(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 659 368**

(51) Int. Cl.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.12.2008** **PCT/EP2008/067006**

(87) Fecha y número de publicación internacional: **02.07.2009** **WO09080480**

(96) Fecha de presentación y número de la solicitud europea: **08.12.2008** **E 08865434 (8)**

(97) Fecha y número de publicación de la concesión europea: **22.11.2017** **EP 2223493**

(54) Título: **Métodos, aparatos, sistema y productos de programa informático relacionados para la seguridad del traspaso**

(30) Prioridad:

19.12.2007 US 15150 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.03.2018

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
KEILALAHDENTIE 4
02150 ESPOO, FI

(72) Inventor/es:

FORSBERG, DAN LARS ANDERS y
NIEMI, PENTTI VALTTERI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 659 368 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Métodos, aparatos, sistema y productos de programa informático relacionados para la seguridad del traspaso

Campo de la invención

La presente invención se refiere a métodos, aparatos, un sistema y productos de programa informático relacionados para la seguridad del traspaso. En particular, la presente invención puede también relacionarse con UTRAN (red de acceso por radio terrestre a UMTS (sistema universal de telecomunicaciones móviles)), GERAN (red de acceso por radio EDGE (tasas de datos mejoradas para evolución global) de GSM (sistema global para comunicaciones móviles)), E-UTRAN (UTRAN evolucionado), 3GPP (proyecto de asociación para la tercera generación) EPS (sistema de paquetes evolucionado) / gestión de claves E-UTRAN y jerarquía de clave, traspasos entre sistemas, gestión de claves UTRAN/GERAN, uso de clave CK/IK (clave de cifrado/clave de integridad) de UTRAN/GERAN en la evolución HSPA (acceso de paquetes a alta velocidad) y los denominados Nodos B locales.

Antecedentes

En 3GPP (proyecto de asociación para la tercera generación), ha habido debates relacionados con la seguridad del traspaso.

Ha habido planteamientos dirigidos a: realización de AKA (autenticación y acuerdo de clave) inmediatamente después del traspaso a E-UTRAN, y posteriormente realización de un cambio de clave sobre la marcha (debatido por ejemplo en 3GPP SA3 (arquitectura del sistema 3)); - uso de una jerarquía de clave también para una actualización de, por ejemplo, el lado UTRAN/GERAN (a ser descrito en el presente documento a continuación); y - una solución parcial para la memorización de clave para E-UTRAN, que se ha mencionado en 3GPP SA3.

Sin embargo, a la vista de lo anterior, en caso de que se comprometan las claves CK e IK usadas, por ejemplo, en el lado UTRAN/GERAN (tal como un atacante que obtenga las claves CK/IK desde un RNC (controlador de la red de radio) un Nodo B local, o una estación base HSPA), y tenga lugar el traspaso a E-UTRAN, hay un problema en que las claves E-UTRAN se comprometerán asimismo, dado que se basan en las CK/IK transferidas, por ejemplo desde el lado UTRAN/GERAN al E-UTRAN.

Considerando lo anterior, es un objetivo de la presente invención superar uno o más de los inconvenientes anteriores. En particular, la presente invención proporciona métodos, aparatos, un sistema y productos de programa informático relacionados para la seguridad del traspaso.

El documento US7065340 divulga un método de autenticación y cifrado en un sistema de comunicaciones móviles, en el que una primera red, previamente al traspaso de un móvil desde ella a una segunda red, genera una segunda clave de cifrado para su uso en la segunda red, y proporciona la segunda clave de cifrado a la segunda red.

De acuerdo con la presente invención, en un aspecto, este objetivo se consigue, por ejemplo, mediante un aparato que comprende:

medios para la recepción, en un equipo de usuario, previamente a una operación de traspaso, de una primera información de indicación de clave;
medios para la creación, en el equipo de usuario, previamente a la operación de traspaso, de una información de clave basada en la primera información de indicación de clave recibida por los medios para la recepción;
medios para la retención, en el equipo de usuario, de la información de clave creada por los medios para la creación, y medios para recuperar, en el equipo de usuario, después de la operación de traspaso, la información de clave retenida por los medios para la retención basándose en la primera información de indicación de clave, y
medios para el envío, desde el equipo de usuario, después de la operación de traspaso, de la primera información de indicación de clave recibida por los medios para la recepción y asociada a la información de clave creada por los medios para la recepción previamente a la operación de traspaso.

De acuerdo con la presente invención, en otro aspecto, este objetivo se consigue por ejemplo mediante **un aparato** que comprende:

medios para la generación, previamente a una operación de traspaso, de una primera información de indicación de clave asociada a la información de clave que se pretende crear;
medios para el envío, a un equipo de usuario, previamente a la operación de traspaso, de la primera información de indicación de clave generada por los medios para la generación; y
medios para la recepción, desde el equipo de usuario, después de la operación de traspaso,

de la segunda información de indicación de clave correspondiente a la información de indicación de clave generada por los medios para la generación.

De acuerdo con la presente invención, en otro aspecto, este objetivo se consigue por ejemplo mediante **un producto de programa informático** que comprende medios de códigos que, cuando el programa se ejecuta por un ordenador, hacen que el ordenador lleve a cabo un método que comprende:

recibir, en un equipo de usuario, previamente a una operación de traspaso, una primera información de indicación de clave;
crear, en el equipo de usuario, previamente a la operación de traspaso, una información de clave basándose en la primera información de indicación de clave recibida;
retener, en el equipo de usuario, la información de clave creada, y
recuperar, en el equipo de usuario, después de la operación de traspaso, la información de clave retenida basándose en la primera información de indicación de clave, y enviar, desde el equipo de usuario, después de la operación de traspaso, la primera información de indicación de clave recibida asociada a la información de clave creada previamente a la operación de traspaso.

De acuerdo con refinamientos adicionales de la invención tal como se define bajo el aspecto anterior,

- el producto de programa informático se realiza sobre un medio legible por ordenador.

De acuerdo con la presente invención, en otro aspecto, este objetivo se consigue por ejemplo mediante **un producto de programa informático** que comprende medios de códigos que, cuando el programa se ejecuta por un ordenador, hacen que el ordenador lleve a cabo un método que comprende:

generar, previamente a una operación de traspaso, una primera información de indicación de clave asociada a la información de clave que se pretende crear;
enviar, a un equipo de usuario, previamente a la operación de traspaso, la primera información de indicación de clave generada; y
recibir, desde el equipo de usuario, después de la operación de traspaso, una segunda información de indicación de clave correspondiente a la primera información de indicación de clave generada.

De acuerdo con refinamientos adicionales de la invención tal como se define bajo el aspecto anterior,

- el producto de programa informático se realiza sobre un medio legible por ordenador.

