(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 808 498**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 29/06 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.06.2007 E 18199994 (7)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2020 EP 3461058**

(54) Título: **Método y sistema para distribución de claves en una red de comunicación inalámbrica**

(30) Prioridad:

23.06.2006 CN 200610090103

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.03.2021

(73) Titular/es:

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

(72) Inventor/es:

HU, WEIHUA y
CHEN, JING

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y sistema para distribución de claves en una red de comunicación inalámbrica

CAMPO DE LA INVENCIÓN

La presente invención se refiere a un campo de comunicaciones inalámbricas y en particular, a un método y sistema para distribución de claves en una red de comunicación inalámbrica.

ANTECEDENTES DE LA INVENCIÓN

Con el rápido crecimiento de los tráficos y servicios basados en el protocolo IP, el denominado Proyecto de Asociación de la Tercera Generación (3GPP), como una tecnología de acceso, falla en la adaptación a dichos cambios. Mientras tanto surgieron nuevas tecnologías de acceso, tales como red de área local inalámbrica (WLAN) y la interoperabilidad mundial para acceso de microondas (WiMAX), representan una amenaza directa para la red 3GPP. Para mantener la ventaja competitiva del sistema de 3GPP en los próximos 10 años o un periodo más largo, la evolución de la tecnología de acceso es permanente en la organización de 3GPP. La organización de 3GPP comienza a trabajar sobre la evolución a largo plazo (LTE) de la tecnología de acceso a red 3GPP, en particular la mejora de la tecnología de comunicación de paquetes puesta en práctica en el sistema de 3GPP con el fin de mantener la posición de liderazgo del sistema de acceso de 3GPP en términos de red y economía de costes.

La Figura 1 ilustra la arquitectura del sistema evolucionado. Las entidades principales en una red base de paquetes evolucionada (EPC) incluyen: una entidad de gestión de la movilidad (MME), adaptada para gestionar la movilidad del plano de control, incluyendo la gestión del estado de movilidad y del contexto del usuario, la distribución de un identificador de estación móvil temporal (TMSI) y la función de la seguridad; una entidad del plano de usuario (UPE) adaptada para iniciar la búsqueda por paginación para los datos de enlace descendente en estado inactivo, para gestionar y memorizar los parámetros de soporte de IP y la información de enrutamiento en la red; y un anclaje entre estratos de acceso AS (IASA) que sirve como el anclaje del plano de usuario entre diferentes sistemas. La entidad UPE puede existir con independencia o como una entidad junto con la MME. La entidad UPE puede existir también como una entidad junto con la IASA, o desplazarse a la red de acceso y existir como una entidad junto con un nodo eNB. En la Figura, las interfaces y sus funciones no están definidas de forma definitiva. La información del usuario se memoriza en un servidor de abonado residencial (HSS).

La evolución de la red de 3GPP está prevista para reducir el retardo y el tiempo de respuesta, aumentar la tasa de datos, ampliar la capacidad del sistema y su cobertura, y reducir el coste operativo. En términos de seguridad, el mecanismo de seguridad del usuario en la red evolucionada debe garantizarse con al menos el mismo nivel de seguridad que en los sistemas 2G y 3G actuales.

Actualmente, en un sistema de telecomunicación móvil universal (UMTS), un punto de terminación seguro está en un controlador de red de radio (RNC). Un equipo de usuario (UE) y el controlador RNC realizan una operación de cifrado/descifrado y protección de la integridad para proporcionar la protección de encriptación para datos de usuario, y la protección de encriptación y de integridad para la señalización entre el equipo UE y el controlador RNC. Bajo esta circunstancia, el equipo UE y el controlador RNC necesitan solamente una clave raíz (CK) y una clave de integridad (IK). El modo de distribución de CK y de IK es como sigue:

1. El equipo UE y una red realizan una autenticación. Después de la autenticación, el equipo UE y un centro de conmutación móvil/registro de localización de visitantes (MSC/VLR) en una red base reciben las claves CK e IK.

2. El MSC/VLR en la red base o el nodo de soporte de GPRS de servicio (SGSN) distribuye las claves CK e IK al controlador RNC.

Mientras que, en la red inalámbrica evolucionada, tres asociaciones de seguridad diferentes pueden participar para proteger, respectivamente, la seguridad de una señalización de estrato de acceso (AS), una señalización de estrato de no acceso (NAS) y datos de usuario, es decir, la seguridad del plano del usuario, el plano de señalización de AS y el plano de señalización de NAS. La seguridad del plano de usuario se termina en la red base o en la red de acceso. La seguridad de la señalización de AS y de la señalización NAS en el plano de señalización se termina, respectivamente, en la red de acceso y la red base. Más concretamente, la seguridad del plano de usuario se termina en la entidad UPE en la red base o en la estación base en la red de acceso. La seguridad de la señalización de AS se termina en la estación base en la red de acceso evolucionada. La seguridad de la señalización de NAS puede terminarse en la entidad MME o la IASA en la red base, lo que no está determinado todavía. Por lo tanto, en la red evolucionada, es necesario distribuir los tres conjuntos anteriores de claves asociadas con la seguridad del plano de usuario y la seguridad del plano de señalización a entidades que realicen la operación de seguridad en la red y en el equipo UE.

El documento de W. Zhang, "Seguridad de interfuncionamiento en redes IP inalámbricas heterogéneas", Actas de la 3ª Conferencia Internacional sobre Conexión en Redes (ICN '04), da a conocer un método de intercambio de claves en una red UMTS.

El documento de publicación de solicitud de patente de Estados Unidos US2003/0207696 para Willenegger et al. da a conocer un denominado servicio de difusión y multidifusión multimedia en una red inalámbrica.

El método existente para distribuir claves en UMTS solamente puede deducir y distribuir un grupo de claves a una entidad que realiza la operación de seguridad en la red y en el equipo UE. Por lo tanto, es necesario formular un método para deducir y distribuir claves en la red evolucionada.

SUMARIO DE LA INVENCIÓN

Formas de realización de la presente invención dan a conocer un método para distribución de claves en una red de comunicaciones inalámbricas con el fin de deducir y distribuir claves en la red evolucionada para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario.

Un método para la distribución de claves en una red de comunicaciones inalámbricas, que incluye: recibir, por una entidad de gestión de la movilidad, MME, una clave raíz desde un servidor de abonado local, HSS; deducir, por la MME, las claves para proteger la seguridad de una señalización de estrato de acceso, AS, una señalización de estrato de no acceso, NAS, y datos de usuario de conformidad con la clave raíz; y enviar, por la MME, las claves a las entidades que realizan operaciones de seguridad.

