ps} y un identificador KSI.

En la etapa 3, la entidad MME objetivo realiza una derivación de claves, una clave Kasme y claves de subcapa K_{NASenc}, K_{NASint} y Kenb a partir de la clave CK_{ps} y la clave IK_{ps}.

En la etapa 4, se inicia un proceso AKA.

En la etapa 5, la entidad MME envía una orden de modo de seguridad, incluyendo la orden del modo de seguridad la clave Kenb derivada obtenida desde la entidad MME y un algoritmo de encriptación de Estrato de No Acceso (NAS) y un algoritmo de protección de integridad de NAS seleccionado por la entidad MME.

En la etapa 6, un nodo eNB selecciona un algoritmo de encriptación de Estrato de Acceso (AS) y un algoritmo de protección de integridad de AS, y envía la orden del modo de seguridad al equipo UE.

En la etapa 7, el equipo UE deriva la clave Kasme y una clave de subcapa a partir de las claves CK_{ps} e IK_{ps}.

En la etapa 8, el equipo UE envía un mensaje de modo de seguridad completo.

En la etapa 9, el nodo eNB transfiere el mensaje de modo de seguridad completo a la entidad MME.

En la etapa 10, la entidad MME envía un mensaje de aceptación de TAU (con protección de integridad) al equipo UE.

En la etapa 11, el equipo UE recibe el mensaje de aceptación de TAU y reenvía un mensaje de TAU completo a la entidad MME.

En la etapa 12, el equipo UE establece un identificador KSI en un módulo USIM a un valor no válido “111”.

En esta forma de realización, el identificador KSI en el módulo USIM se establece a 111, lo que indica que actualmente ninguna clave CK_{ps}’ ni IK_{ps}’ es válida, de modo que en el proceso posterior (tal como la nueva activación del equipo UE o que el UE realice una transferencia entre redes), se inicia un nuevo proceso AKA y se establece un nuevo parámetro de seguridad. A modo de ejemplo, después de que un equipo UE se desplace desde una red EUTRAN a una red UTRAN se derivan una nueva clave CK_{ps}’ y una nueva clave IK_{ps}’ en un equipo ME. Cuando el equipo UE está en la red UTRAN, el equipo ME es desactivado. Cuando se vuelve a activar el equipo ME, puesto que el módulo USIM no tiene ningún parámetro de seguridad, un mensaje de capa 3 (según se ilustra en la Figura 19) enviado por el equipo UE no incluye un KSI. Cuando la red detecta que el equipo UE no incluye un identificador de contexto de seguridad, se inicia un nuevo proceso AKA. De este modo, se evita la desincronización de contexto de seguridad descrita en el apartado de ANTECEDENTES DE LA INVENCIÓN.

Para una décima forma de realización, es preciso referirse a un diagrama de flujo de señalización ilustrado en la Figura 24. Sobre la base de la novena forma de realización, se añade la etapa 7b. En la etapa 7b, después de que el equipo UE reciba la orden del modo de seguridad y se realice la derivación de claves, el equipo ME envía una instrucción al módulo USIM para suprimir los parámetros de seguridad (las claves CK, IK y KSI) en el módulo USIM.

Preferentemente, la etapa de supresión del parámetro de seguridad en el módulo USIM puede preceder también a la etapa 7.

Por lo tanto, cuando el equipo UE se desplaza a la red UTRAN, y cuando el equipo UE se desactiva y activa de nuevo, puesto que el parámetro de seguridad en el módulo USIM está ya suprimido, el identificador KSI informado por el UE es “111”. Después de que la red efectúe la lectura del KSI, se inicia un nuevo proceso AKA. Se evita así la desincronización del contexto de seguridad.

En la décima forma de realización y en la novena forma de realización, los escenarios operativos de la “transferencia” de un terminal de usuario en el estado inactivo (movilidad inactiva) se ilustran a este respecto. El método para poner en práctica una transferencia de un terminal de usuario en un estado activo (una transferencia activa) puede ser de forma análoga. Haciendo referencia a la Figura 25, en una undécima forma de realización, un proceso de transferencia de un equipo UE en un estado activo (una transferencia activa) se describe con la inclusión de las etapas siguientes:

En la etapa 1, un controlador RNC original envía una decisión de transferencia (a modo de ejemplo, analizando un informe de medición).

En la etapa 2, el controlador RNC envía una demanda de transferencia a un nodo SGSN.

En la etapa 3, el nodo SGSN reenvía la demanda de transferencia a una entidad MME objetivo, y al mismo tiempo, un parámetro de seguridad de un sistema original se incluye en la demanda de transferencia.

En la etapa 4, la entidad MME objetivo deriva una clave Kasme en conformidad con los parámetros de seguridad CK e IK del sistema original, y calcula, además, una clave de subcapa.

En la etapa 5, la entidad MME objetivo entrega la demanda de transferencia a un nodo eNB objetivo.

En la etapa 6, el nodo eNB envía una respuesta de demanda de transferencia a la entidad MME.

En la etapa 7, la entidad MME objetivo reenvía la respuesta de demanda de transferencia al nodo SGSN original.

En la etapa 8, el nodo SGSN original envía una orden de transferencia al controlador RNC.

En la etapa 9, el controlador RNC envía la orden de transferencia al equipo UE.

En la etapa 10, el equipo UE recibe la orden de transferencia, y deriva la clave Kasme desde las claves CK e IK.

En la etapa 10b, se modifican los parámetros en el módulo USIM, que incluye: enviar, por un equipo ME, una instrucción al módulo USIM para demandar la supresión de los parámetros de seguridad CK e IK en el módulo USIM, o estableciendo un KSI en el módulo USIM a un valor no válido “111”.

En la etapa 11, el equipo UE envía un mensaje de demanda completa al nodo eNB.

En la etapa 12, el nodo eNB envía el mensaje de transferencia completa a la entidad MME.

En la etapa 13, la entidad MME reenvía el mensaje de transferencia completa al nodo SGSN.

En la etapa 14, el nodo SGSN reenvía un mensaje de confirmación de transferencia completa a la entidad MME.

En las etapas precedentes, un proceso del parámetro de seguridad en el módulo USIM se añade en la etapa 10b. La etapa 10b puede realizarse también entre la etapa 9 y la etapa 10, lo que no se describe aquí de nuevo. Los efectos ventajosos de la undécima forma de realización son similares a los proporcionados por la novena y décima formas de realización y por ello no se repetirán aquí de nuevo.

En correspondencia con las formas de realización del método, en esta forma de realización, la presente invención da a conocer, además, un dispositivo para evitar la desincronización de seguridad de red. Según se ilustra en la Figura 20, el dispositivo está situado en un lado del terminal de usuario, e incluye una unidad de acceso 201 y una unidad de modificación 202.

La unidad de acceso 201 está configurada para acceder a una red original y para realizar un proceso AKA en la red original.

La unidad de modificación 202 está configurada para establecer un parámetro de seguridad en un módulo USIM a un estado indisponible.

Preferentemente, la unidad de modificación incluye una primera unidad de modificación, una segunda unidad de modificación y una tercera unidad de modificación, o una cuarta unidad de modificación.

La primera unidad de modificación está configurada para establecer un valor de START del módulo USIM a un valor umbral.

La segunda unidad de modificación está configurada para establecer un identificador KSI en el módulo USIM a 111.

La tercera unidad de modificación está configurada para modificar el KSI en el módulo USIM.

La cuarta unidad de modificación está configurada para suprimir una clave CK y una clave IK en el módulo USIM.

Modificando el parámetro de seguridad en el módulo USIM en un terminal, ya no se utiliza el parámetro de seguridad en el módulo USIM (a modo de ejemplo, se suprime la clave CK y la clave IK). Cuando el terminal (una parte de ME) se desactiva y activa de nuevo, el equipo ME efectúa la lectura del parámetro de seguridad desde el módulo USIM, pero en ese momento operativo, no está disponible ningún parámetro de seguridad. Se inicia un nuevo proceso de autenticación, y no se produce la situación de desincronización de seguridad de la red.

Preferentemente, el dispositivo incluye, además, una unidad de envío, configurada para enviar un KSI modificado por la unidad de modificación a la red para la comparación de parámetros de seguridad.

Cuando un usuario se registra a la entrada de una red, el KSI modificado se envía a la red para comparación de parámetros de seguridad. Si se comprueba una incompatibilidad durante la comparación, se inicia un nuevo proceso de autenticación, y no se produce la situación de desincronización de seguridad.

En una forma de realización, la presente invención da a conocer, además, un terminal para evitar la desincronización de seguridad de red. El terminal incluye cualquiera de los dispositivos precedentes en el lado del terminal para evitar la desincronización de seguridad de la red.

Haciendo referencia a la Figura 21, en una forma de realización, la presente invención da a conocer un dispositivo para evitar la desincronización de seguridad de red, estando situado el dispositivo en la red y el dispositivo incluye una unidad de recepción 211, una unidad de modificación 212 y una unidad de notificación 213.

La unidad de recepción 211 está configurada para recibir un KSI durante una transferencia de red.

La unidad de modificación 212 está configurada para modificar el KSI.

La unidad de notificación 213 está configurada para enviar información de notificación para notificar un nuevo identificador de red.

Con el dispositivo dado a conocer en esta forma de realización, la red recibe el KSI y modifica el KSI.

Cuando la red es una red original, y cuando se realiza una transferencia de red, se envía un KSI modificado a una red objetivo por intermedio de la unidad de notificación, y la red objetivo utiliza el KSI recibido como un nuevo KSI.

Cuando la red es una red objetivo, puede modificarse un KSI recibido de una red original, y el KSI modificado se utiliza como un nuevo KSI y un terminal de usuario es objeto de notificación por intermedio de la unidad de notificación.

Preferentemente, la unidad de modificación incluye, además, un módulo de algoritmo.

El módulo de algoritmo está configurado para obtener un nuevo KSI realizando el cálculo en conformidad con un KSI antiguo.

Y/o, la unidad de algoritmo está configurada para asignar un nuevo nombre de un nuevo KSI a un KSI antiguo.

O bien, la unidad de algoritmo está configurada para demandar un nuevo KSI desde una entidad de red.

O bien, la unidad de algoritmo está configurada para obtener un nuevo KSI realizando un cálculo en conformidad con un algoritmo preestablecido.

El KSI de la red original se modifica con diferentes unidades de algoritmos utilizando diferentes algoritmos. La modificación puede realizarse en la red objetivo y puede realizarse también en la red original.