En conexión con esto, se ha de señalar que la presente invención permite uno o más de lo siguiente:

- Portabilidad de claves, por ejemplo, en el lado E-UTRAN.
- Independencia de una versión de edición, por ejemplo, del SGSN (nodo de soporte del GPRS (servicio general de paquetes de radio) en servicio) implicado.
- Independencia de una versión de edición del UE (equipo de usuario), dado que el AKA puede realizarse sin el SMC (comando en modo seguridad).
- Permite la detección de la versión de edición del UE (por ejemplo, si es posible para el UE el traspaso a E-UTRAN, el UE es de la edición 8 o más reciente).
- Uso eficiente del KSI (identificador del conjunto de clave) para identificar claves también en el lado E-UTRAN (por ejemplo si el KSI apunta al CK e IK previo (también llamado “viejo”) usado en el lado UTRAN/GERAN o a las nuevas claves basándose en el AKA sin el procedimiento SMC respectivo).
- Protección de integridad por ejemplo del primer mensaje al E-UTRAN (por ejemplo mensaje de solicitud de servicio o L3 (nivel 3) inicial o solicitud de conexión RRC (control de recursos de radio), etc.), dado que con las claves memorizadas y transferidas (traspaso desde UTRAN/GERAN a E-UTRAN), el UE puede, por ejemplo, firmar el primer mensaje para el E-UTRAN.
- Transición más rápida de separar-a-adscribir debido a la memorización del contexto de seguridad, especialmente en traspasos de vuelta al E-UTRAN independientemente de la RAT (tecnología de acceso por radio) de origen.
- Permitir la recuperación de fallos, por ejemplo, en caso de que se pierda la conexión por radio a la RAT de origen (es decir la memorización del contexto de seguridad en E-UTRAN no requiere ninguna información desde otras RAT).

Breve descripción de los dibujos

Se describe en el presente documento a continuación una realización de la presente invención con referencia a los dibujos adjuntos, en los que:

La Fig. 1 muestra métodos respectivos para la seguridad del traspaso de acuerdo con una realización de la presente invención;

La Fig. 2 muestra aparatos respectivos (por ejemplo, SGSN/MME (entidad de gestión de la movilidad) y UE) para la seguridad del traspaso de acuerdo con la realización de la presente invención; y

La Fig. 3 muestra un sondeo de una realización de la presente invención.

Descripción detallada de una realización de la presente invención

Se describe en el presente documento a continuación una realización de la presente invención a modo de ejemplo con referencia a los dibujos adjuntos.

Se ha de observar que para esta descripción, los términos “clave de cifrado/clave de integridad, identificador del conjunto de clave, SGSN y MME” son ejemplos de “información de clave, información de indicación de clave, primera entidad de red y segunda entidad de red”, sin restricción de los términos señalados en segundo lugar a la técnica especial o detalles de implementación impuestos a los primeros términos señalados.

La Fig. 1 muestra métodos para la seguridad del traspaso de acuerdo con la realización de la presente invención. La señalización entre elementos se indica en la dirección horizontal, mientras que los aspectos de tiempo entre señalizaciones se reflejan en la disposición vertical de la secuencia de señalización así como en los números de secuencia. Se ha de observar que los aspectos de tiempo indicados en la Fig. 1 no restringen necesariamente ninguna de las etapas del método mostradas a la secuencia de etapas descrita. Esto se aplica en particular a las etapas del método que son funcionalmente disjuntas entre sí, por ejemplo, la etapa opcional de enviar/recibir información de indicación de clave desde un SGSN a un MME (por ejemplo, una transferencia de contexto de seguridad debida al traspaso desde UTRAN/GERAN a E-UTRAN) puede realizarse en cualquier momento antes de la operación de traspaso, y la etapa opcional de enviar/recibir una respuesta indicativa de una creación con éxito puede realizarse en cualquier momento antes de la operación de traspaso.

Como se muestra en la Fig. 1, una red de comunicación 200 puede comprender un equipo de usuario UE 201 y una red 202. La red 202 puede comprender a su vez una primera entidad de red (a la que se hace referencia como “SGSN” en lo que sigue del presente documento) 2021 y una segunda entidad de red (a la que se hace referencia como “MME” en lo que sigue del presente documento) 2022. El SGSN 2021 y el MME 2022 pueden disponerse también como una entidad integral, tal como se indica por la caja en línea de puntos que rodea los bloques funcionales del SGSN 2021/MME 2022.

En la etapa S1-1, por ejemplo, el SGSN 2021 puede realizar la generación, previamente a una operación de traspaso (por ejemplo entre un lado basado en UTRAN/GERAN de la red 202 y un lado basado en E-UTRAN de la red 202, tal como se indica por una línea de puntos gruesos en la Fig. 1), de una primera información de indicación de clave (por ejemplo, un primer indicador del conjunto de clave KSI) asociada a la información de clave que se pretende crear (por ejemplo a ser creada en el UE 201).

En la etapa S1-2, por ejemplo, el SGSN 2021 puede realizar el envío, previamente a la operación de traspaso, de la primera información de indicación de clave generada (por ejemplo, el identificador del conjunto de clave), por ejemplo, al UE 201. En la etapa S2-1, por ejemplo, el UE 201 puede realizar la recepción, también previamente a la operación de traspaso, de la primera información de indicación de clave (por ejemplo KSI).

A continuación, en la etapa S2-2, por ejemplo, el UE 201 puede realizar la creación, previamente a la operación de traspaso, de la información de clave (por ejemplo, una clave de cifrado CK y/o una clave de integridad IK) basándose en la primera información de indicación de clave recibida (por ejemplo, CK, IK basado en la KSI recibida).

Opcionalmente, en la etapa S2-2a, por ejemplo, el UE 201 puede realizar el envío de una respuesta indicativa de la creación con éxito, y en la etapa S1-2a, por ejemplo, el SGSN 2021 puede realizar la recepción de la respuesta. Esa transmisión de la respuesta puede realizarse para proporcionar a la red 202 información de si el UE 201 contiene o no ahora la información de clave.

En la etapa S2-3, por ejemplo, el UE 201 puede realizar la retención de la información de clave generada (tal como la retención de CK y/o IK para uso posterior, por ejemplo después del traspaso).

Adicionalmente, las etapas S1-1, S1-2, S2-1, S2-2 y S2-3 pueden resumirse de acuerdo con lo siguiente sin quedar restringido a ello: por ejemplo, puede ejecutarse un (EAP-) AKA sin un procedimiento SMC asociado al RNC, de modo que las CK e IK creadas no puedan usarse por ejemplo a través de un lado UTRAN/GERAN o en el RNC.

Se ha de observar que pueden realizarse en cualquier momento previamente al traspaso, las etapas opcionales de envío y recepción de información de indicación de clave (por ejemplo KSI) entre el SGSN 2021 y el MME 2022, por ejemplo en un caso en el que SGSN 2021 y el MME 2022 se disponen como entidades separadas (indicado por la flecha de puntos entre el SGSN 2021 y el MME 2022 en la Fig. 1). A su vez, pueden omitirse también las etapas opcionales anteriores, por ejemplo, en caso de que el SGSN 2021 y el MME 2022 se dispongan como una entidad única/combinada. Por ejemplo, estas etapas opcionales pueden efectuarse por ejemplo como una parte de una transferencia de contexto de seguridad debido al traspaso desde, por ejemplo, UTRAN/GERAN a E-UTRAN.