Un método para la distribución de claves en una red de comunicaciones inalámbricas, que incluye: deducir, por un equipo de usuario, UE, una clave raíz; y deducir, por el equipo UE, las claves para proteger la seguridad de una señalización de estrato de acceso, AS, una señalización de estrato de no acceso, NAS, y datos de usuario de conformidad con la clave raíz.

Una entidad de gestión de la movilidad, MME, que incluye:

un módulo de deducción de claves, configurado para deducir las claves para proteger la seguridad de una señalización de estrato de acceso, AS, una señalización de estrato de no acceso, NAS, y datos de usuario de conformidad con una clave raíz recibida desde un servidor de abonado local, HSS; y un módulo de distribución de claves, configurado para enviar las claves a entidades que realizan operaciones de seguridad.

Un sistema para la distribución de claves en una red de comunicaciones inalámbricas, que incluye la entidad MME y el servidor HSS, en donde el servidor HSS incluye:

un módulo de deducción de clave raíz, configurado para deducir la clave raíz y enviar la clave raíz a la entidad MME.

Un equipo de usuario, UE, que incluye:

un módulo de deducción de claves, configurado para deducir una clave raíz y deducir las claves para proteger la seguridad de una señalización de estrato de acceso, AS, una señalización de estrato de no acceso, NAS, y datos de usuario de conformidad con la clave raíz.

En las formas de realización anteriores de la presente invención, la red deduce claves para proteger la seguridad de la señalización de AS, la señalización de NAS y los datos de usuario, y distribuye las claves a entidades que realizan operaciones de seguridad pertinentes en la red y en el equipo UE. El equipo UE puede deducir claves para proteger la seguridad de la señalización de AS, la señalización de NAS y los datos del usuario, de modo que las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y los datos de usuarios en una red de comunicaciones inalámbricas sean objeto de deducción y distribución y esté garantizada la seguridad de la comunicación de red.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 ilustra la arquitectura de una red evolucionada inalámbrica en conformidad con la técnica anterior;

La Figura 2 representa un diagrama de flujo que ilustra el procedimiento de distribución de claves en conformidad con una primera forma de realización de la presente invención;

La Figura 3 representa un diagrama que ilustra el servidor HSS o el equipo UE que deducen las claves en conformidad con una primera forma de realización de la presente invención;

La Figura 4 representa un diagrama de flujo que ilustra el procedimiento de distribución de claves en conformidad con una segunda forma de realización de la presente invención;

La Figura 5 representa un diagrama que ilustra el HSS o el equipo UE que deducen una clave raíz en conformidad con una segunda forma de realización de la presente invención;

La Figura 6 representa un diagrama que ilustra la entidad MME o el equipo UE que deduce claves en conformidad con una segunda forma de realización de la presente invención;

La Figura 7 representa otro diagrama esquemático que ilustra la entidad MME o el equipo UE que deduce claves en conformidad con una segunda forma de realización de la presente invención;

La Figura 8 representa un diagrama de flujo que ilustra el procedimiento de distribución de claves en conformidad con una tercera forma de realización de la presente invención;

La Figura 9 es un diagrama esquemático del sistema de distribución de claves de la red de comunicación móvil evolucionada en conformidad con una forma de realización de la presente invención;

La Figura 10 es un diagrama esquemático de un primer sistema de distribución de claves en conformidad con una forma de realización de la presente invención;

La Figura 11 es un diagrama esquemático de un segundo sistema de distribución de claves en conformidad con una forma de realización de la presente invención; y

La Figura 12 es un diagrama esquemático de un tercer sistema de distribución de claves en conformidad con una forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

Las formas de realización de la presente invención dan a conocer un método para la distribución de claves en una red de comunicación móvil. La red deduce, respectivamente, claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario, y distribuye las claves deducidas a un equipo UE y entidades que realizan una operación de seguridad pertinente en la red; el equipo UE puede deducir también claves para proteger la seguridad de la señalización AS, la señalización NAS y datos de usuario, por separado.

En las formas de realización de la invención, la deducción y la distribución de las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario pueden ponerse en práctica mediante dos formas: una es que la red deduce las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario y notifica al equipo UE la deducción de las mismas claves, y luego, la red distribuye las claves a entidades que realizan una operación de seguridad pertinente; la otra es que la red deduce las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario y distribuye, respectivamente, las claves al equipo de usuario UE y a las entidades que realizan una operación de seguridad pertinente.

La red tiene, además, dos formas para deducir las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario: una es que un servidor para memorizar información del usuario en la red deduce directamente las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario; la otra es que el servidor y una entidad MME deducen las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y los datos de usuario, de forma cooperativa.

A continuación se describe concretamente las formas de realización de la presente invención con los dibujos adjuntos.

Forma de realización 1

En esta forma de realización, el servidor HSS y el equipo UE deducen, respectivamente, las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario en conformidad con una clave compartida, y la entidad MME distribuye las claves a entidades que realizan una operación de seguridad pertinente.

La Figura 2 representa un diagrama de flujo que ilustra el procedimiento de distribución de claves en conformidad con una primera forma de realización de la presente invención. El servidor HSS y el equipo UE están previamente establecidos con una función de deducción KGA para deducir claves para proteger la señalización de AS, la señalización de NAS y los datos de usuario en conformidad con la clave compartida. El procedimiento para deducir y distribuir claves incluye las etapas siguientes:

Etapa 1: El equipo UE y el servidor HSS previamente comparten una o más claves.

La utilización compartida de claves en el equipo UE y en el servidor HSS puede ponerse en práctica estableciendo las mismas claves en el equipo UE y en el servidor HSS. El equipo UE y el servidor HSS pueden compartir previamente una o más claves, pares de claves públicas/privadas o certificados. En esta forma de realización, el equipo UE y el

servidor HSS comparten previamente una clave K.

Etapa 2: El servidor HSS deduce las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos del usuario.

El servidor HSS utiliza una función de deducción KG A para deducir claves CKas y IKas para la señalización de AS, claves CKnas e IKnas para la señalización de NAS, y claves CKu e IKu para datos de usuario en conformidad con la clave K previamente compartida. La clave CK es una clave que proporciona protección de encriptación y la clave IK es una clave que proporciona protección de la integridad, de forma similar a como se describe a continuación. El proceso de deducción de claves puede necesitar también algunos parámetros, a modo de ejemplo, un número aleatorio de dificultad de autenticación (RAND) generado por el servidor HSS.