En una forma de realización, la presente invención da a conocer, además, un equipo de red para evitar la desincronización de seguridad de red, y el equipo incluye el dispositivo precedente en la red para evitar la desincronización de seguridad de red.

En una forma de realización, la presente invención da a conocer un dispositivo para subsanar la desincronización de seguridad de red. Según se ilustra en la Figura 22, el dispositivo está situado en la red, y el dispositivo incluye una unidad de recepción 221, una unidad de adaptación de coincidencia 222, una unidad de envío 223 y una unidad de iniciación 224.

La unidad de recepción 221 está configurada para recibir un parámetro de seguridad enviado por un terminal de usuario.

La unidad de adaptación de coincidencia 222 está configurada para la adaptación de coincidencia del parámetro de seguridad recibido con su propio parámetro de seguridad.

La unidad de envío 223 está configurada para enviar información de seguridad al terminal de usuario.

La unidad de iniciación 224 está configurada para reiniciar el proceso de AKA si no se recibe ningún mensaje de respuesta procedente del terminal de usuario dentro de un periodo de tiempo predeterminado.

Con el dispositivo dado a conocer en la forma de realización de la presente invención, pueden tomarse medidas de subsanamiento correspondientes cuando se produce una desincronización de seguridad de red. Cuando la red no recibe ningún mensaje de respuesta enviado por el equipo UE dentro de un periodo de tiempo predeterminado, la red inicia activamente un proceso AKA, de modo que se evite el fallo operativo del usuario para acceder a la red debido a la desincronización de seguridad de red y se mejora así la disponibilidad de red en los escenarios operativos relacionados con la transferencia.

REIVINDICACIONES

1. Un método para evitar una desincronización de seguridad de una red, que comprende:

realizar (1101) por un terminal de usuario, un proceso de acuerdo de autenticación y de clave, AKA, en una red original, en donde la red original es una red de acceso de radio terrestre universal evolucionada, EUTRAN;

realizar (1102), por el terminal de usuario, una transferencia de red desde la red original a una nueva red, en donde la nueva red es una red de acceso de radio terrestre universal, UTRAN;

realizar (1102), por el terminal de usuario, una derivación de clave en la nueva red, en donde una clave de cifrado, CK_{ps}', y una clave de integridad, IK_{ps}', se derivan a partir de una clave raíz, Kasme, de un dominio de paquetes conmutados; y

establecer un parámetro de seguridad memorizado en un módulo de identidad universal de abonado, USIM, en el terminal de usuario como estando indisponible, incluyendo la supresión de una clave CK_{ps} original y de una clave IK_{ps} original en el módulo USIM después de que la clave CK_{ps}' y la clave IK_{ps}' sean derivadas cuando el terminal de usuario realiza una transferencia desde la red EUTRAN a la red UTRAN.

2. El método según la reivindicación 1, en donde el método comprende, además:

sincronizar (1102), por el terminal de usuario, con la nueva red.

3. El método según cualquiera de las reivindicaciones 1 a 2, en donde la transferencia de red comprende:

una transferencia del terminal de usuario en un estado activo entre diferentes redes; o

la movilidad del terminal de usuario en un estado inactivo entre diferentes redes.

4. Un dispositivo para evitar la desincronización de seguridad de una red, situado en un terminal de usuario, comprendiendo dicho dispositivo:

una unidad, configurada para realizar un proceso de acuerdo de autenticación y de clave, AKA, en una red original, en donde la red original es una red de acceso de radio terrestre universal evolucionada, EUTRAN;

una unidad de transferencia, configurada para realizar una transferencia de red del terminal de usuario desde la red original a una nueva red, en donde la nueva red es una red de acceso de radio terrestre universal, UTRAN, y realizar una derivación de clave en la nueva red, en donde la unidad de transferencia está configurada, además, para derivar una clave de cifrado, CK_{ps}', y una clave de integridad IK_{ps}', a partir de una clave raíz, Kasme, de un dominio de paquetes conmutados;

una unidad de modificación, configurada para modificar un parámetro de seguridad memorizado en un módulo de identidad universal de abonado, USIM, en el terminal de usuario como estando indisponible mediante la supresión de una clave CK_{ps} original y una clave IK_{ps} original en el módulo USIM después de que las claves CK_{ps}' e IK_{ps}' sean derivadas cuando el terminal de usuario realiza una transferencia desde la red EUTRAN a la red UTRAN.

5. Un terminal de usuario, que comprende el dispositivo según la reivindicación 4.

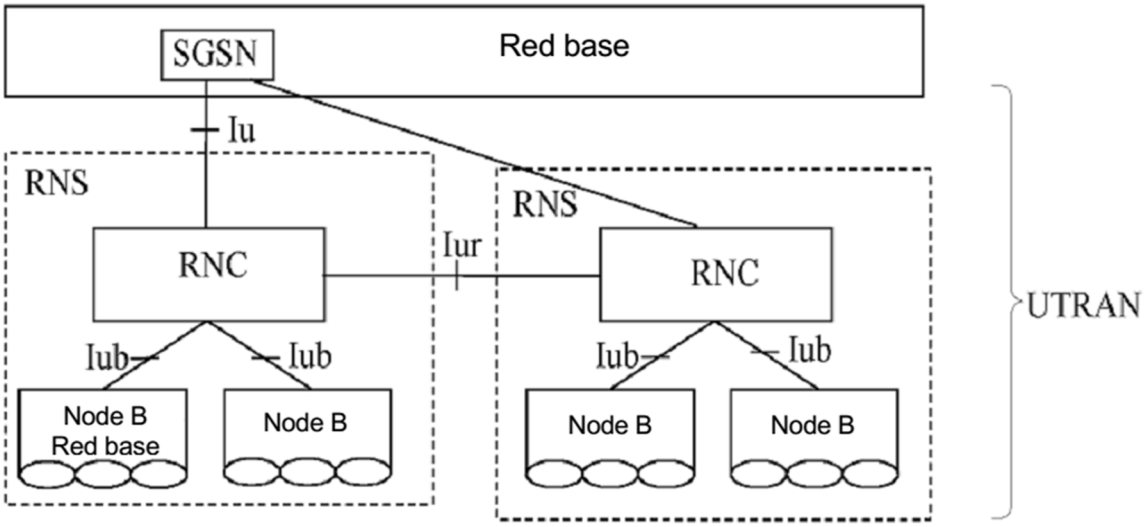
SGSN
Red base
Iu
RNS
RNC
Iur
RNS
RNC
UTRAN
Iub
Iub
Iub
Iub
Node B
Red base
Node B
Node B
Node B

FIG. 1

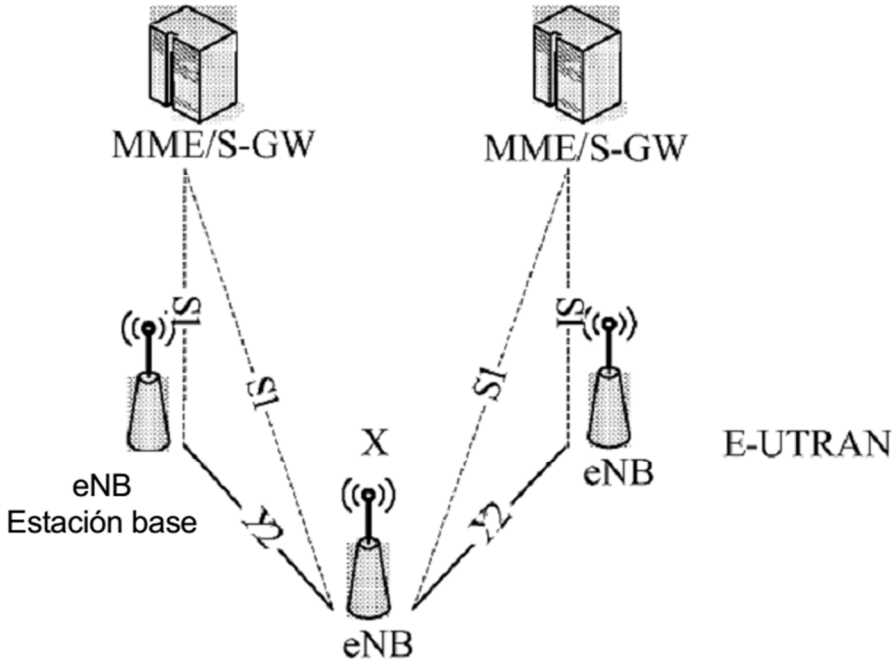
MME/S-GW
MME/S-GW
S1
S1
S1
S1
X
X2
X2
eNB
Estación base
eNB
eNB
E-UTRAN

FIG. 2

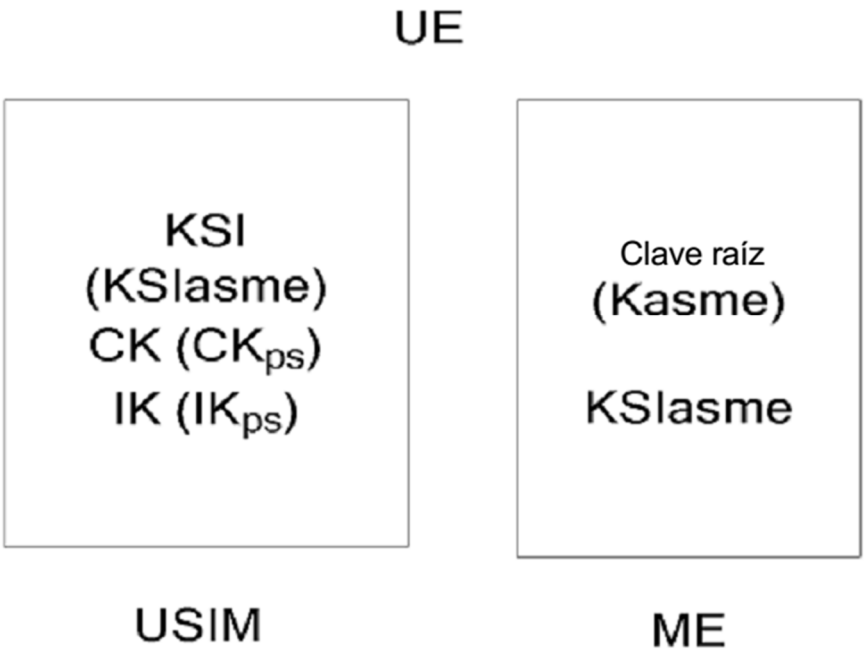
UE
KSI
(KSIasme)
CK (CKps)
IK (IKps)
Clave raíz
(Kasme)
KSIasme
USIM
ME