En la etapa S2-4, por ejemplo, el UE 201 puede realizar el envío, después de la operación de traspaso, de la primera

información de indicación de clave recibida (por ejemplo KSI) asociada a la información de clave (por ejemplo CK y/o IK) creada previamente a la operación de traspaso. En la etapa S1-3, por ejemplo, el MME 2022 puede realizar la recepción, después de la operación de traspaso, de la primera información de indicación de clave, por ejemplo, desde el UE 201 como segunda información de generación de clave (por ejemplo KSI) que corresponde a la primera información de indicación de clave generada (por ejemplo KSI).

Y, en la etapa S2-5, por ejemplo, el UE 201 puede realizar la recuperación, después de la operación de traspaso, de la información de clave retenida (por ejemplo CK y/o IK) basándose en la primera información de indicación de clave (por ejemplo KSI).

Adicionalmente, las etapas S2-4, S1-3 y S2-5 pueden resumirse de acuerdo con lo siguiente sin quedar limitado al mismo: usar por ejemplo, la KSI para indicar el origen de las claves E-UTRAN (por ejemplo identificar la CK e IK que se está usando por ejemplo, entre el UE 201 y el MME 2022).

De acuerdo con realizaciones adicionales de los métodos de acuerdo con la presente invención, la operación de traspaso puede realizarse entre una primera entidad de red (tal como un SGSN, por ejemplo en el lado basado en UTRAN/GERAN de la red 202) y una segunda entidad de red (tal como un MME, por ejemplo, en el lado basado en E-UTRAN de la red 202). Además, puede constituirse un protocolo de desafío/respuesta mediante un protocolo de autenticación y acuerdo de clave (AKA) y/o un protocolo de autenticación extensible (EAP). Adicionalmente, la información de clave puede comprender al menos una de entre una clave de cifrado (CK) y una clave de integridad (IK), y la primera y/o segunda información de identificación de clave puede comprender un identificador del conjunto de clave (KSI).

De acuerdo con desarrollos adicionales del método relacionado, por ejemplo, con el UE 201, al menos una de entre la recepción y la creación puede ser una parte del protocolo de desafío/respuesta (por ejemplo, el protocolo anterior (EAP-) AKA). Además, la retención puede comprender prescindir de un SMC (comando en modo seguridad). Adicionalmente, el UE 201 puede realizar adicionalmente el envío de la respuesta indicativa de la creación con éxito.

De acuerdo con desarrollos adicionales del método relacionado, por ejemplo, con el SGSN 2021/MME 2022, al menos una de la generación y el envío previamente a la operación de traspaso puede ser una parte del protocolo de desafío/respuesta (por ejemplo el protocolo anterior (EAP-) AKA). Más aún, la recepción después de la operación de traspaso puede comprender una transferencia de contexto de seguridad.

La Fig. 2 muestra aparatos respectivos (por ejemplo el UE 201 y el SGSN 2021/MME 2022) para seguridad del traspaso de acuerdo con la realización de la presente invención. Dentro de la Fig. 2, por facilidad de descripción, las partes que proporcionan las funcionalidades principales se representan con bloques funcionales en línea continua y caracteres normales, mientras que las partes que proporcionan funciones opcionales se representan con bloques funcionales en líneas de puntos y caracteres en cursiva.

El UE 201 puede comprender una unidad de procesamiento central CPU o funcionalidad núcleo CF (a la que se hace referencia como “CPU” en lo que sigue del presente documento) 2011, una memoria 2012, un emisor Tx 2013, un Rx receptor 2014, un creador 2015, un retentor 2016 y un recuperador 2017. Se ha de observar que el emisor 2013 puede convertirse también en obligatorio para el UE 201, por ejemplo, para la realización de comunicación de datos con el SGSN 2021/MME 2022.

El SGSN 2021 puede comprender una CPU (o funcionalidad de núcleo CF) 20211, una memoria 20212 para mantener vectores de autenticación AV n.º 1, …, AV n.º n (proporcionados por ejemplo desde un servidor de abonados local no mostrado), un emisor Tx 20213, un receptor opcional Rx 20214 y un generador 20215. El MME 2022 puede comprender una CPU 20221, una memoria 20222, un emisor opcional Tx 20223, un receptor Rx 20224 y un generador 20225. Como se ha indicado por la extensión en líneas de puntos (CPU 20211; 20221 del SGSN 2021/MME 2022) o el hueco en líneas de puntos (CPU 2011 del UE 201) de los bloques funcionales de las CPU 2011 y 20211; 20221, el generador 20215; 20225, el creador 2015, el retentor 2016 y el recuperador 2017 pueden ser funcionalidades que se ejecutan en las CPU 2011 y 20211; 20221 o pueden ser alternativamente entidades funcionales o medios separados. Adicionalmente, el generador 20215 y 20225 puede disponerse de modo intercambiable entre el SGSN 2021 y el MME 2022, independientemente de si el SGSN 2021 y el MME 2022 se disponen como entidades separadas o como una entidad única/combinada.

Las CPU 20x1 (en la que x = 1, 21 y 22) pueden configurarse respectivamente para procesar varias entradas de datos y para controlar las funciones de las memorias 20x2, los emisores 202x3 y los receptores 20x4 (y el creador 2015, el retentor 2016 y el recuperador 2017 del UE 201 así como el generador 20215; 20225 del SGSN 2021/MME 2022). Las memorias 20x2 pueden servir respectivamente, por ejemplo, para almacenar medios de códigos para llevar a cabo, por ejemplo, el método respectivo de acuerdo con la invención, cuando se ejecuta en las CPU 20x1. Se ha de observar que los emisores (opcionales) 20x3 y los receptores (opcionales) 20x4 pueden proporcionarse alternativamente como transceptores integrales respectivos (no mostrado) o como entidades separadas. Se observará adicionalmente que los emisores/receptores pueden implementarse i) como emisores/receptores físicos para la recepción por ejemplo a través de una interfaz por aire (por ejemplo en el caso del UE 201), o ii) como

entidades de enrutado por ejemplo para el envío/recepción de paquetes de datos, por ejemplo, en una red PS (de conmutación de paquetes) (por ejemplo, entre el SGSN 2021 y el MME 2022 cuando se disponen como entidades de red separadas), o iii) como funcionalidades para la escritura/lectura de información en/desde un área de memoria dada (por ejemplo, en el caso de las CPU o memorias compartidas/comunes por ejemplo del SGSN 2021 y el MME 2022 cuando se disponen como una entidad de red integral), o iv) como cualquier combinación adecuada de i) a iii).