A continuación se describe un ejemplo de claves para proteger la señalización de AS, la señalización de NAS y el plano de usuario. No todas las circunstancias se describen en esta especificación. En algunos casos, solamente se necesita la clave CKu si el plano del usuario necesita solamente protección de encriptación. Si las entidades que realizan la operación de seguridad son idénticas, las claves pueden ser también las mismas. A título de ejemplo, si una entidad que realiza una operación de seguridad para el plano del usuario es idéntica con la correspondiente a la señalización AS, las claves que protegen la seguridad de la señalización de AS pueden ser las mismas que las que protegen el plano del usuario. A la recepción de las claves, las entidades que realizan una operación de seguridad deducen, además, las claves realmente utilizadas para proteger la señalización de AS, la señalización de NAS y el plano del usuario. A título de ejemplo, el servidor HSS deduce una clave para proteger la seguridad del plano del usuario y distribuye la clave a la entidad que realiza la operación de seguridad del plano del usuario. La entidad deduce, además, una clave realmente utilizada para proteger el plano del usuario.

La Figura 3 representa el modo de deducción de claves de la forma de realización, es decir, la clave se deduce sobre la base de a función de deducción KGA, la clave K compartida y las RAND, KGA 1-6 son, respectivamente, las funciones de deducción para las claves CKas, IKas, CKnas, IKnas, CKu e IKu. Los procesos de deducción de todas las claves utilizan el mismo RAND. Los modos de deducción pueden variarse y no limitarse al modo ilustrado en la Figura 3. A modo de ejemplo, el servidor HSS puede generar tres grupos de claves sobre la base de un RAND o generar tres grupos de claves sobre la base de diferentes RANDs. El servidor HSS puede generar también claves para proteger la señalización de NAS en conformidad con RANDs y generar claves para proteger la señalización de AS y los datos de usuario mediante simples operaciones de desagregación y agregación.

La deducción de claves por el servidor HSS puede iniciarse mediante una demanda procedente de la entidad MME. A modo de ejemplo, después de que la entidad MME envíe una demanda de vector de autenticación (AV) el servidor HSS inicia la deducción de las claves.

Etapa 3: El servidor HSS envía las claves deducidas y el RAND generado a la entidad MME.

Esta información puede transmitirse a través de un mensaje de respuesta de AV y enviarse a la entidad MME.

Etapa 4: La entidad MME envía el número aleatorio RAND al equipo UE.

Esta información puede transmitirse en un mensaje de dificultad de autenticación y enviarse al equipo UE.

Etapa 5: El equipo UE deduce claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario.

El equipo UE utiliza la función de deducción KGA para deducir las claves CKas e IKas para la señalización de AS, CKnas e IKnas para la señalización de NAS, CKu e IKu para los datos de usuario en conformidad con la clave K previamente compartida y el número RAND generado por el servidor HSS. Habida cuenta de la función de deducción, la clave compartida y el parámetro adoptado por el equipo UE en el proceso de deducción de claves son los mismos que los adoptados por el servidor HSS en el proceso de deducción de claves, las claves deducidas por el equipo UE son las mismas que las deducidas por el servidor HSS. La Figura 3 ilustra un modo de deducción.

El equipo UE puede incluir una tarjeta inteligente y un terminal. La deducción de claves puede realizarse en la tarjeta inteligente o en el terminal o, a la vez, en el terminal y en la tarjeta inteligente.

Etapa 6: El equipo UE envía un mensaje de confirmación a la entidad MME.

El mensaje de confirmación puede ser un mensaje de respuesta de autenticación.

Etapa 7: La entidad MME distribuye las claves recibidas desde el servidor HSS a entidades que realizan una operación de seguridad pertinente.

A modo de ejemplo, la entidad MME distribuye las claves CKas e IKas a la red de acceso evolucionada y las claves

CKu e IKu a la entidad UPE.

En el procedimiento anterior, la entidad MME, antes o en el momento de enviar el número aleatorio RAND al equipo UE, puede distribuir las claves recibidas desde el servidor HSS a entidades que realizan una operación de seguridad pertinente.

Forma de realización 2

En esta forma de realización, el servidor HSS y el equipo de usuario UE deducen una clave raíz de forma cooperativa. La entidad MME y el equipo UE deducen, respectivamente, las claves para proteger la señalización de AS, la señalización de NAS y los datos de usuario en conformidad con la clave raíz. La entidad MME distribuye las claves a las entidades de red que realizan una operación de seguridad pertinente.

La Figura 4 representa un diagrama de flujo que ilustra el procedimiento de distribución de claves en conformidad con una segunda forma de realización de la presente invención. El servidor HSS y el equipo de usuario UE están preestablecidos con una misma función de deducción HA de la clave raíz. La entidad MME y el equipo de usuario UE están preestablecidos con una misma función de deducción MA para deducir las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario. El procedimiento para generar y distribuir claves incluye las etapas siguientes:

Etapa 1: El equipo UE y el servidor HSS comparten previamente una o más claves.

La utilización compartida de claves en el equipo UE y en el servidor HSS puede ponerse en práctica estableciendo las mismas claves en el equipo UE y en el servidor HSS. El equipo UE y el servidor HSS pueden compartir previamente una o más claves, pares de claves públicas/privadas o certificados. En esta forma de realización, el equipo UE y el servidor HSS comparten previamente una clave K.

Etapa 2: El servidor HSS deduce una clave raíz.

El servidor HSS utiliza la función de deducción de clave raíz HA para deducir una o más claves raíces en conformidad con la clave K previamente compartida con el equipo UE. Pueden existir una o más funciones de deducción de claves raíces y puede deducirse una o más claves raíces. El proceso de deducción de clave raíz puede necesitar algunos otros parámetros, tales como un número RAND generado por el servidor HSS. En la forma de realización, la función de deducción de clave raíz HA1 se utiliza para deducir la clave raíz de cifrado CKm y la función HA2 se utiliza para deducir la clave de integridad raíz IKm. El modo de deducción se ilustra en la Figura 5. Los modos de deducción de claves raíces pueden variarse y no limitarse al modo ilustrado en la Figura 5.

La deducción de clave raíz por el servidor HSS puede iniciarse por una demanda procedente de la entidad MME. A modo de ejemplo, después de que la entidad MME envíe una demanda de vector de autenticación (AV), el servidor HSS inicia la deducción de claves.

Etapa 3: El servidor HSS envía las claves raíces deducidas CKm e IKm y el número aleatorio RAND generado a la entidad MME.

Esta información puede transmitirse en un mensaje de respuesta de AV y enviarse a la entidad MME.