FIG. 3

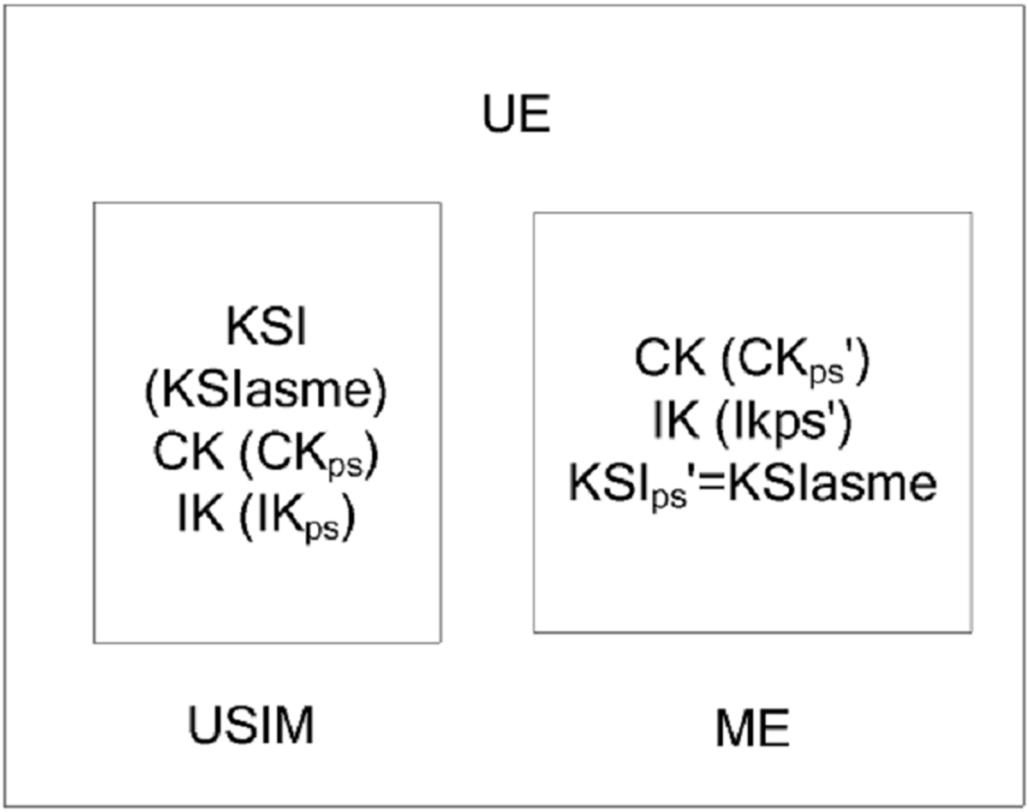
UE
KSI
(KSIasme)
CK (CKps)
IK (IKps)
CK (CKps')
IK (Ikps')
KSIps'=KSIasme
USIM
ME

FIG. 4

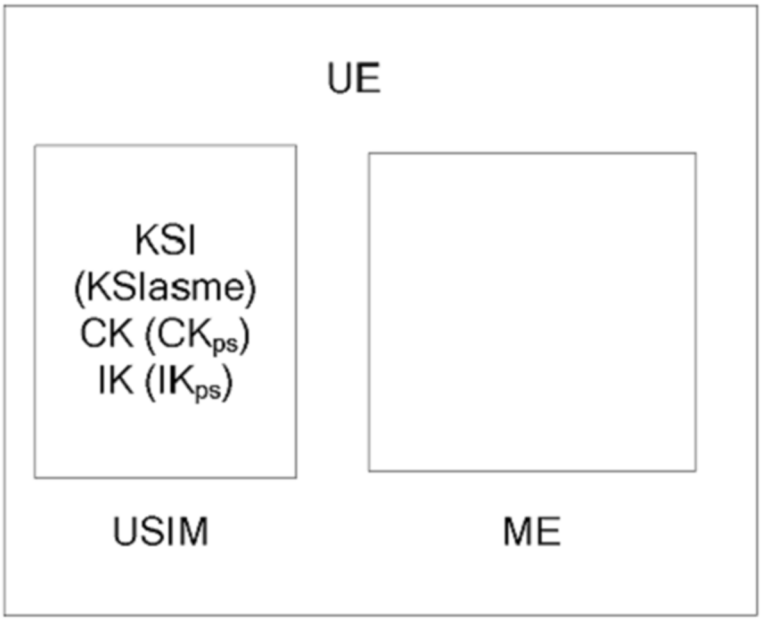
UE
KSI
(KSIasme)
CK (CKps)
IK (IKps)
USIM
ME

FIG. 5

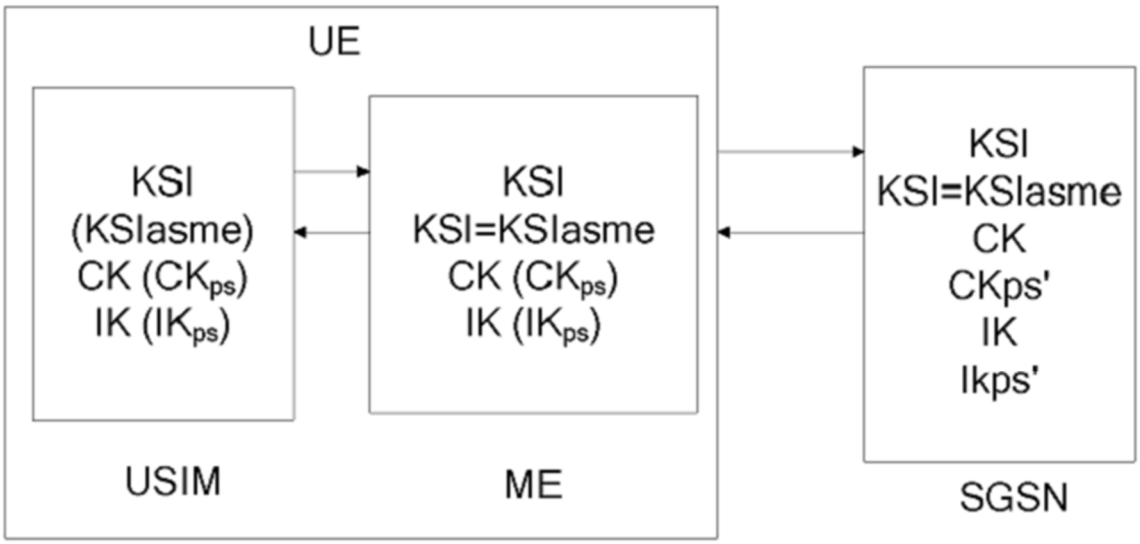
UE
KSI
(KSIasme)
CK (CKps)
IK (IKps)
KSI
KSI=KSIasme
CK (CKps)
IK (IKps)
KSI
KSI=KSIasme
CK
CKps'
IK
Ikps'
USIM
ME
SGSN

FIG. 6

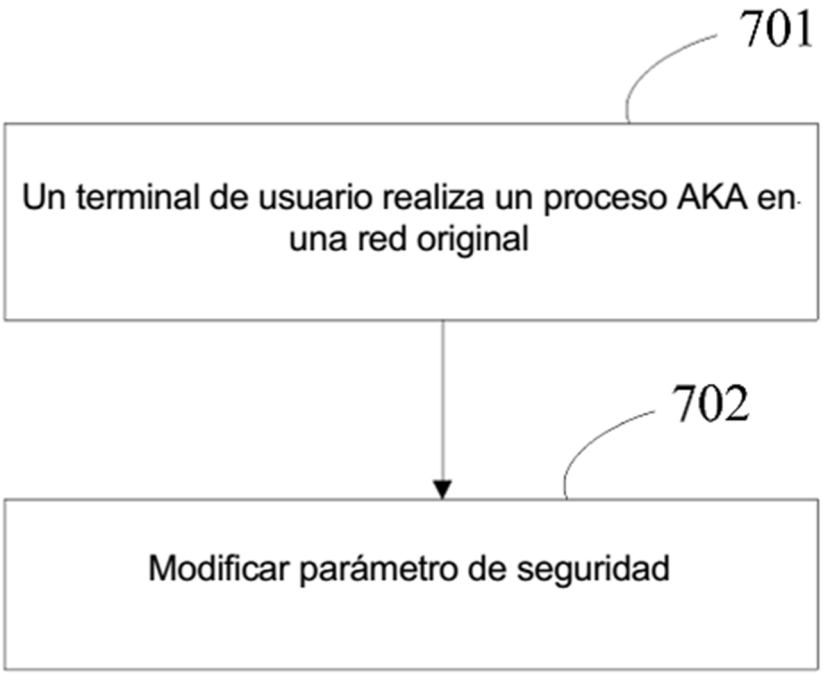
701
Un terminal de usuario realiza un proceso AKA en una red original
702
Modificar parámetro de seguridad

FIG. 7

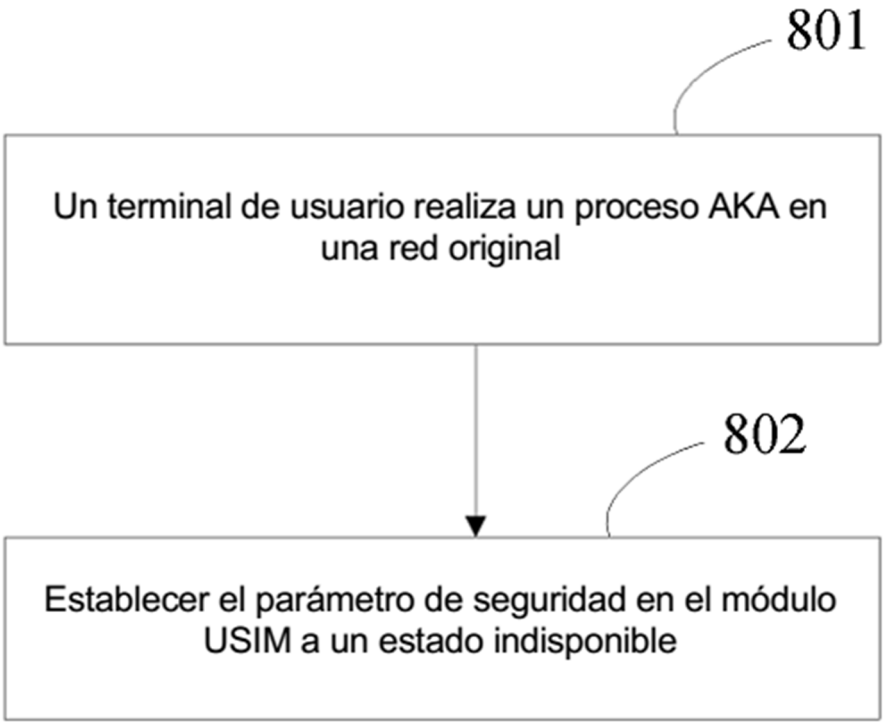
801
Un terminal de usuario realiza un proceso AKA en una red original
802
Establecer el parámetro de seguridad en el módulo USIM a un estado indisponible