Adicionalmente, como se indica por las conexiones en líneas de puntos entre los bloques funcionales del SGSN 2021 y el MME 2022, se ha de observar que el SGSN 2021 y el MME 2022 pueden implementarse también como una entidad integral/combinada, como se ha mencionado anteriormente. En ese caso, las CPU 20211, 20221, las memorias 20212, 20222, los emisores (opcionales) 20213, 20223 y los receptores (opcionales) 20234, 20244 deben ser respectivamente recursos comunes y/o compartidos.

En consecuencia, por ejemplo, el generador 20215; 20225 del SGSN 2021/MME 2022, por ejemplo, en unión con las CPU 20211; 20221 pueden configurarse para generar, previamente a una operación de traspaso (véase el lado izquierdo de la línea de líneas y puntos en la Fig. 2, etiquetada “antes del traspaso”), la primera información de indicación de clave (por ejemplo, un identificador del conjunto de clave KSI) asociada a la información de clave (por ejemplo, CK y/o IK) que se pretende crear (por ejemplo a ser creada por el generador 2015 del UE 201). El identificador del conjunto de clave puede crearse a partir de uno común de los vectores de autenticación AV n.º 1, …, AV n.º n.

Y, por ejemplo, el emisor 20213; 20223 del SGSN 2021/MME 2022 puede configurarse para enviar, previamente a la operación de traspaso, la primera información de indicación de clave (por ejemplo KSI) generada por el generador 20215; 20225. A continuación, por ejemplo, el receptor 2014 del UE 201 puede configurarse para recibir, previamente a la operación de traspaso, la primera información de indicación de clave (por ejemplo KSI).

Por ejemplo, el creador 2015 del UE 201 puede configurarse para crear, previamente a la operación de traspaso, información de clave (por ejemplo CK y/o IK) basándose en la primera información de indicación de clave (por ejemplo KSI basada en CK, IK) recibida por el receptor 2014.

Opcionalmente, por ejemplo, el emisor 2013 del UE 201 puede configurarse para enviar la respuesta indicativa de una creación con éxito de la primera información de clave. Si, por ejemplo, el receptor 20214 del SGSN 2021 puede configurarse para recibir la respuesta. Esta transmisión de la respuesta puede realizarse para proporcionar al SGSN 2021 y posteriormente al MME 2022 información de si el UE 201 contiene ahora o no la primera información de clave.

A continuación, por ejemplo, el receptor 2016 del UE 201 puede configurarse para retener la información de clave (por ejemplo retener la CK y/o IK para uso posterior después de la operación de traspaso) creada por el creador 2015.

Adicionalmente, por ejemplo, el emisor 2013 del UE 201 puede configurarse adicionalmente para enviar, después de la operación de traspaso, la primera información de indicación de clave (por ejemplo, el identificador del conjunto de clave KSI) asociada a la información de clave (por ejemplo CK y/o IK) creada por el creador 2015 previamente a la operación de traspaso. En consecuencia, por ejemplo, el receptor 20214; 20224 del SGSN 2021/MME 2022 puede configurarse adicionalmente para recibir, después de la operación de traspaso (véase el lado derecho de la línea de líneas y puntos en la Fig. 2, etiquetada “después del traspaso”), la primera información de indicación de clave (por ejemplo desde el UE 201) como segunda información de indicación de clave (por ejemplo, KSI relacionada con CK y/o IK retenida por el UE 203) correspondiente a la primera información de indicación de clave (por ejemplo KSI que se refiere a la CK y/o IK correspondiente, por ejemplo en el MME 2022) generada por el generador 20215; 20225.

Y, por ejemplo, el recuperador 2017 del UE 201 puede configurarse para recuperar, después de la operación de traspaso, la información de clave (por ejemplo CK y/o IK) retenida por el receptor 2016 basándose en la información de indicación de clave (por ejemplo KSI).

De acuerdo con desarrollos adicionales del aparato (por ejemplo, UE 201 y SGSN 2021/MME 2022) de acuerdo con la presente invención, la operación de traspaso puede realizarse entre una primera entidad de red (tal como un SGSN, por ejemplo, en el lado basado en UTRAN/GERAN de la red 202) y una segunda entidad de red (tal como un MME, por ejemplo en el lado basado en E-UTRAN de la red 202). Además, puede constituirse un protocolo de desafío/respuesta mediante un protocolo de autenticación y acuerdo de clave (AKA) y/o un protocolo de autenticación extensible (EAP-) AKA. Adicionalmente, la información de clave puede comprender al menos una de entre una clave de cifrado (CK) y una clave integridad (IK), y la primera y/o segunda información de identificación de clave puede comprender un identificador del conjunto de clave (KSI).

De acuerdo con desarrollos adicionales de, por ejemplo, el UE 201, al menos uno de entre el receptor 2014 y el creador 2015 pueden configurarse para realizar una parte del protocolo de desafío/respuesta (por ejemplo, el protocolo anterior (EAP-) AKA). Además, el retentor 2016 puede configurarse adicionalmente para prescindir del SMC (comando en modo de seguridad). Finalmente, el UE puede estar de acuerdo con al menos uno de entre una

red de acceso por radio terrestre del sistema universal de telecomunicaciones móviles (UTRAN), transferencias de datos mejoradas para el sistema global de comunicaciones móviles para la evolución global de la red de acceso por radio (GERAN) y una UTRAN evolucionada. Adicionalmente, el emisor 2013 puede configurarse para enviar la respuesta indicativa de la creación con éxito de la primera información de clave.

De acuerdo con desarrollos adicionales de, por ejemplo, el SGSN 2021/MME 2022, al menos uno de entre el generador 20215; 20255 y el emisor 20213 puede configurarse para realizar una parte del protocolo de desafío/respuesta (por ejemplo, el protocolo anterior (EAP-) AKA). Más aún, el receptor 20224 puede configurarse para recibir basándose en una transferencia de contexto de seguridad. Adicionalmente, el receptor 20214 puede configurarse adicionalmente para recibir la respuesta anteriormente descrita.

La Fig. 3 muestra un sondeo de la realización de la presente invención.

De acuerdo con el sondeo, la etapa S1 puede realizar lo siguiente sin quedar restringida a ello: por ejemplo, puede ejecutarse un (EAP-) AKA sin un procedimiento SMC asociado al RNC, de modo que las CK e IK creadas pueden no usarse, por ejemplo, a través del aire en el lado UTRAN/GERAN o en el RNC.

Adicionalmente, la etapa S2 puede realizar lo siguiente, sin quedar restringida a ello: transferencia del contexto de seguridad debido al traspaso, por ejemplo, desde el UTRAN/GERAN al-UTRAN.

Finalmente, la etapa S3 puede realizar lo siguiente sin quedar restringida a ello: usar, por ejemplo, la KSI para indicar el origen de las claves E-UTRAN (por ejemplo, identificar la CK e IK que están siendo usadas, por ejemplo, entre el UE 201 y el MME 2022).