Etapa 4: La entidad MME deduce claves para proteger la seguridad de la señalización de AS, la señalización de NAS y los datos de usuario.

La entidad MME utiliza las funciones de deducción HA1-6 para deducir las claves CKas e IKas para la señalización de AS, CKnas e IKnas para la señalización de NAS, CKu e IKu para los datos de usuario en conformidad con las claves raíces recibidas CKm e IKm. El proceso de deducción puede necesitar algunos otros parámetros, a modo de ejemplo, un RANDmme generado por la entidad MME.

La Figura 6 y la Figura 7 ilustran, respectivamente, un modo de deducción de claves. La diferencia radica en lo que sigue: en el modo de deducción ilustrado en la Figura 6, las claves raíces CKM e IKm son necesarias para deducir todas las claves, mientras que en el modo de deducción ilustrado en la Figura 7, las claves CKm e IKm se necesitan, respectivamente, para deducir la clave de cifrado y la clave de integridad.

Los modos de deducción pueden variarse y no limitarse a los modos ilustrados en las Figuras 6 y 7. Los procesos en los que la entidad MME deduce claves para proteger la señalización de AS, la señalización de NAS y datos de usuario pueden ser independientes o asociados. A modo de ejemplo, la entidad MME puede generar tres grupos de claves sobre la base de un número aleatorio RAND o generar tres grupos de claves sobre la base de números RANDs diferentes. La entidad MME puede generar también claves para proteger la señalización de NAS en conformidad con los números aleatorios RANDs y generar claves para proteger la señalización de AS y los datos de usuario mediante simples procedimientos de desagregación y agregación. La entidad MME puede utilizarse también directamente la

clave raíz como la clave para proteger la seguridad de la señalización de NAS o datos de usuario.

Etapa 5: La entidad MME envía los números RANDmme y RAND recibidos desde el servidor HSS hacia el equipo de usuario UE.

Esta información puede transmitirse en un mensaje de dificultad de autenticación y enviarse al equipo UE.

Etapa 6: El equipo UE deduce claves para proteger la seguridad de la señalización de AS, la señalización de NAS y datos de usuario.

El equipo UE utiliza la función de deducción de clave raíz para deducir la clave raíz en conformidad con la clave K previamente compartida con el servidor HSS y el número RAND.

Habida cuenta de la función de deducción, la clave compartida y el parámetro adoptados por el equipo UE, en el proceso de deducción de claves raíces, son los mismos que los adoptados por el servidor HSS en el proceso de deducción de claves raíces, las claves deducidas por el equipo UE son las mismas que las deducidas por el servidor HSS. El modo de deducción es según se ilustra en la Figura 5.

Después de deducir las claves raíces, el equipo UE utiliza las funciones de deducción MA1-6 para deducir las claves CKas e IKas para la señalización de AS, las claves CKnas e IKnas para la señalización de NAS, las claves CKu e IKu para la seguridad de datos de usuario en conformidad con el parámetro RANDmme generado por la entidad MME y las claves raíces CKm e IKm. Habida cuenta de la función de deducción, la clave compartida y el parámetro adoptado por el equipo UE en el proceso de deducción de claves raíces son los mismos que los adoptados por el servidor HSS en el proceso de deducción de claves raíces, las claves deducidas por el equipo UE son las mismas que las deducidas por la entidad MME. Los modos de deducción son según se ilustran en las Figuras 6 y 7.

El equipo UE puede incluir una tarjeta inteligente y un terminal. La deducción de las claves raíces CKm e IKm puede realizarse en la tarjeta inteligente o en el terminal. Y las claves CKas, IKas, CKnas, IKnas, CKu e IKu pueden deducirse en la tarjeta inteligente o en el terminal.

Etapa 7: El equipo UE envía un mensaje de confirmación a la entidad MME.

El mensaje de confirmación puede ser un mensaje de respuesta de autenticación.

Etapa 8: La entidad MME distribuye las claves generadas a entidades pertinentes que realizan la operación de seguridad. A modo de ejemplo, la entidad MME distribuye las claves CKas e IKas que protegen la señalización de AS para la red de acceso evolucionada y distribuye las claves CKu e IKu que protegen la seguridad de los datos de usuario hacia la entidad UPE.

En el procedimiento anterior, la entidad MME, antes o en el momento de envío del número aleatorio RAND y RANDmme al equipo UE, puede distribuir las claves deducidas a entidades que realizan una operación de seguridad pertinente.

En la forma de realización, el equipo UE deduce la clave raíz y las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y el plano de usuario, simultáneamente. El equipo UE puede deducir también estas claves por separado. Es decir, la entidad MME envía primero los parámetros para deducir las claves raíces al equipo UE. El equipo UE deduce la clave raíz. A continuación, la entidad MME envía las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y el plano de usuario al equipo UE. El equipo UE deduce las claves para proteger la seguridad de la señalización de AS, señalización de NAS y el plano de usuario en conformidad con la clave raíz.

Forma de realización 3

En esta forma de realización, el servidor HSS y la entidad UPE deducen una clave raíz de forma cooperativa. La entidad MME deduce las claves para proteger la señalización de AS, la señalización de NAS y los datos de usuario y la entidad MME realiza el cifrado de las claves con la clave raíz y las distribuye al equipo UE y a las entidades de red que realizan una operación de seguridad.

La Figura 8 ilustra un diagrama de flujo que representa el proceso de distribución de claves en conformidad con una tercera forma de realización de la presente invención. El servidor HSS y el equipo UE son previamente establecidos con la función de deducción de claves raíces HA. El procedimiento para deducir y distribuir claves incluye las etapas siguientes:

Las etapas 1-4 son las mismas que las etapas 1 a 4 en la forma de realización 2.

Etapa 5: La entidad MME realiza el cifrado de las claves deducidas para proteger la señalización de AS, la señalización

de NAS y los datos de usuario con la clave raíz, y envía las claves cifradas al equipo UE. El proceso en que la entidad MME deduce las claves es el mismo que el descrito para la forma de realización 2. Las claves pueden deducirse también utilizando otros métodos.

Esta información puede transmitirse en un mensaje de dificultad de autenticación y enviarse al equipo UE.

Etapa 6: El equipo UE deduce la clave raíz y analiza sintácticamente las claves recibidas con la clave raíz.

Etapa 7: El equipo UE envía un mensaje de confirmación a la entidad MME.

El mensaje de confirmación puede ser un mensaje de respuesta de autenticación.

Etapa 8: La entidad MME distribuye las claves a entidades pertinentes que realizan la operación de seguridad.