FIG. 8

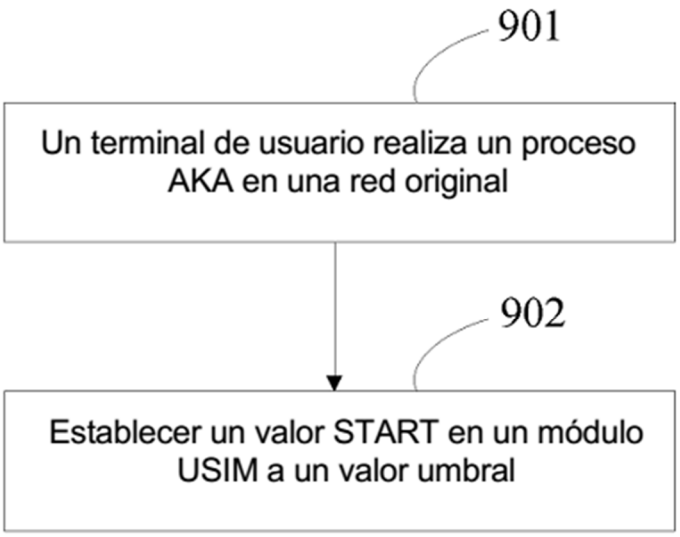
901
Un terminal de usuario realiza un proceso AKA en una red original
902
Establecer un valor START en un módulo USIM a un valor umbral

FIG. 9

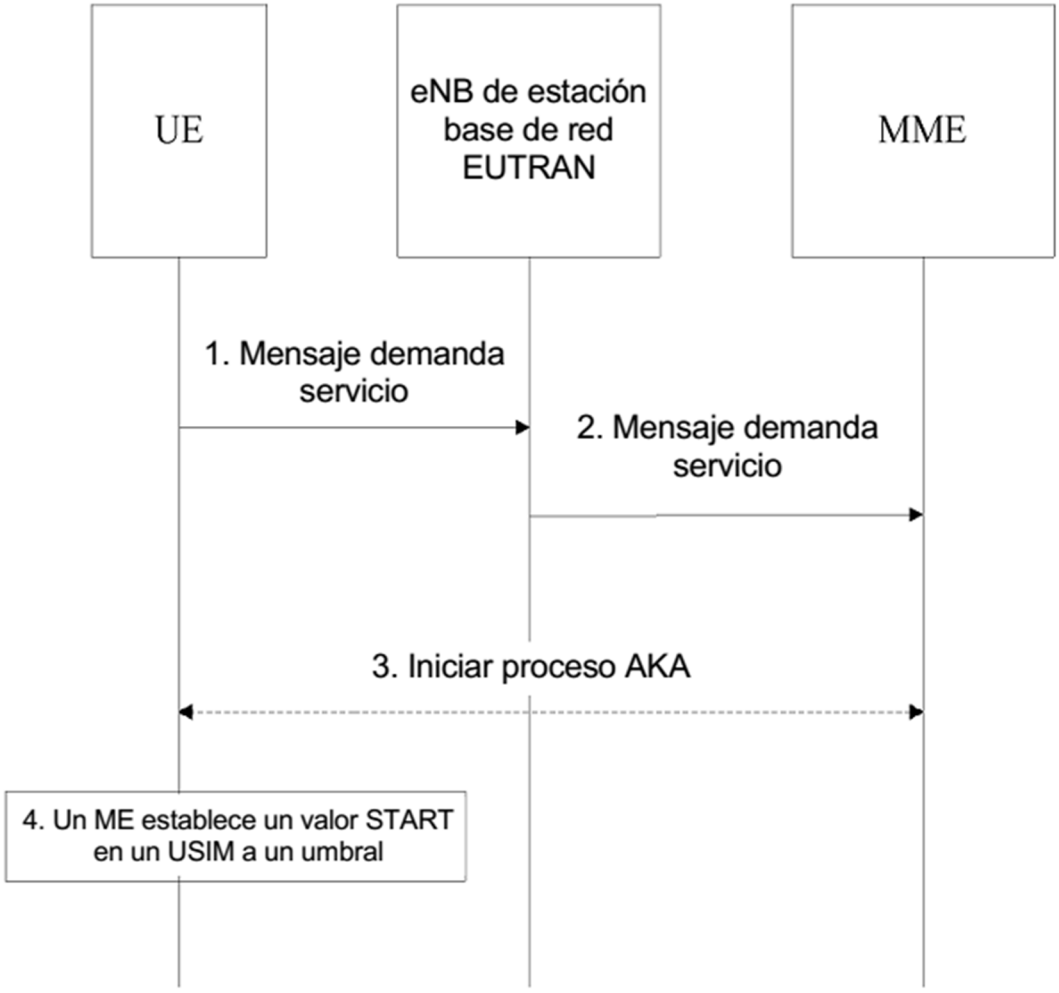
UE
eNB de estación base de red EUTRAN
MME
1. Mensaje demanda servicio
2. Mensaje demanda servicio
3. Iniciar proceso AKA
4. Un ME establece un valor START en un USIM a un umbral

FIG. 10

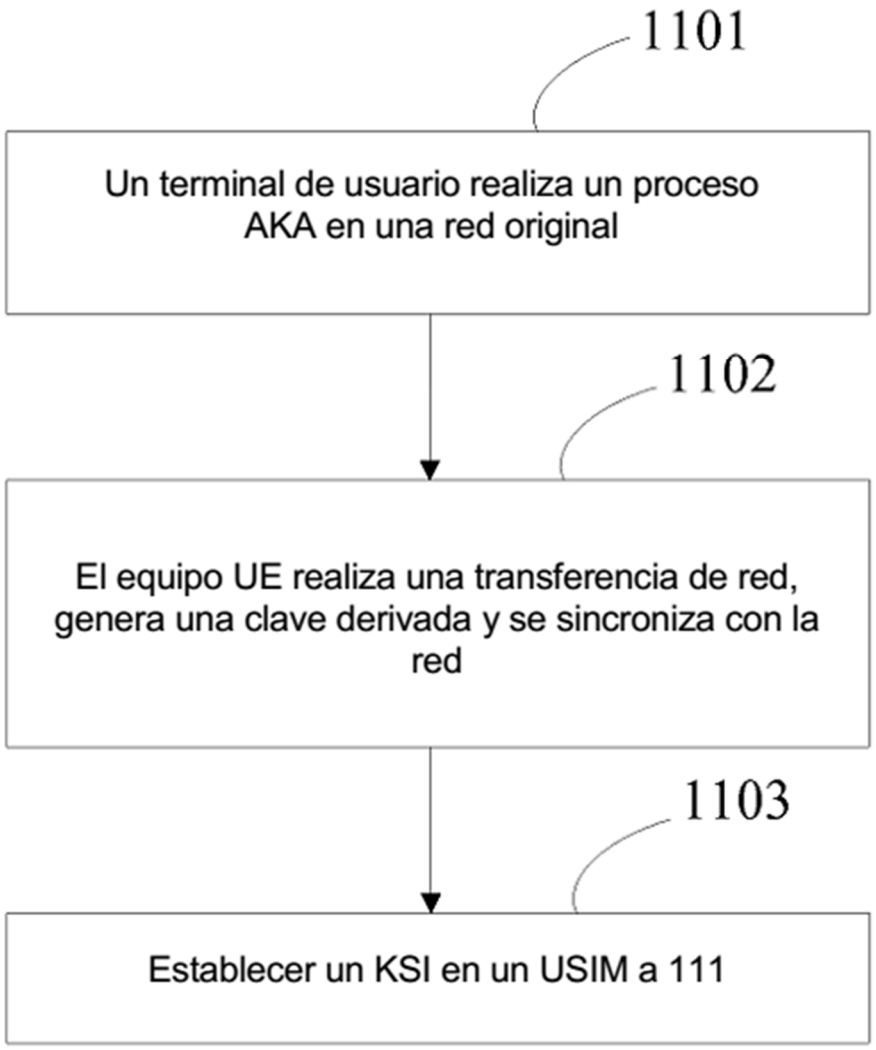
1101
Un terminal de usuario realiza un proceso AKA en una red original
1102
El equipo UE realiza una transferencia de red, genera una clave derivada y se sincroniza con la red
1103
Establecer un KSI en un USIM a 111