Adicionalmente, el UE 201 y/o SGSN 2021/MME 2022 de acuerdo con la presente realización pueden implementarse también como un conjunto de chips o módulo.

Además, la presente realización también se refiere a un sistema que pueda comprender tanto el UE 201 como el SGSN 2021/MME 2022.

Sin quedar restringido a los detalles que siguen de esta sección, la realización de la presente invención puede resumirse como sigue:

La realización puede residir en la ejecución del (EAP-) AKA sin el procedimiento de Comando en Modo de Seguridad en el lado UTRAN/GERAN antes del traspaso al E-UTRAN y usar estas claves frescas a partir de la ejecución del procedimiento (EAP-) AKA en el lado E-UTRAN el lugar de las CK e IK usadas. Las claves frescas pueden identificarse en el lado E-UTRAN con el identificador del conjunto de clave (KSI) a partir del procedimiento (EAP-) AKA.

La realización también puede residir en que el UE puede usar la KSI para apuntar a las claves memorizadas en el lado E-UTRAN en lugar de las claves transferidas desde el SGSN de UTRAN/GERAN (tanto las CK e IK antiguas como las claves frescas basadas en la ejecución (EAP-) AKA sin SMC).

La realización también puede residir en que el contexto de seguridad del lado E-UTRAN en el MME puede transferirse al lado UTRAN/GERAN (por ejemplo, como un contenedor transparente) de modo que el MME del lado E-UTRAN no tenga que memorizar el contexto UE para los UE que no están adscritos. El contexto (de seguridad) E-UTRAN “memorizado” (por ejemplo, claves de sesión, valores de contador, identificadores del conjunto de clave, capacidades de seguridad del UE, etc.) se mueve con el UE desde el SGSN al MME y desde el MME al SGSN.

[Realizaciones adicionales]

Para la finalidad de la presente invención tal como se ha descrito en el presente documento anteriormente, debería observarse que

- una tecnología de acceso puede ser cualquier tecnología por medio de la que un equipo de usuario puede acceder a una red de acceso (o estación base, respectivamente). Puede usarse cualquier tecnología actual o futura, tal como WLAN (red de acceso local inalámbrico), WiMAX (interoperabilidad mundial para acceso por microondas), Bluetooth, infrarrojos, y similares; aunque las tecnologías anteriores son principalmente tecnologías de acceso inalámbrico, por ejemplo, en diferentes espectros de radio, la tecnología de acceso en el sentido de la presente invención puede implicar también tecnologías cableadas, por ejemplo, tecnologías de acceso basadas en IP, redes por cable o de línea fija.
- una red de acceso puede ser cualquier dispositivo, unidad o medio mediante el que una entidad de estación u otro equipo de usuario puede conectar a y/o utilizar los servicios ofrecidos por la red de acceso; dichos servicios incluyen, entre otros, comunicación de datos y/o (audio-) visual, descarga de datos, etc.;
- en general, la presente invención es aplicable en aquellos entornos de red/equipos de usuario que se basan en un esquema de transmisión basado en paquetes de datos de acuerdo con el que los datos se transmiten en

paquetes de datos y que se basan, por ejemplo, en el protocolo de Internet IP. La presente invención no está, sin embargo, limitada a ello, y cualquier otra versión de IP presente o futura o IP móvil (MIP) o, más generalmente, un protocolo que siga principios similares al (M)IPv4/6, también es aplicable;

- un equipo de usuario puede ser cualquier dispositivo, unidad o medio mediante el que un usuario del sistema puede experimentar servicios desde una red de acceso;
- las etapas del método probablemente se implementan como partes de código de software y se ejecutan usando un procesador en el elemento de red, son independientes del código de software y pueden especificarse usando cualquier lenguaje de programación conocido o desarrollado en el futuro siempre que se preserve la funcionalidad definida por las etapas del método;
- en general, cualquier etapa del método es adecuada para ser implementada como software o por hardware sin cambiar la idea de la presente invención en términos de la funcionalidad implementada;
- las etapas del método y/o dispositivos, unidades o medios se implementan probablemente como componentes de hardware en un equipo de usuario o estación base, o cualquier módulo(s) del mismo, son independientes del hardware y pueden implementarse usando cualquier tecnología de hardware conocida o desarrollada en el futuro o cualquier híbrido de estas, tales como MOS (semiconductor de óxido metálico), CMOS (MOS complementario), BiMOS (CMOS bipolar), ECL (lógica acoplada por emisor), TTL (lógica transistor-transistor), etc., usando por ejemplo componentes ASIC (IC (circuitos integrados) de aplicación específica), componentes FPGA (matrices de puertas programables en campo, componentes CPLD (dispositivos lógicos complejos programables) o componentes DSP (procesadores de señal digital); además, cualesquiera etapas del método y/o dispositivos, unidades o medios que se implementen probablemente como componentes de software pueden por ejemplo basarse en cualquier arquitectura de seguridad capaz de, por ejemplo, autenticación, autorización, gestión de claves y/o protección de tráfico, tal como AKA y/o EAP-AKA;
- los dispositivos, unidades o medios (por ejemplo, equipo de usuario y estación base) pueden implementarse como dispositivos, unidades o medios individuales, pero esto no excluye que se implementen en una forma distribuida a todo lo largo del sistema, siempre que se preserve la funcionalidad del dispositivo, unidad o medio.

Lista de abreviaturas

3GPP	Proyecto de Asociación para la Tercera Generación
UE	Equipo de Usuario
MME	Entidad de Gestión de la Movilidad
SGSN	Nodo de Soporte GPRS en Servicio
GPRS	Servicio General de Paquetes de Radio
UTRAN	Red de Acceso por Radio Terrestre a UMTS
GSM	Sistema Global para Comunicaciones Móviles
EDGE	Tasa Mejorada de Datos para Evolución Global
GERAN	Red de Acceso por Radio EDGE a GSM
UMTS	Sistema Universal de Telecomunicaciones Móviles
EAP	Protocolo de Autenticación Extensible
AKA	Autenticación y Acuerdo de clave
SMC	Comando en Modo de Seguridad
E-UTRAN	UTRAN Evolucionado
EPS	Sistema de Paquetes Evolucionado
KSI	Identificador del Conjunto de clave
CK	Clave de Cifrado
IK	Clave de Integridad
HSPA	Acceso de Paquetes a Alta Velocidad (o HSUPA/HSPDA)

REIVINDICACIONES

1. Un aparato (201), que comprende:

medios para la recepción (2014), en un equipo de usuario, previamente a una operación de traspaso, de una primera información de indicación de clave;
medios para la creación (2015), en el equipo de usuario, previamente a la operación de traspaso, de una información de clave basada en la primera información de indicación de clave recibida por los medios para la recepción;
medios para la retención (2016), en el equipo de usuario, de la información de clave creada por los medios para la creación, y
medios para la recuperación (2017), en el equipo de usuario, después de la operación de traspaso, de la información de clave retenida por los medios para la retención basándose en la primera información de indicación de clave,
caracterizado por
medios para el envío (2013), desde el equipo de usuario, después de la operación de traspaso, de la primera información de indicación de clave recibida por los medios para la recepción y asociada a la información de clave creada por los medios para la creación previamente a la operación de traspaso.