A modo de ejemplo, la entidad MME distribuye las claves CKas e IKas a la red de acceso evolucionada y las claves CKu e IKu a la entidad UPE. Las claves distribuidas por la entidad MME no están cifradas con la clave raíz.

En el procedimiento anterior, la entidad MME, puede distribuir las claves a entidades pertinentes que realizan una operación de seguridad antes o en el momento de enviar las claves cifradas al equipo UE.

Forma de realización 4

En esta forma de realización el servidor HSS y el equipo UE deducen una clave raíz de forma cooperativa. La entidad MME y el equipo UE deducen, respectivamente, las claves para proteger la señalización de AS, la señalización de NAS y los datos de usuario en conformidad con la clave raíz. La entidad MME distribuye las claves a las entidades de red que realizan una operación de seguridad. Las entidades de red que realizan una operación de seguridad deducen, además, claves que protegen la señalización de AS, la señalización de NAS y datos de usuario en conformidad con las claves recibidas. En la forma de realización, la entidad que protege la señalización de AS también protege los datos del plano de usuario. Por lo tanto, la clave que protege la señalización de AS es la misma que la que protege los datos de usuario.

El servidor HSS y el equipo UE son previamente establecidos con la misma función de deducción de la clave raíz. La entidad MME y el equipo UE son previamente establecidos con la misma función de deducción MA para deducir claves para proteger la señalización de AS, la señalización de NAS y los datos de usuario. El procedimiento para generar y distribuir claves incluye las etapas siguientes:

Etapa 1: El equipo UE y el servidor HSS comparten previamente una o más claves.

A modo de ejemplo, el equipo UE y el servidor HSS comparten previamente una clave K en esta forma de realización.

Etapa 2: El servidor HSS deduce una clave raíz.

El servidor HSS deduce una clave raíz Km en conformidad con la clave K previamente compartida con el equipo UE.

Etapa 3: El servidor HSS envía la clave raíz Km deducida y el parámetro necesario para el equipo UE para poder deducir la clave Km para la entidad MME.

Etapa 4: La entidad MME envía el parámetro necesario para deducir la clave Km para el equipo UE.

Etapa 5: El equipo UE deduce la clave raíz Km.

Etapa 6: La entidad MME deduce claves para proteger la señalización de AS, la señalización de NAS y los datos de usuario en conformidad con la clave raíz recibida desde el servidor HSS.

La entidad MME deduce claves CKnas e IKnas que protegen la señalización de NAS y la clave Kran que protege la señalización de AS y los datos de usuario. El proceso de deducción puede necesitar algunos otros parámetros, a modo de ejemplo, un parámetro RANDmme generado por la entidad MME.

Etapa 7: El equipo UE recibe los parámetros para deducir las claves que protegen la señalización de AS, la señalización de NAS y los datos de usuario. El equipo UE deduce claves CKnas e IKnas que protegen la señalización de NAS y Kran que protege la señalización de AS y los datos de usuario en conformidad con la clave raíz Km deducida por sí mismo.

Etapa 8: La entidad MME distribuye las claves deducidas para la entidad que protege la seguridad de la señalización de NAS y la entidad que protege la seguridad de la señalización de AS y los datos de usuario. En esta forma de realización, la entidad que protege la seguridad de la señalización de AS también protege la seguridad de los datos

de usuario. El equipo UE y la entidad que protege la señalización de AS y los datos de usuario, sobre la base de la clave Kran, deducen las claves realmente utilizadas para proteger la señalización de AS y los datos de usuario, tal como las claves CKas, IKas y CKup.

En las formas de realización precedentes 1 a 4, si el proceso de deducción necesita algunos otros parámetros y el equipo UE tiene dichos parámetros, resulta innecesario enviar dichos parámetros al equipo UE.

En las formas de realización 1 a 4 precedentes, las entidades que realizan la operación de seguridad, a la recepción de las claves, puede utilizar las claves para proteger la comunicación entre el equipo UE y las entidades. Las entidades pueden deducir, además, las claves derivadas en conformidad con las claves recibidas para proteger la comunicación entre el equipo UE y las entidades. En este caso, puede existir una sola clave, tal como una clave raíz, en lugar de dos claves.

Si la entidad que protege la señalización de NAS es la misma que la protege los datos de usuario, las claves que protegen la señalización de NAS y los datos de usuario pueden ser las mismas. A modo de ejemplo, en la forma de realización 1, la clave CKnas puede ser la misma que la clave CKu. Es decir, si el servidor HSS y el equipo UE utilizan la misma función de deducción para deducir las claves CKnas y CKu, puede reducirse el número de la función utilizada por el servidor HSS y el equipo UE. De modo similar, si la entidad que protege la señalización de AS es idéntica que la que protege los datos de usuario, las claves que protegen la señalización de AS y los datos de usuario pueden ser las mismas.

Puesto que no todos los tipos de información necesitan protección de integridad y de encriptación, algunas de las claves descritas en las formas de realización pueden no ser necesarias. A modo de ejemplo, si la señalización de AS no necesita una protección de encriptación, las claves que protegen la señalización de AS pueden incluir la clave de integridad IKas solamente. A modo de otro ejemplo, si los datos de usuario no necesitan una protección de integridad, las claves que protegen los datos de usuario pueden incluir la clave de cifrado CKu solamente.

Sobre la base del método para deducir y distribuir claves en la red evolucionada anteriormente descrita, las formas de realización de la invención dan a conocer un sistema para distribuir claves en la red evolucionada, lo que se describirá con más detalle a continuación.

La Figura 9 es un diagrama esquemático de un sistema de distribución de claves en la red de comunicación móvil evolucionada en conformidad con una forma de realización de la presente invención. Un sistema para la distribución de claves en la red de comunicación móvil evolucionada incluye: un lado de usuario y una red, en donde el lado de usuario incluye un equipo UE y la red incluye un módulo de deducción de claves que deduce claves para proteger la señalización de AS, la señalización de NAS y datos de usuario, un módulo de distribución de claves y entidades que realizan una operación de seguridad. El módulo de deducción de claves distribuye las claves deducidas para proteger la señalización de AS, la señalización de NAS y datos de usuario para el módulo de distribución de claves. El módulo de distribución de claves distribuye las claves recibidas a entidades que realizan una operación de seguridad o además, al equipo de usuario UE. El equipo UE puede deducir también claves para proteger la seguridad de la señalización de AS, la señalización de NAS y los datos de usuario por sí mismo.

Formas de realización de la presente invención dan a conocer tres arquitecturas del sistema de distribución de claves.