FIG. 11

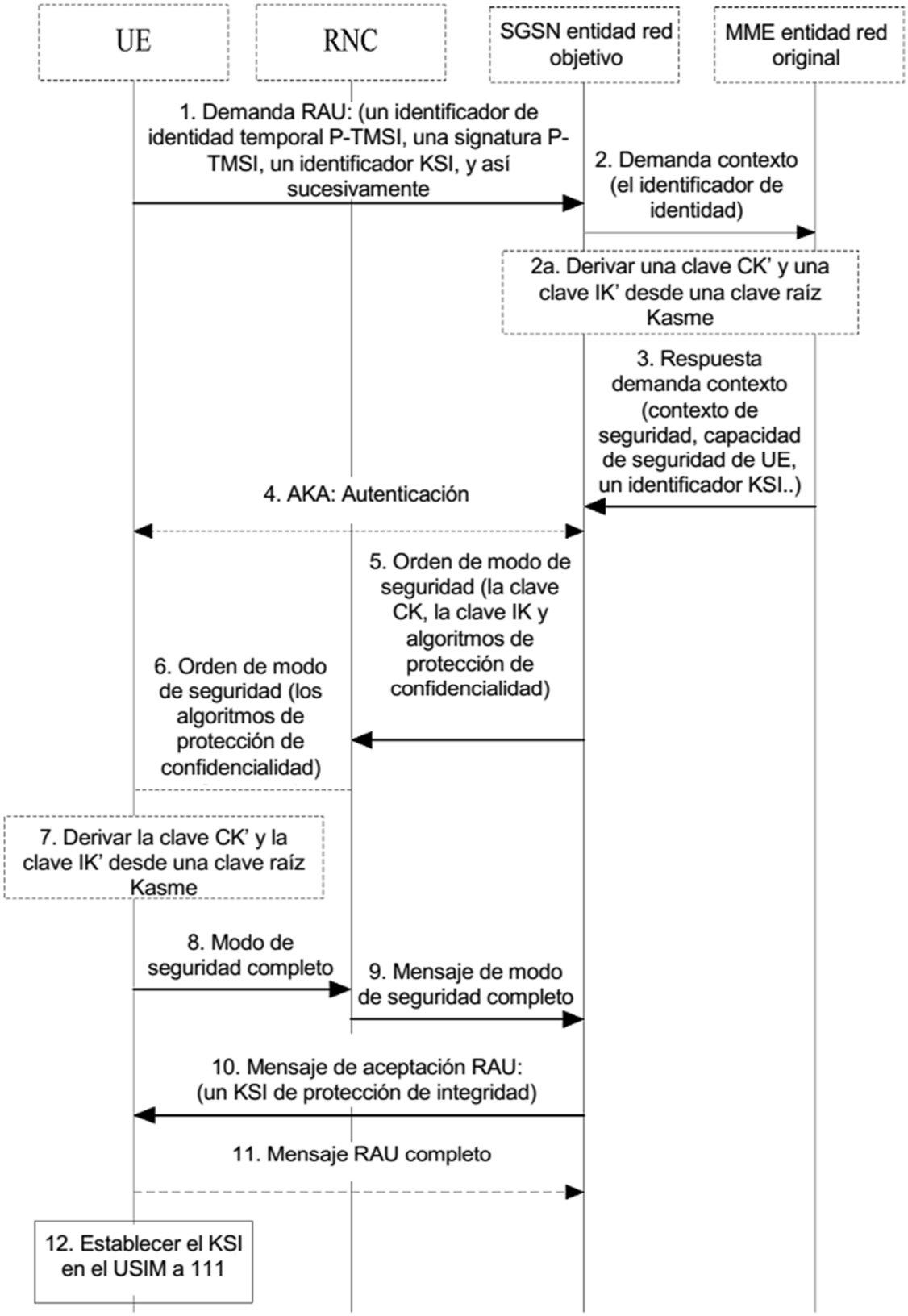
UE
RNC
SGSN entidad red objetivo
MME entidad red original
1. Demanda RAU: (un identificador de identidad temporal P-TMSI, una signatura P-TMSI, un identificador KSI, y así sucesivamente
2. Demanda contexto (el identificador de identidad)
2a. Derivar una clave CK' y una clave IK' desde una clave raíz Kasme
3. Respuesta demanda contexto (contexto de seguridad, capacidad de seguridad de UE, un identificador KSI..)
4. AKA: Autenticación
5. Orden de modo de seguridad (la clave CK, la clave IK y algoritmos de protección de confidencialidad)
6. Orden de modo de seguridad (los algoritmos de protección de confidencialidad)
7. Derivar la clave CK' y la clave IK' desde una clave raíz Kasme
8. Modo de seguridad completo
9. Mensaje de modo de seguridad completo
10. Mensaje de aceptación RAU: (un KSI de protección de integridad)
11. Mensaje RAU completo
12. Establecer el KSI en el USIM a 111

FIG. 12

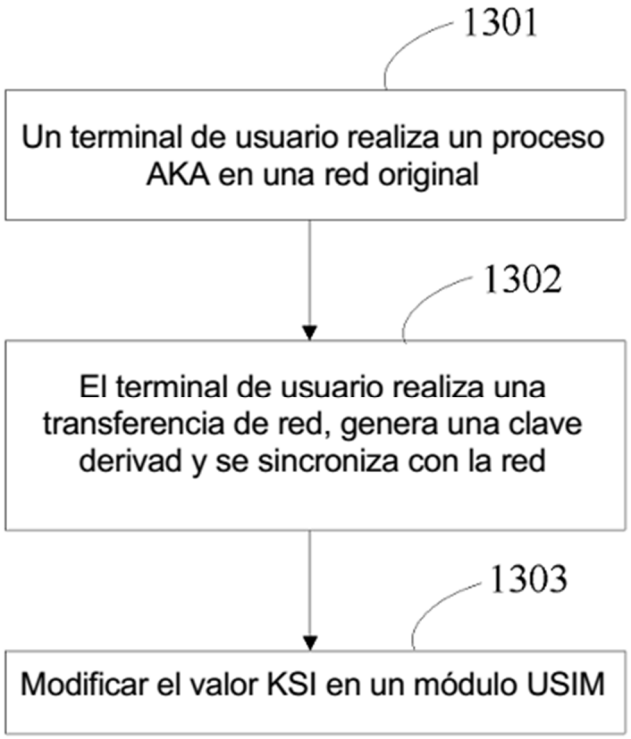
1301
Un terminal de usuario realiza un proceso AKA en una red original
1302
El terminal de usuario realiza una transferencia de red, genera una clave derivad y se sincroniza con la red
1303
Modificar el valor KSI en un módulo USIM

FIG. 13

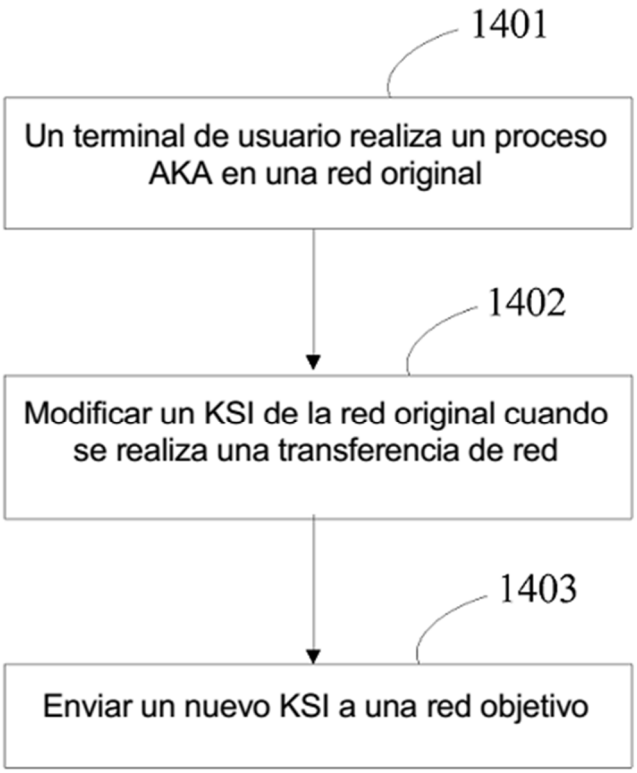
1401
Un terminal de usuario realiza un proceso AKA en una red original
1402
Modificar un KSI de la red original cuando se realiza una transferencia de red
1403
Enviar un nuevo KSI a una red objetivo

FIG. 14

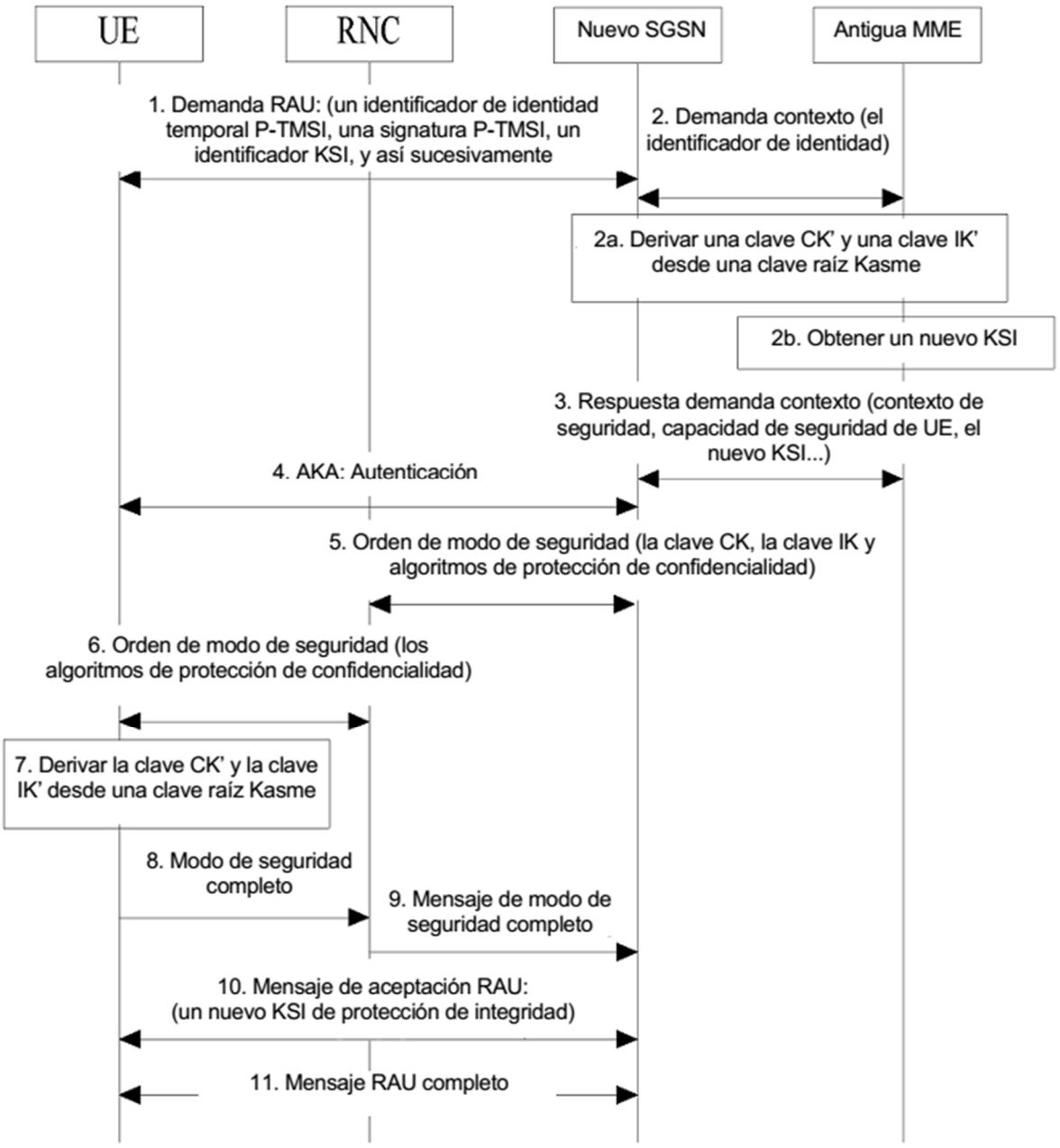
UE
RNC
Nuevo SGSN
Antigua MME
1. Demanda RAU: (un identificador de identidad temporal P-TMSI, una signatura P-TMSI, un identificador KSI, y así sucesivamente
2. Demanda contexto (el identificador de identidad)
2a. Derivar una clave CK' y una clave IK' desde una clave raíz Kasme
2b. Obtener un nuevo KSI
3. Respuesta demanda contexto (contexto de seguridad, capacidad de seguridad de UE, el nuevo KSI...)
4. AKA: Autenticación
5. Orden de modo de seguridad (la clave CK, la clave IK y algoritmos de protección de confidencialidad)
6. Orden de modo de seguridad (los algoritmos de protección de confidencialidad)
7. Derivar la clave CK' y la clave IK' desde una clave raíz Kasme
8. Modo de seguridad completo
9. Mensaje de modo de seguridad completo
10. Mensaje de aceptación RAU: (un nuevo KSI de protección de integridad)
11. Mensaje RAU completo