2. El aparato (201) de la reivindicación 1, que comprende adicionalmente:

medios para la recuperación (2017), después de una operación de traspaso, de información de clave retenida previamente a la operación de traspaso basándose en la primera información de indicación de clave recibida previamente a la operación de traspaso.

3. El aparato (201) de la reivindicación 1, que comprende adicionalmente:

medios para el envío (2013), previamente a una operación de traspaso, de primera información de indicación de clave asociada a la información de clave que se pretende generar previamente a la operación de traspaso.

4. El aparato (201) de la reivindicación 1, que comprende adicionalmente:

medios para la indicación (2011) de un contexto seleccionado mediante la inclusión de un identificador del conjunto de clave correspondiente en un mensaje de confirmación del traspaso a un nodo B evolucionado objetivo, siendo el contexto seleccionado uno de entre un contexto de seguridad memorizado y un contexto de seguridad mapeado dependiendo de si el contexto de seguridad memorizado está presente o no.

5. El aparato (201) de la reivindicación 1, que comprende adicionalmente:

medios para la inserción (2011) de uno de un identificador del conjunto de clave relacionado con una entidad de gestión de la seguridad de acceso y un identificador del conjunto de clave relacionado con un nodo de soporte del servicio de radio de paquetes generales en servicio de un contexto de seguridad mapeado en un contenedor transparente dependiendo de si está presente o no un contexto de seguridad memorizado.

6. El aparato (201) de la reivindicación 1, que comprende adicionalmente:

medios para proporcionar (2011) una clave relacionada con un nodo B evolucionado basándose en un contexto de seguridad mapeado y un contexto de seguridad memorizado para un nodo B evolucionado objetivo junto con un identificador del conjunto de clave relacionado con una entidad de gestión de la seguridad de acceso y un identificador del conjunto de clave relacionado con un nodo de soporte del servicio de radio por paquetes general en servicio dependiendo de si el contexto de seguridad memorizado está presente o no en una entidad de gestión de la movilidad.

7. Un aparato (2021, 2022), que comprende:

medios para la generación (20215), previamente a una operación de traspaso, de una primera información de indicación de clave asociada a la información de clave que se pretende crear; y
medios para el envío (20213), a un equipo de usuario, previamente a la operación de traspaso, de la primera información de indicación de clave generada por los medios para la generación,
caracterizado por

medios para la recepción (20224), desde el equipo de usuario, después de la operación de traspaso, de la segunda información de indicación de clave correspondiente a la información de indicación de clave generada por los medios para la generación.

8. El aparato (2021, 2022) de la reivindicación 7, que comprende adicionalmente:

medios para la recuperación (20221), después de una operación de traspaso, de información de clave retenida previamente a la operación de traspaso basándose en una primera información de indicación de clave recibida previamente a la operación de traspaso.

9. El aparato (2021, 2022) de la reivindicación 7, que comprende adicionalmente:

medios para el envío (20213), previamente a una operación de traspaso, de una primera información de indicación de clave que está asociada a la información de clave que se pretende generar previamente a la operación de traspaso.

10. El aparato (2021, 2022) de la reivindicación 7, que comprende adicionalmente:

medios para la indicación (20211) de un contexto seleccionado mediante la inclusión de un identificador del conjunto de clave correspondiente en un mensaje de confirmación del traspaso a un nodo B evolucionado objetivo, siendo el contexto seleccionado uno de entre un contexto de seguridad memorizado y un contexto de seguridad mapeado dependiendo de si el contexto de seguridad memorizado está presente o no.

11. El aparato (2021, 2022) de la reivindicación 7, que comprende adicionalmente:

medios para la inserción (20211) de uno de entre un identificador del conjunto de clave relativo a una entidad de gestión de la seguridad de acceso y un identificador del conjunto de clave relativo a un nodo de soporte del servicio de radio por paquetes general en servicio de un contexto de seguridad mapeado en un contenedor transparente dependiendo de si el contexto de seguridad memorizado está presente o no.

12. El aparato (2021, 2022) de la reivindicación 7, que comprende adicionalmente:

medios para proporcionar (20211) una clave relacionada con un nodo B evolucionado basándose en un contexto de seguridad mapeado y un contexto de seguridad memorizado para un nodo B evolucionado objetivo junto con un identificador del conjunto de clave relacionado con una entidad de gestión de la seguridad de acceso y un identificador del conjunto de clave relacionado con un nodo de soporte de servicio de radio por paquetes general en servicio dependiendo de si el contexto de seguridad memorizado está presente o no en una entidad de gestión de la movilidad.

13. Un producto de programa informático que comprende medios de códigos que, cuando el programa es ejecutado por un ordenador, hacen que el ordenador lleve a cabo un método que comprende:

recibir, en un equipo de usuario, previamente a una operación de traspaso, una primera información de indicación de clave;
crear, en el equipo de usuario, previamente a la operación de traspaso, una información de clave basándose en la primera información de indicación de clave recibida;
retener, en el equipo de usuario, la información de clave creada, y
recuperar, en el equipo de usuario, después de la operación de traspaso, la información de clave retenida basándose en la primera información de indicación de clave,
caracterizado por
enviar, desde el equipo de usuario, después de la operación de traspaso, la primera información de indicación de clave recibida asociada a la información de clave creada previamente a la operación de traspaso.

14. El producto de programa informático de acuerdo con la reivindicación 13, en donde el producto de programa informático se realiza sobre un medio legible por ordenador.

15. Un producto de programa informático que comprende medios de códigos que, cuando el programa es ejecutado por un ordenador, hacen que el ordenador lleve a cabo un método que comprende:

generar, previamente a una operación de traspaso, una primera información de indicación de clave asociada a la información de clave que se pretende crear; y
enviar, a un equipo de usuario, previamente a la operación de traspaso, la primera información de indicación de clave generada,
caracterizado por
recibir, desde el equipo de usuario, después de la operación de traspaso, una segunda información de indicación de clave correspondiente a la primera información de indicación de clave generada.

16. El producto de programa informático de acuerdo con la reivindicación 15, en donde el producto de programa informático se realiza sobre un medio legible por ordenador.