La Figura 10 es un diagrama esquemático de un primer sistema de distribución de claves en conformidad con una forma de realización de la presente invención. El primer sistema de distribución de claves corresponde al procedimiento para deducir y distribuir claves que se describe en la forma de realización 1.

En el sistema, el módulo de distribución de claves está situado en la entidad MME. El sistema incluye dos módulos de deducción de claves idénticos, respectivamente situados en el equipo UE y situados en el servidor HSS en la red. El módulo de deducción de claves en el servidor HSS está conectado con el módulo de distribución de claves en la entidad MME.

Los módulos de deducción de claves en el servidor HSS y el equipo de usuario UE son previamente preestablecidos con el mismo algoritmo de deducción y uno o más pares de claves públicas/privadas o certificados para deducir claves. Los módulos de deducción de claves en el servidor HSS y en el equipo de usuario UE deducen las mismas claves para proteger la señalización de AS, la señalización de NAS y datos de usuario.

El módulo de deducción de claves en el servidor HSS distribuye las claves deducidas al módulo de distribución de claves en la entidad MME. El módulo de distribución de claves distribuye las claves, respectivamente, a entidades de red que realizan una operación de seguridad.

La Figura 11 es un diagrama esquemático de un segundo sistema de distribución de claves en conformidad con una forma de realización de la presente invención. Un primer sistema de distribución de claves corresponde al procedimiento para deducir y distribuir claves que se describe en la forma de realización 1.

En el sistema, el módulo de distribución de claves está situado en la entidad MME. El sistema incluye dos módulos de deducción de claves idénticos, situados, respectivamente, en la entidad MME en la red y en el equipo de usuario UE. El módulo de deducción de claves en la entidad MME está conectado con el módulo de distribución de claves en la MME. El sistema incluye también dos módulos de deducción de claves raíces idénticos, situados respectivamente en el servidor HSS en la red y en el equipo de usuario UE. El módulo de deducción de claves raíces en el servidor HSS está conectado con el módulo de deducción de claves en la entidad MME.

Los módulos de deducción de claves en la entidad MME y en el equipo de usuario UE están previamente establecidos con el mismo algoritmo de deducción de claves y uno o más mismos pares de claves públicas/privadas o certificados para deducir las claves. Los módulos de deducción de claves raíces en el servidor HSS y en el equipo de usuario UE son previamente establecidos con el mismo algoritmo de deducción de claves, y uno o más mismos pares de claves públicas/privadas o certificados para deducir claves raíces.

El módulo de deducción de clave raíz en el servidor HSS deduce la misma clave raíz que las deducidas por el módulo de deducción de claves raíces en el equipo de usuario UE. El módulo de deducción de claves raíces en el servidor HSS envía la clave raíz deducida al módulo de deducción de claves en la entidad MME. Los módulos de deducción de claves en la entidad MME y en el equipo UE deducen las mismas claves para proteger la señalización de AS, la señalización de NAS y los datos de usuario en conformidad con las mismas claves raíces. El módulo de deducción de claves en la entidad MME distribuye las claves deducidas al módulo de distribución de claves en la entidad MME. El módulo de distribución de claves distribuye las claves, respectivamente, a entidades de red que realizan operaciones de seguridad pertinentes.

La Figura 12 es un diagrama esquemático de un tercer sistema de distribución de claves en conformidad con una forma de realización de la presente invención. El tercer sistema de distribución de claves corresponde al procedimiento para deducir y distribuir claves descrito en la forma de realización 3.

En el sistema, el módulo de distribución de claves y el módulo de deducción de claves están en la entidad MME. El sistema incluye también dos módulos de deducción de claves, situados respectivamente en el servidor HSS y en el equipo de usuario UE. El módulo de deducción de claves raíces en el servidor HSS está conectado con el módulo de deducción de claves en la entidad MME. En el sistema, el equipo de usuario UE incluye un módulo de descifrado de claves o un módulo de recepción de claves, que está conectado con el módulo de deducción de claves raíces en el equipo UE y el módulo de distribución de claves en la entidad MME.

Los módulos de deducción de claves raíces en el servidor HSS y en el equipo UE son previamente establecidos con el mismo algoritmo de deducción de claves, y uno o más mismos pares de claves públicas/privadas o certificados para deducir claves raíces. El módulo de deducción de claves raíces en el servidor HSS deduce la misma clave raíz que las deducidas por el módulo de deducción de claves raíces en el equipo UE. El módulo de deducción de claves raíces en el servidor HSS envía las claves raíces deducidas al módulo de deducción de claves en la entidad MME. El módulo de deducción de claves en la entidad MME deduce las claves para proteger la señalización de AS, la señalización de NAS y los datos de usuario y envía las claves al módulo de distribución de claves en la entidad MME. La entidad MME utiliza la clave raíz recibida para efectuar el cifrado de las claves deducidas y enviarlas al módulo de distribución de claves en la entidad MME. El módulo de distribución distribuye las claves cifradas al equipo UE y las claves no cifradas a las entidades de red que realizan operaciones de seguridad pertinentes. A la recepción de las claves cifradas enviadas por la entidad MME, el módulo de descifrado de claves en el equipo UE obtiene una clave raíz a partir del módulo de deducción de claves raíces en el equipo UE, y utiliza la clave raíz para descifrar las claves para proteger la señalización de AS, señalización de NAS y los datos de usuario.

En conformidad con los procedimientos anteriores, un método para distribuir claves proporcionadas por las formas de realización de la invención deduce claves para proteger la señalización de AS, la señalización de NAS y datos de usuario, y distribuye las claves al equipo UE y las entidades de red que realizan una operación de seguridad. Formas de realización de la presente invención proporcionan varios métodos para deducir y distribuir claves, que incluyen: el servidor HSS en la red y el equipo UE deducen, respectivamente, claves y la entidad MME distribuye las claves a entidades de red que realizan una operación de seguridad; o bien, el servidor HSS y la entidad MME en la red deducen claves de forma cooperativa, la entidad MME distribuye las claves a entidades de red que realizan una operación de seguridad y el equipo UE deduce claves de forma separada; o bien, el servidor HSS y la entidad MME en la red deducen claves por separado, y la entidad MME distribuye las claves al equipo UE y las entidades de red que realizan una operación de seguridad pertinente. Formas de realización de la invención dan a conocer varias opciones y mejoran la flexibilidad del sistema.