FIG. 15

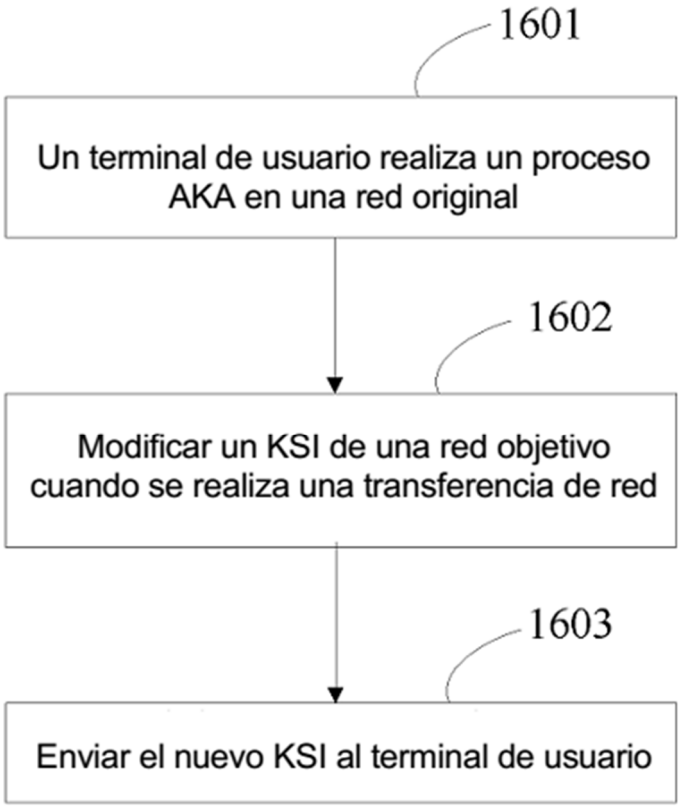
1601
Un terminal de usuario realiza un proceso AKA en una red original
1602
Modificar un KSI de una red objetivo cuando se realiza una transferencia de red
1603
Enviar el nuevo KSI al terminal de usuario

FIG. 16

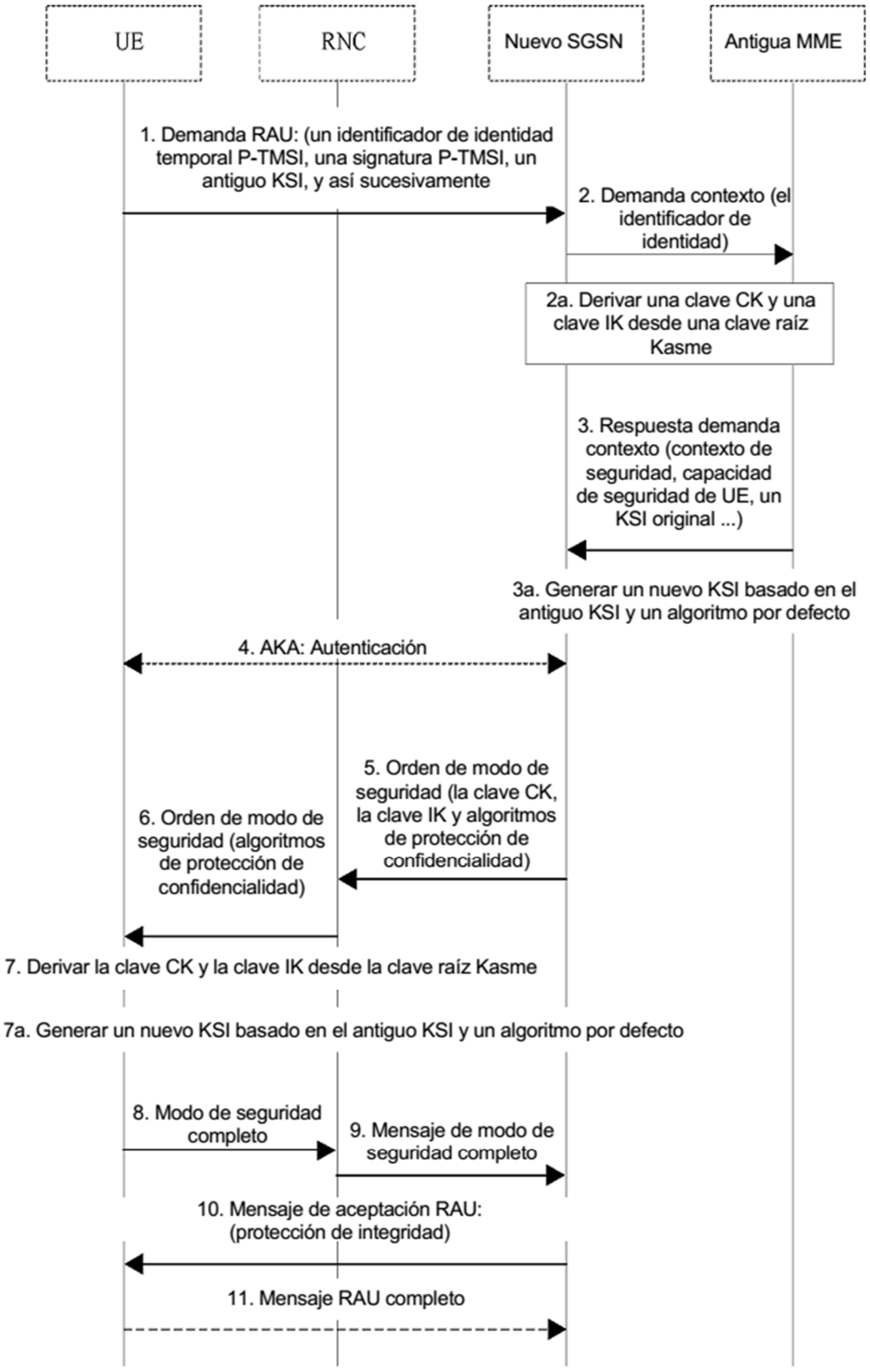
UE
RNC
Nuevo SGSN
Antigua MME
1. Demanda RAU: (un identificador de identidad temporal P-TMSI, una signatura P-TMSI, un antiguo KSI, y así sucesivamente
2. Demanda contexto (el identificador de identidad)
2a. Derivar una clave CK y una clave IK desde una clave raíz Kasme
3. Respuesta demanda contexto (contexto de seguridad, capacidad de seguridad de UE, un KSI original ...)
3a. Generar un nuevo KSI basado en el antiguo KSI y un algoritmo por defecto
4. AKA: Autenticación
5. Orden de modo de seguridad (la clave CK, la clave IK y algoritmos de protección de confidencialidad)
6. Orden de modo de seguridad (algoritmos de protección de confidencialidad)
7. Derivar la clave CK y la clave IK desde la clave raíz Kasme
7a. Generar un nuevo KSI basado en el antiguo KSI y un algoritmo por defecto
8. Modo de seguridad completo
9. Mensaje de modo de seguridad completo
10. Mensaje de aceptación RAU: (protección de integridad)
11. Mensaje RAU completo

FIG. 17

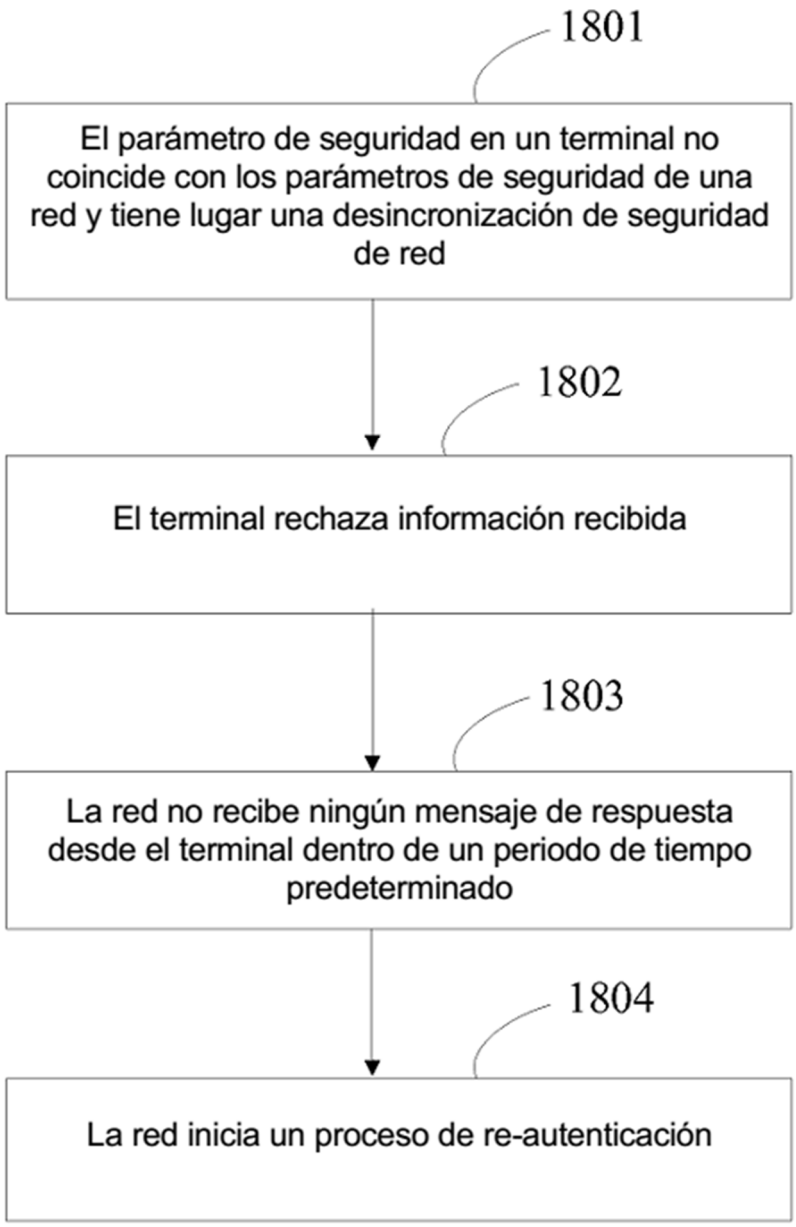
1801
El parámetro de seguridad en un terminal no coincide con los parámetros de seguridad de una red y tiene lugar una desincronización de seguridad de red
1802
El terminal rechaza información recibida
1803
La red no recibe ningún mensaje de respuesta desde el terminal dentro de un periodo de tiempo predeterminado
1804
La red inicia un proceso de re-autenticación