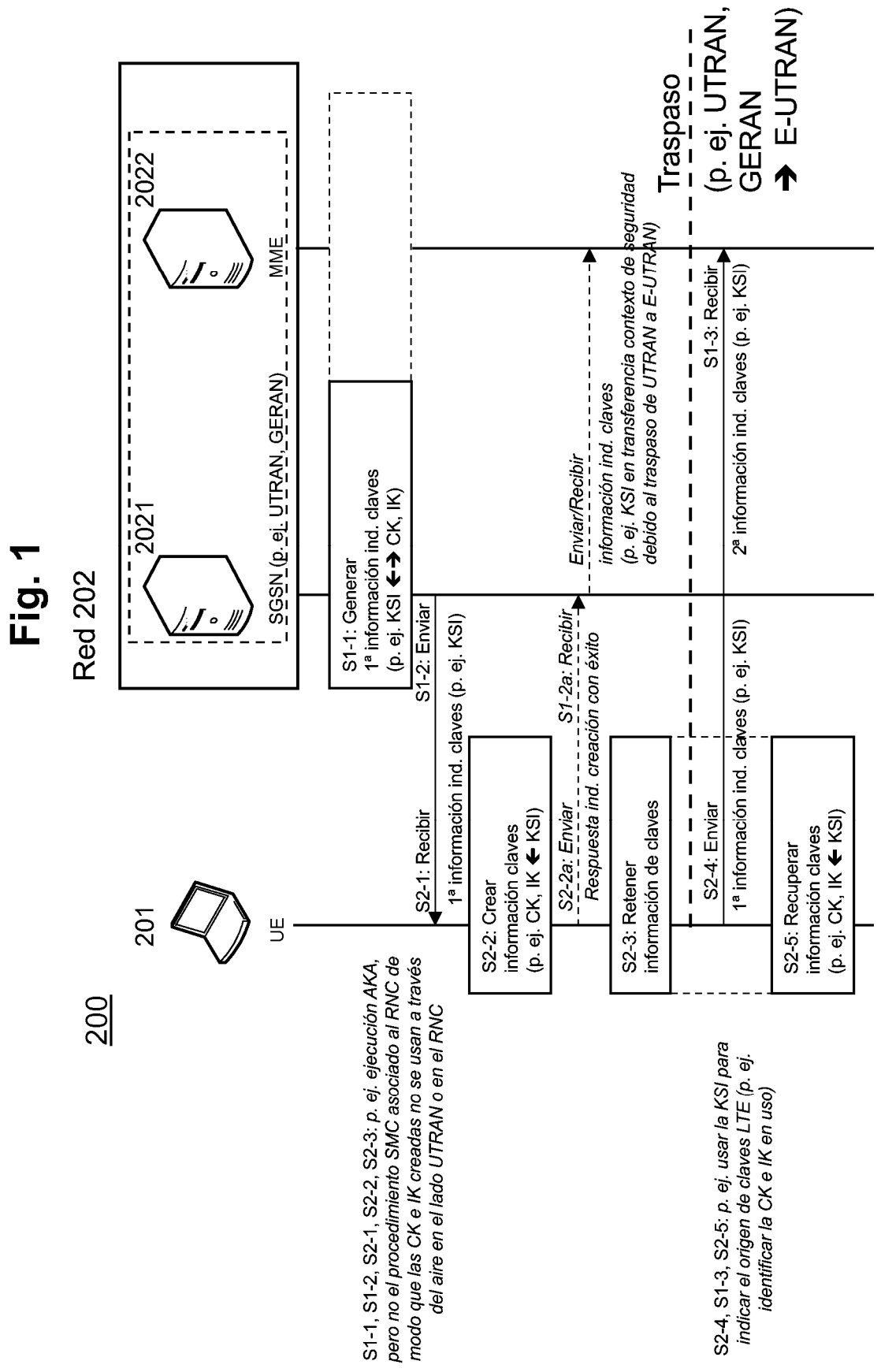


Fig. 1
200
Red 202
2021
2022
SGSN (p. ej. UTRAN, GERAN)
MME
201
UE
S1-1: Generar
1ª información ind. claves
(p. ej. KSI ↔ CK, IK)
S1-2: Enviar
1ª información ind. claves (p. ej. KSI)
S2-1: Recibir
S2-2: Crear
información claves
(p. ej. CK, IK ← KSI)
S2-2a: Enviar
Respuesta ind. creación con éxito
S1-2a: Recibir
Enviar/Recibir
información ind. claves
(p. ej. KSI en transferencia contexto de seguridad
debido al traspaso de UTRAN a E-UTRAN)
S2-3: Retener
información de claves
S2-4: Enviar
1ª información ind. claves (p. ej. KSI)
S1-3: Recibir
2ª información ind. claves (p. ej. KSI)
Traspaso
(p. ej. UTRAN,
GERAN
→ E-UTRAN)
S2-5: Recuperar
información claves
(p. ej. CK, IK ← KSI)
S1-1, S1-2, S2-1, S2-2, S2-3: p. ej. ejecución AKA,
pero no el procedimiento SMC asociado al RNC de
modo que las CK e IK creadas no se usan a través
del aire en el lado UTRAN o en el RNC
S2-4, S1-3, S2-5: p. ej. usar la KSI para
indicar el origen de claves LTE (p. ej.
identificar la CK e IK en uso)