Aunque la invención ha sido descrita utilizando algunas formas de realización a modo de ejemplo, la invención no está limitada a dichas formas de realización. Es evidente que los expertos en esta técnica pueden realizar modificaciones y variaciones a la invención sin desviarse por ello del alcance de la invención. La invención está prevista para cubrir las modificaciones y variaciones a condición de que caigan dentro del alcance de protección definido por las reivindicaciones siguientes o sus equivalentes.

REIVINDICACIONES

1. Un método para la deducción de claves en una red de comunicación inalámbrica, que comprende: deducir, por un servidor de abonado local, HSS, una clave raíz;

enviar, por el HSS, la clave raíz a una entidad de gestión de la movilidad, MME;

deducir, por la MME, claves para proteger la seguridad de un estrato de acceso, AS, una señalización de estrato de no acceso, NAS, y datos de usuarios de conformidad con la clave raíz.

2. El método según la reivindicación 1, en donde la deducción de la clave raíz por el HSS comprende:

deducir, por el HSS, la clave raíz de conformidad con una función de deducción preestablecida y una o más claves en el HSS, estando las unas o más claves compartidas con un equipo de usuario, UE.

3. El método según la reivindicación 1, en donde la deducción, por la MME, de las claves de conformidad con la clave raíz comprende:

deducir, por la MME, las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y los datos del usuario de conformidad con una función de deducción preestablecida y la clave raíz.

4. El método según una cualquiera de las reivindicaciones 1 a 3, en donde:

las claves para proteger la seguridad de la señalización de AS comprenden, además, una clave para protección del cifrado y/o una clave para protección de la integridad; las claves para proteger la seguridad de la señalización de NAS comprenden, además, una clave para protección del cifrado y/o una clave para protección de la integridad; y las claves para proteger la seguridad de los datos de uso comprenden, además, una clave para protección del cifrado y/o una clave para protección de la integridad.

5. Un sistema para la deducción de claves en una red de comunicación inalámbrica, que comprende un servidor de abonado local, HSS, y una entidad de gestión de la movilidad, MME; en donde:

el servidor HSS está configurado para deducir una clave raíz y enviar la clave raíz a la MME;

la MME está configurada para deducir claves para proteger la seguridad de una señalización de estrato de acceso, AS, una señalización de estrato de no acceso, NAS, y datos de usuario de conformidad con la clave raíz.

6. El sistema según la reivindicación 5, en donde el servidor HSS está configurado, además, para:

deducir la clave raíz de conformidad con una función de deducción preestablecida y una o más claves en el HSS, estando la una o más claves compartidas con un equipo de usuario, UE.

7. El sistema según la reivindicación 5, en donde la MME está configurada, además, para:

deducir las claves para proteger la seguridad de la señalización de AS, la señalización de NAS y los datos del usuario de conformidad con una función de deducción preestablecida y la clave raíz.

8. El sistema según una cualquiera de las reivindicaciones 5 a 7, en donde:

las claves para proteger la seguridad de la señalización de AS comprenden, además, una clave para la protección del cifrado y/o una clave para la protección de la integridad; las claves para proteger la seguridad de la señalización de NAS comprenden, además, una clave para la protección del cifrado y/o una clave para la protección de la integridad; y las claves para proteger la seguridad de los datos de uso comprenden, además, una clave para la protección del cifrado y/o una clave para la protección de la integridad.

9. Un equipo de usuario, UE, configurado para:

deducir una clave raíz de conformidad con una función de deducción preestablecida y una o más claves en el equipo UE, estando las una o más claves compartidas con un servidor de abonado local, HSS;

deducir las claves para proteger la seguridad de una señalización de estrato de acceso, AS, una señalización de estrato de no acceso, NAS, y datos de usuario de conformidad con la clave raíz.

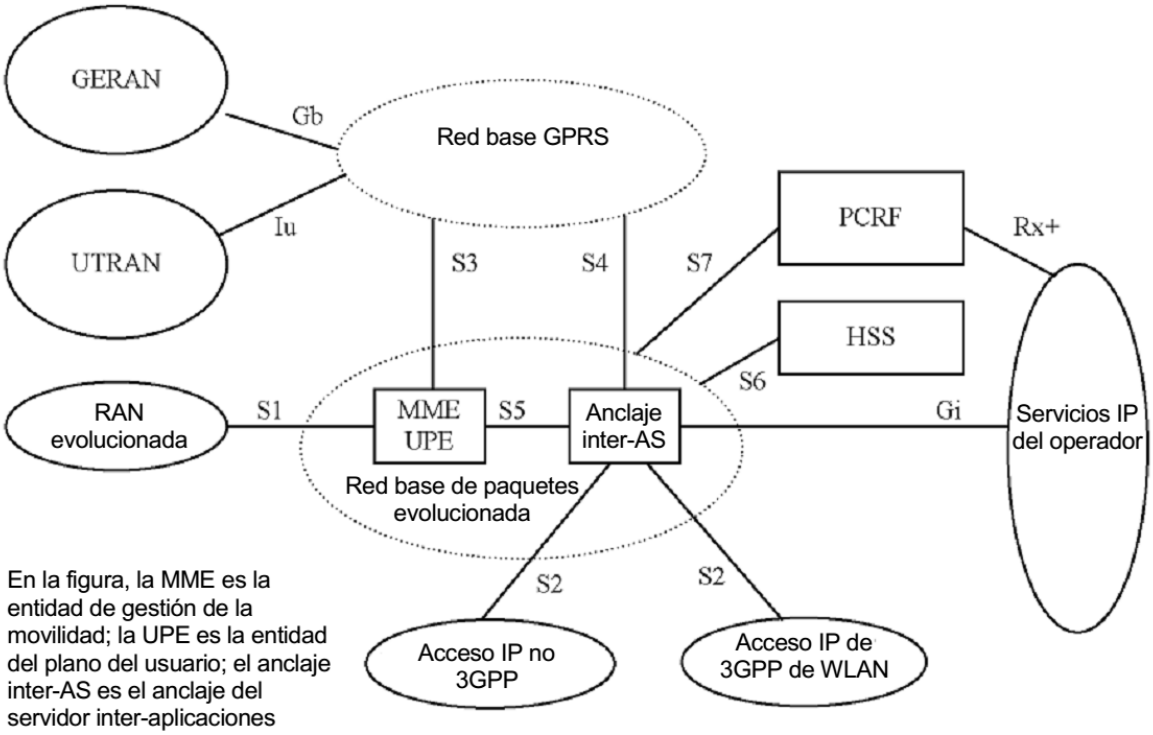
GERAN
Gb
Red base GPRS
UTRAN
Iu
S3
S4
S7
PCRF
Rx+
HSS
S6
RAN evolucionada
S1
MME UPE
S5
Anclaje inter-AS
Gi
Servicios IP del operador
Red base de paquetes evolucionada
S2
S2
Acceso IP no 3GPP
Acceso IP de 3GPP de WLAN
En la figura, la MME es la entidad de gestión de la movilidad; la UPE es la entidad del plano del usuario; el anclaje inter-AS es el anclaje del servidor inter-aplicaciones