FIG. 18

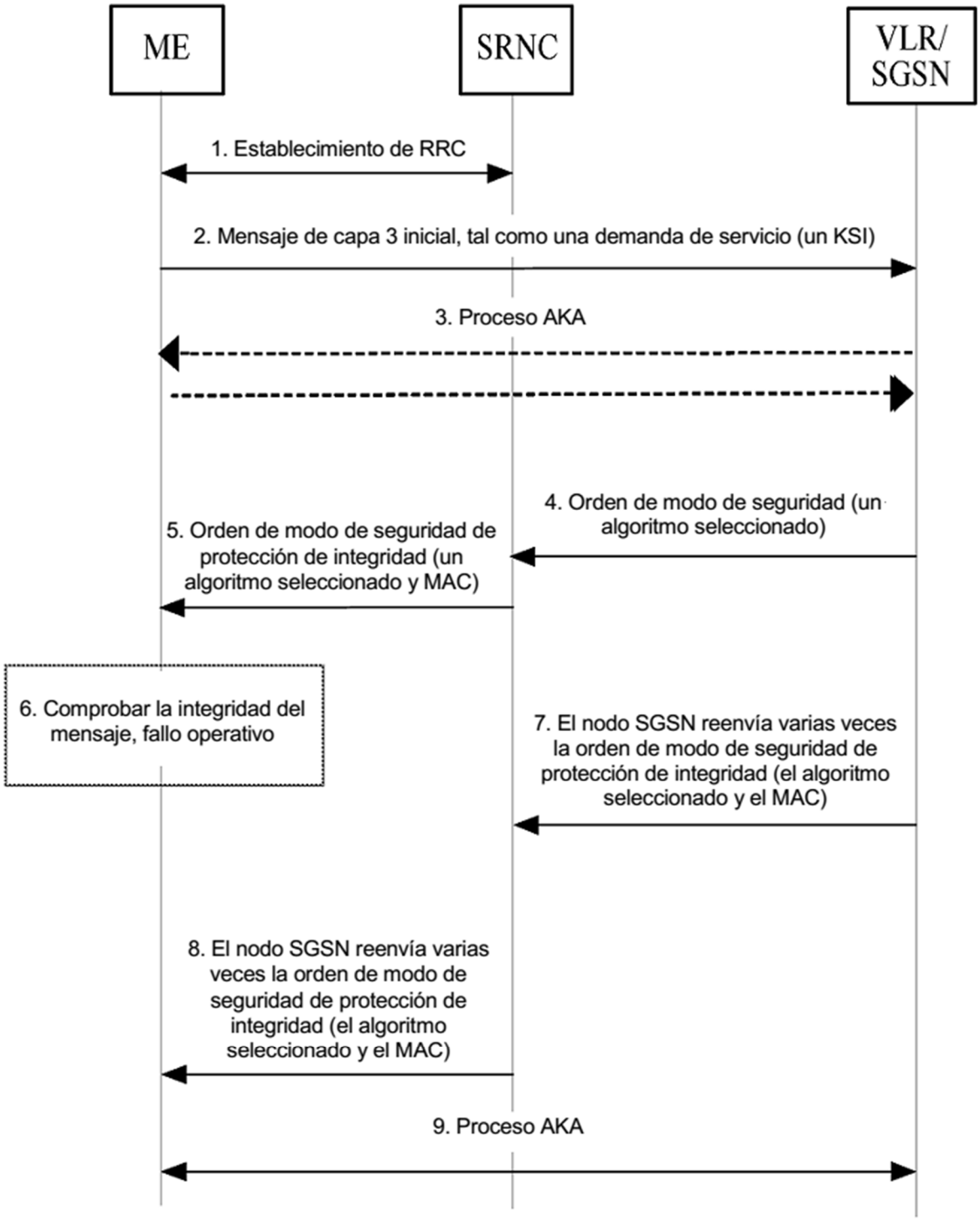
ME
SRNC
VLR/
SGSN
1. Establecimiento de RRC
2. Mensaje de capa 3 inicial, tal como una demanda de servicio (un KSI)
3. Proceso AKA
4. Orden de modo de seguridad (un algoritmo seleccionado)
5. Orden de modo de seguridad de protección de integridad (un algoritmo seleccionado y MAC)
6. Comprobar la integridad del mensaje, fallo operativo
7. El nodo SGSN reenvía varias veces la orden de modo de seguridad de protección de integridad (el algoritmo seleccionado y el MAC)
8. El nodo SGSN reenvía varias veces la orden de modo de seguridad de protección de integridad (el algoritmo seleccionado y el MAC)
9. Proceso AKA

FIG. 19

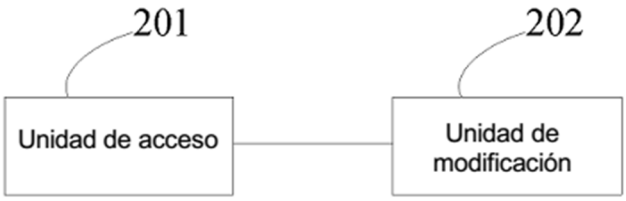

FIG. 20

FIG. 21

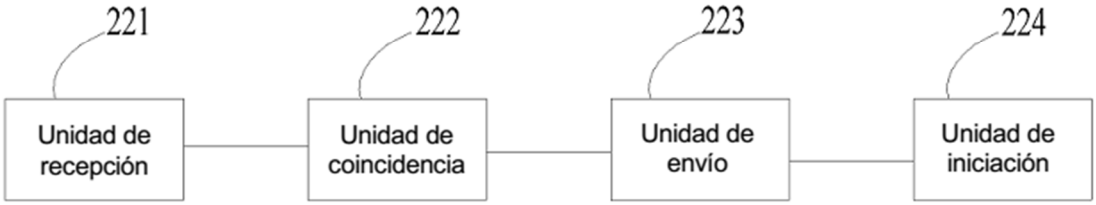

FIG. 22

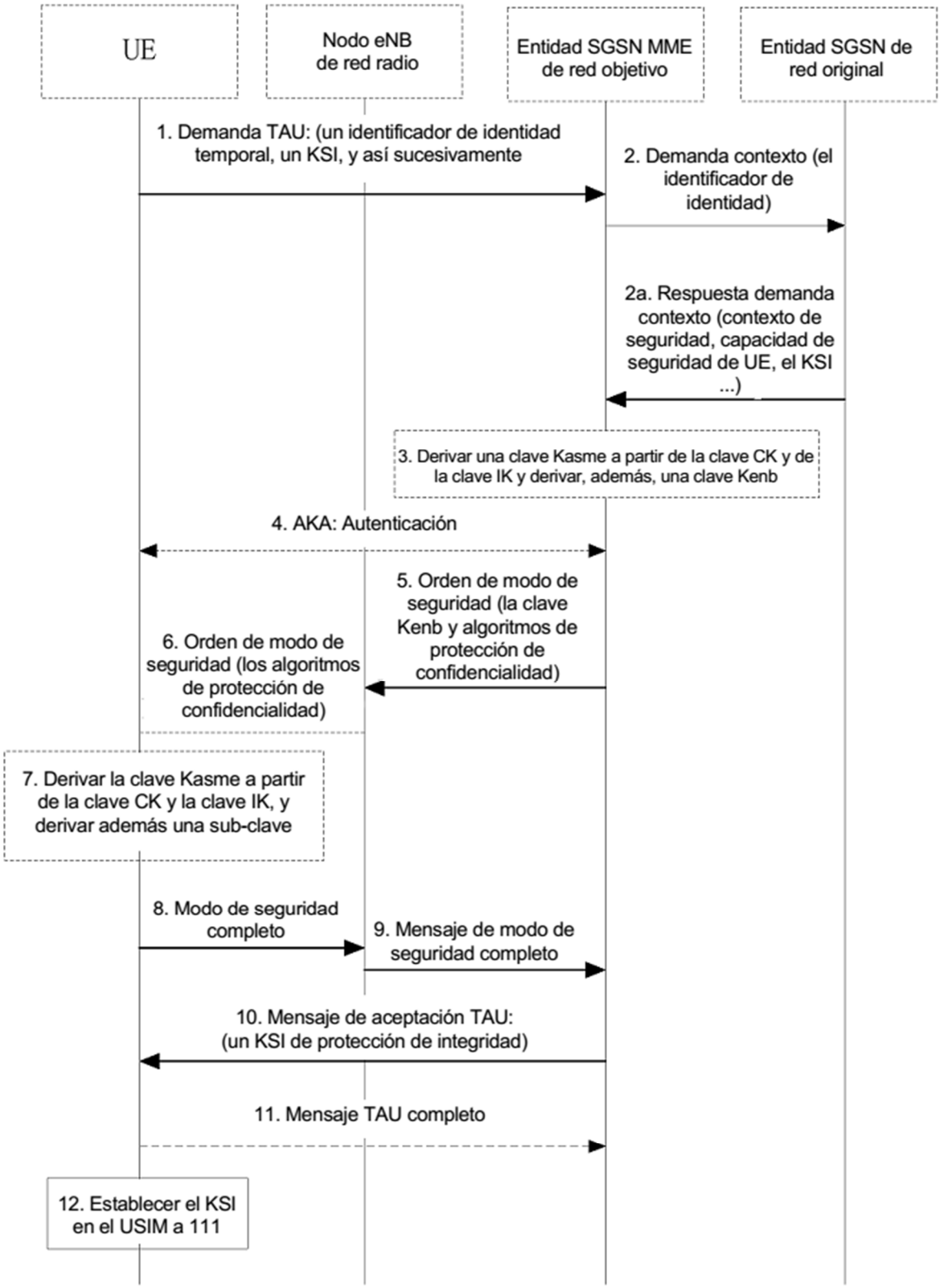
UE
Nodo eNB de red radio
Entidad SGSN MME de red objetivo
Entidad SGSN de red original
1. Demanda TAU: (un identificador de identidad temporal, un KSI, y así sucesivamente
2. Demanda contexto (el identificador de identidad)
2a. Respuesta demanda contexto (contexto de seguridad, capacidad de seguridad de UE, el KSI ...)
3. Derivar una clave Kasme a partir de la clave CK y de la clave IK y derivar, además, una clave Kenb
4. AKA: Autenticación
5. Orden de modo de seguridad (la clave Kenb y algoritmos de protección de confidencialidad)
6. Orden de modo de seguridad (los algoritmos de protección de confidencialidad)
7. Derivar la clave Kasme a partir de la clave CK y la clave IK, y derivar además una sub-clave
8. Modo de seguridad completo
9. Mensaje de modo de seguridad completo
10. Mensaje de aceptación TAU: (un KSI de protección de integridad)
11. Mensaje TAU completo
12. Establecer el KSI en el USIM a 111