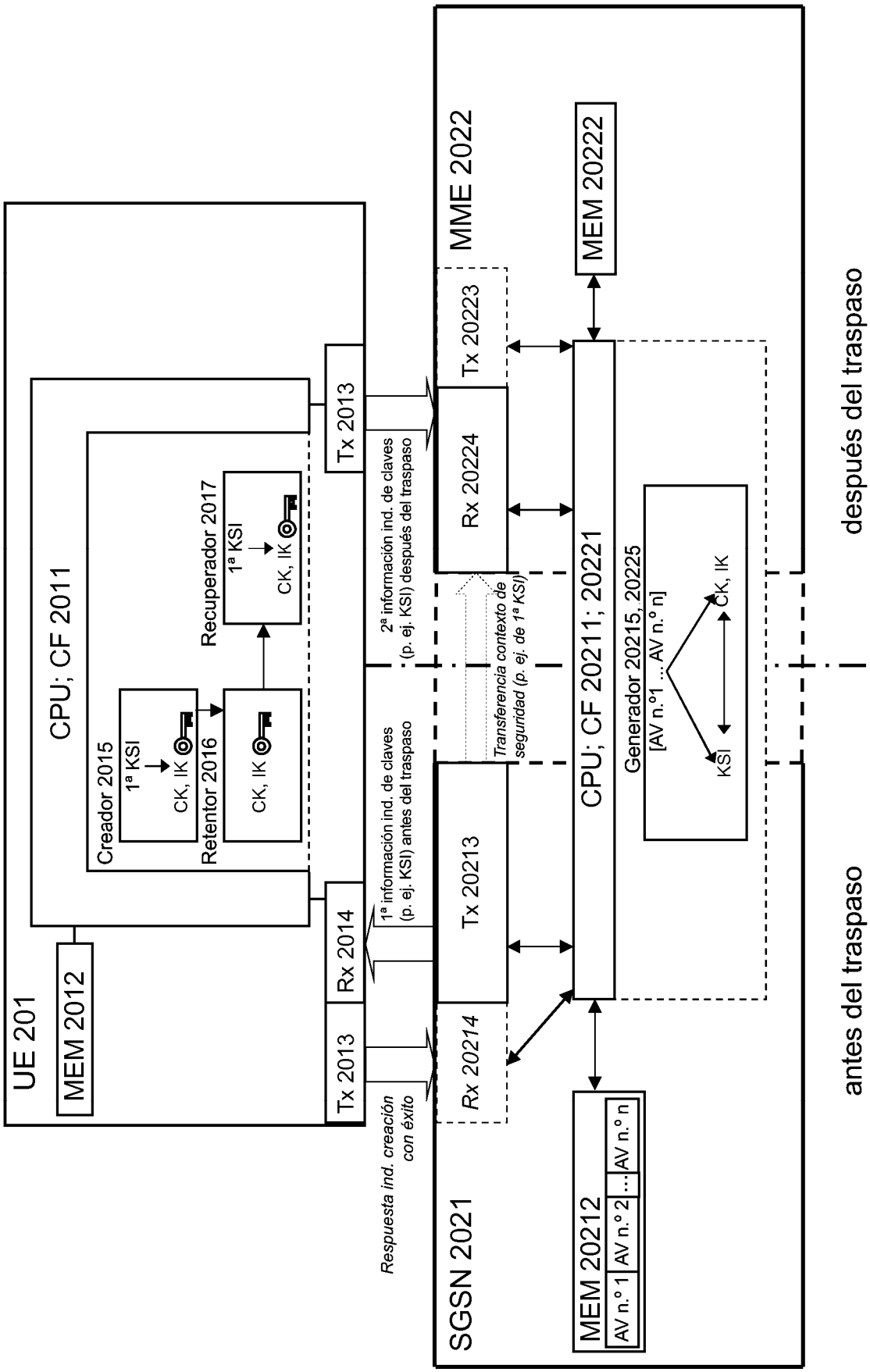
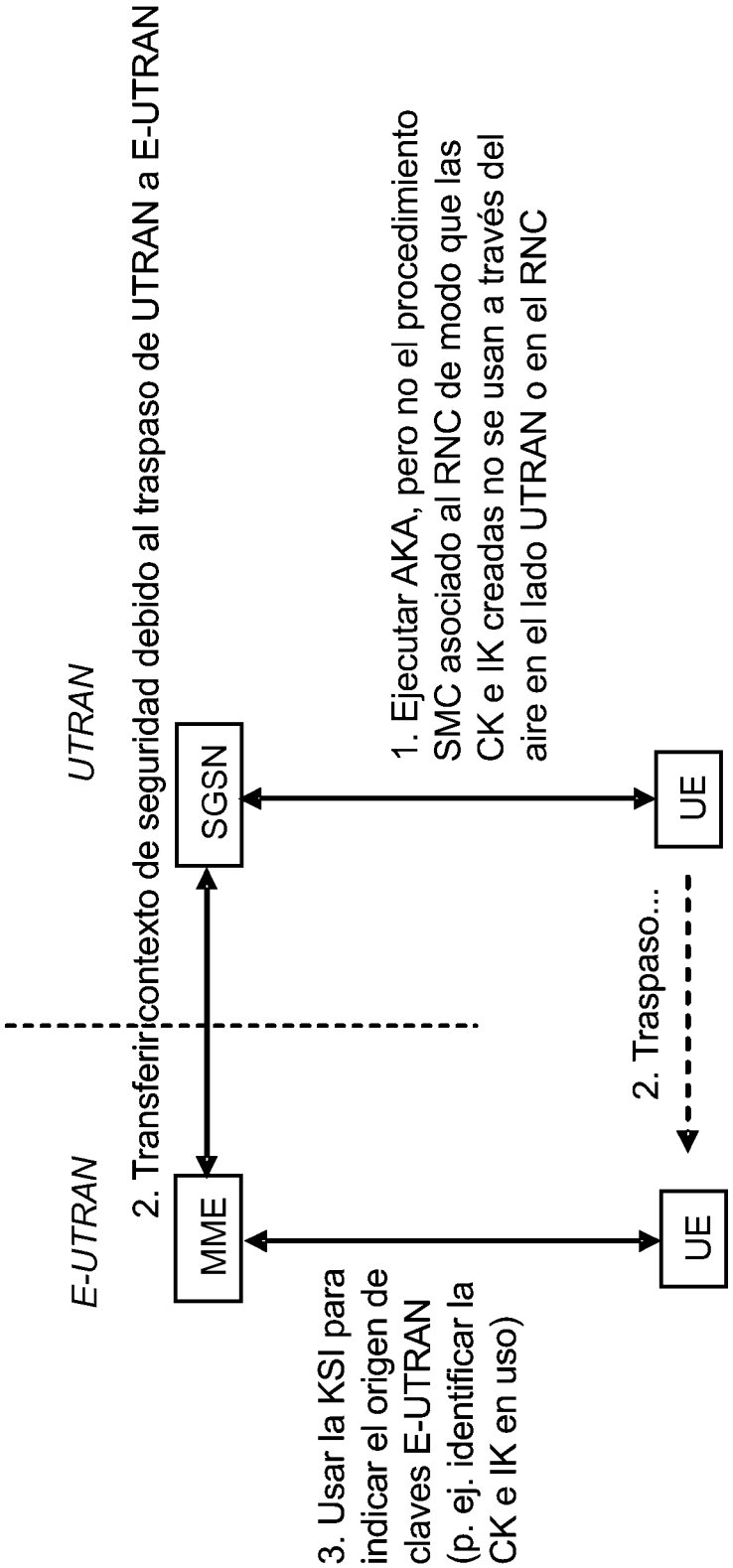

UE 201
MEM 2012
CPU; CF 2011
Creador 2015
1ª KSI
CK, IK
Retentor 2016
CK, IK
Recuperador 2017
1ª KSI
CK, IK
Tx 2013
Rx 2014
Tx 2013
Respuesta ind. creación con éxito
1ª información ind. de claves (p. ej. KSI) antes del traspaso
2ª información ind. de claves (p. ej. KSI) después del traspaso
SGSN 2021
Rx 20214
Tx 20213
Rx 20224
Tx 20223
MME 2022
Transferencia contexto de seguridad (p. ej. de 1ª KSI)
CPU; CF 20211; 20221
MEM 20222
Generador 20215, 20225
[AV n.º1 ... AV n.º n]
CK, IK
KSI
MEM 20212
AV n.º 1
AV n.º 2
...
AV n.º n
antes del traspaso
después del traspaso

Fig. 2

Fig. 3


UTRAN
E-UTRAN
SGSN
MME
UE
UE
2. Transferir contexto de seguridad debido al traspaso de UTRAN a E-UTRAN
1. Ejecutar AKA, pero no el procedimiento SMC asociado al RNC de modo que las CK e IK creadas no se usan a través del aire en el lado UTRAN o en el RNC
2. Traspaso...
3. Usar la KSI para indicar el origen de claves E-UTRAN (p. ej. identificar la CK e IK en uso)