FIG. 23

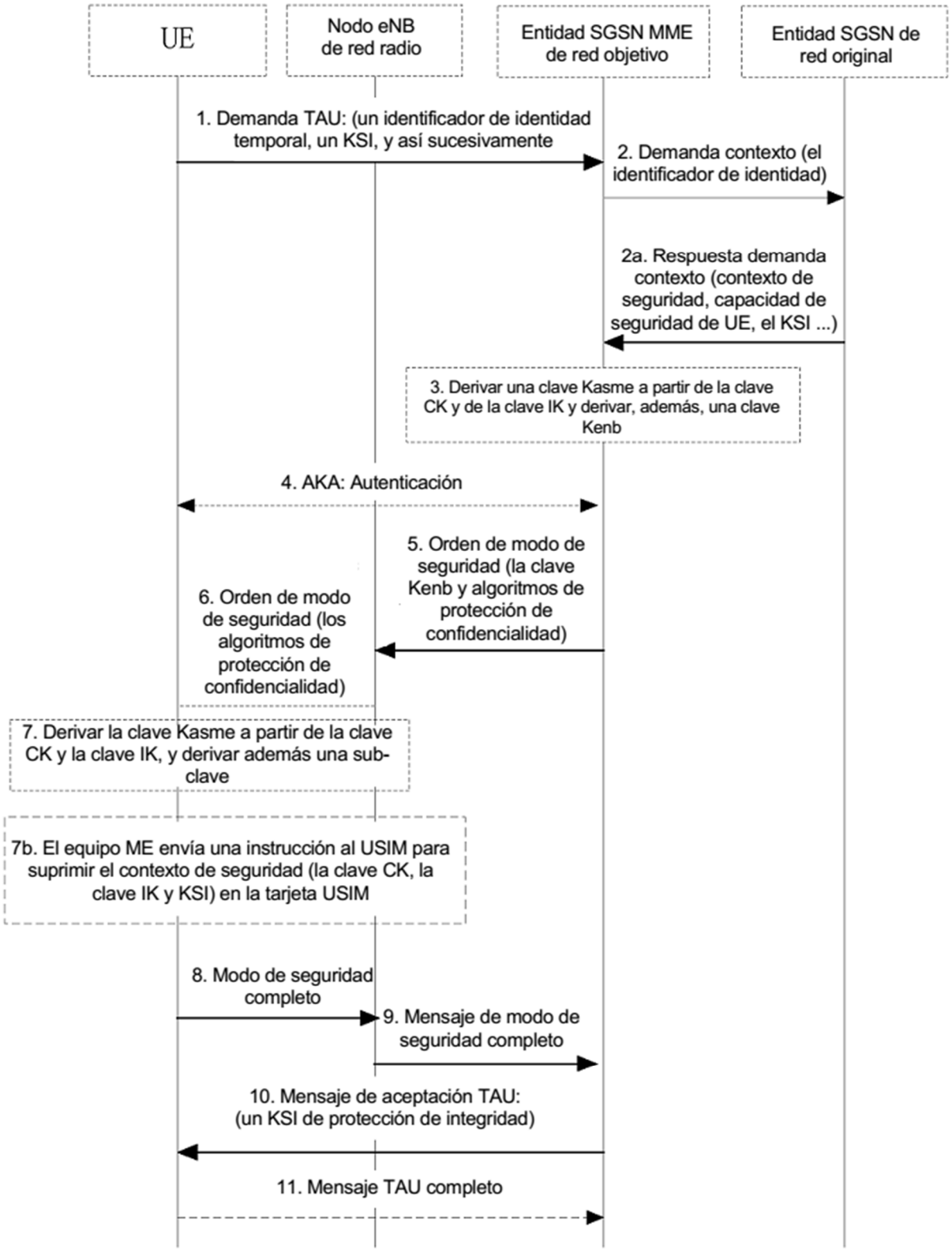
UE
Nodo eNB de red radio
Entidad SGSN MME de red objetivo
Entidad SGSN de red original
1. Demanda TAU: (un identificador de identidad temporal, un KSI, y así sucesivamente
2. Demanda contexto (el identificador de identidad)
2a. Respuesta demanda contexto (contexto de seguridad, capacidad de seguridad de UE, el KSI ...)
3. Derivar una clave Kasme a partir de la clave CK y de la clave IK y derivar, además, una clave Kenb
4. AKA: Autenticación
5. Orden de modo de seguridad (la clave Kenb y algoritmos de protección de confidencialidad)
6. Orden de modo de seguridad (los algoritmos de protección de confidencialidad)
7. Derivar la clave Kasme a partir de la clave CK y la clave IK, y derivar además una sub-clave
7b. El equipo ME envía una instrucción al USIM para suprimir el contexto de seguridad (la clave CK, la clave IK y KSI) en la tarjeta USIM
8. Modo de seguridad completo
9. Mensaje de modo de seguridad completo
10. Mensaje de aceptación TAU: (un KSI de protección de integridad)
11. Mensaje TAU completo

FIG. 24

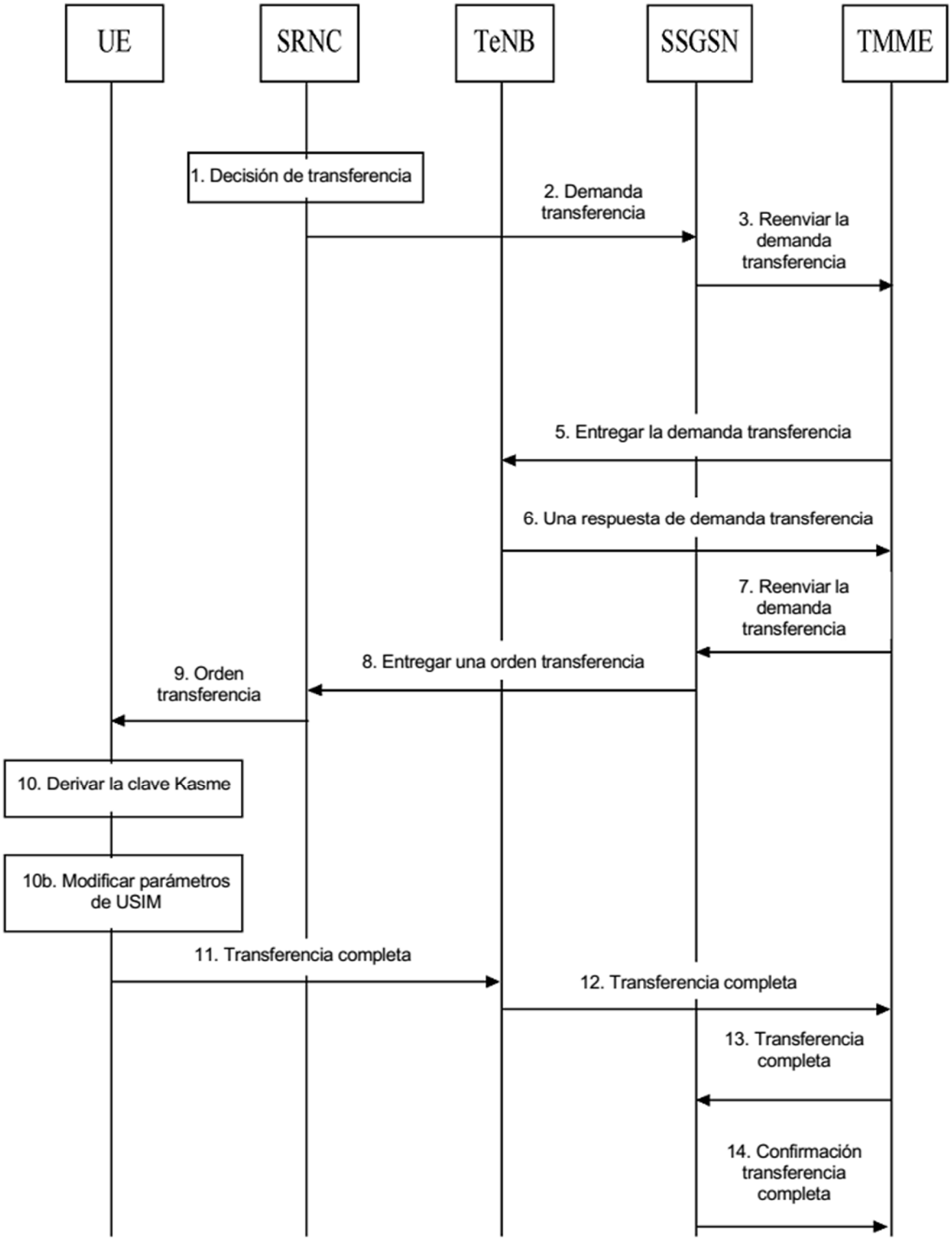
UE
SRNC
TeNB
SSGSN
TMME
1. Decisión de transferencia
2. Demanda transferencia
3. Reenviar la demanda transferencia
5. Entregar la demanda transferencia
6. Una respuesta de demanda transferencia
7. Reenviar la demanda transferencia
8. Entregar una orden transferencia
9. Orden transferencia
10. Derivar la clave Kasme
10b. Modificar parámetros de USIM
11. Transferencia completa
12. Transferencia completa
13. Transferencia completa
14. Confirmación transferencia completa

FIG. 25