Figura 1

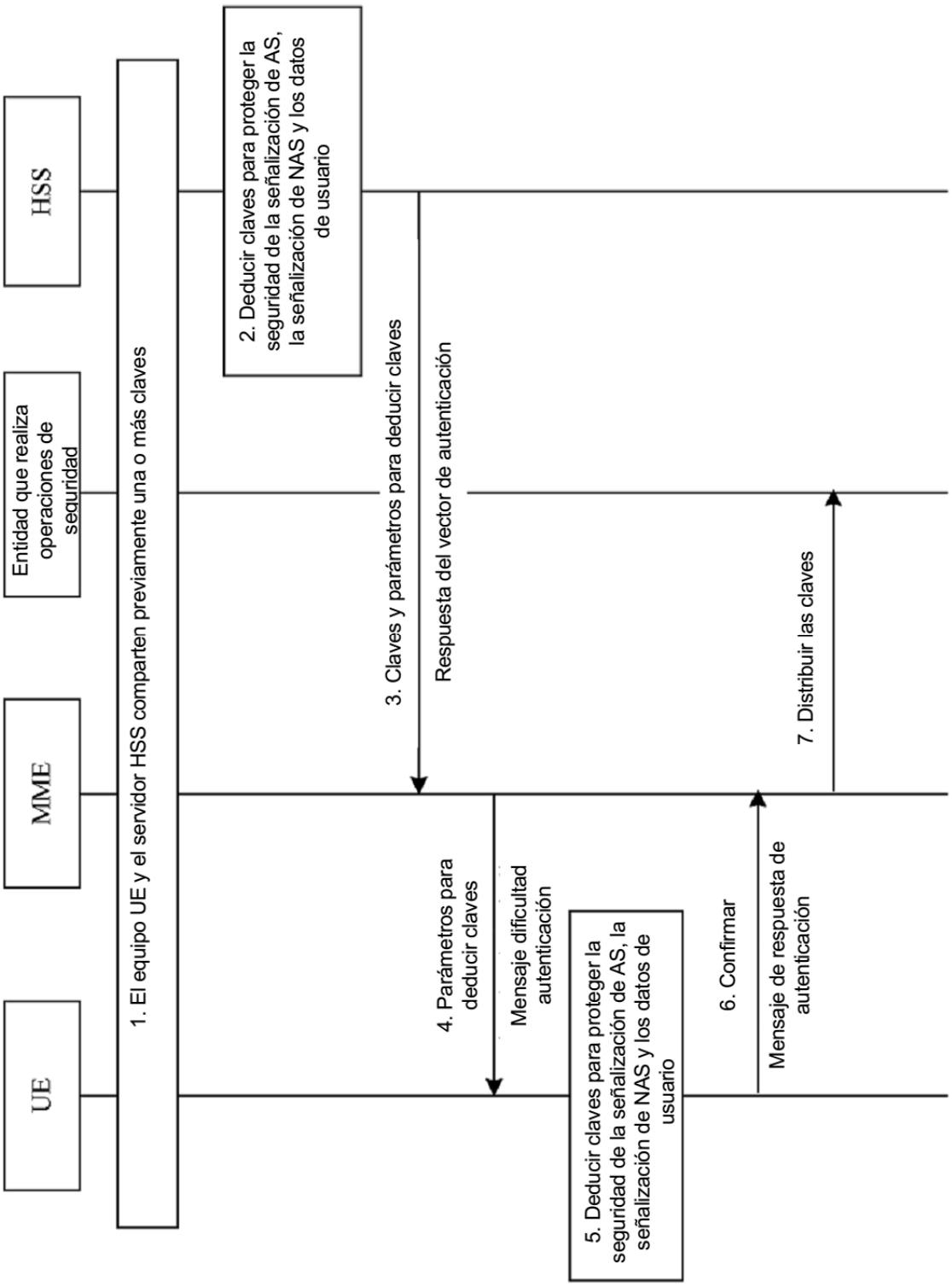
UE
MME
Entidad que realiza operaciones de seguridad
HSS
1. El equipo UE y el servidor HSS comparten previamente una o más claves
2. Deducir claves para proteger la seguridad de la señalización de AS, la señalización de NAS y los datos de usuario
3. Claves y parámetros para deducir claves
Respuesta del vector de autenticación
4. Parámetros para deducir claves
Mensaje dificultad autenticación
5. Deducir claves para proteger la seguridad de la señalización de AS, la señalización de NAS y los datos de usuario
6. Confirmar
Mensaje de respuesta de autenticación
7. Distribuir las claves

Figura 2

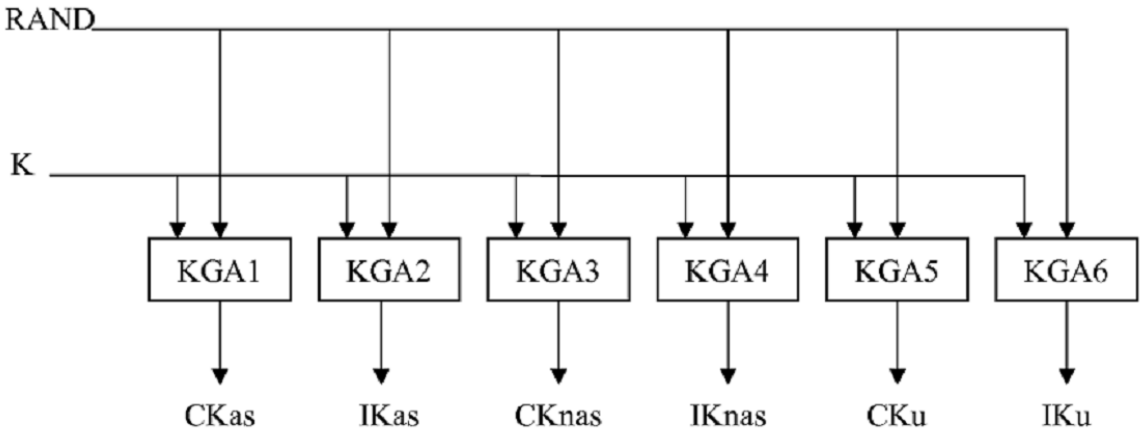

Figura 3

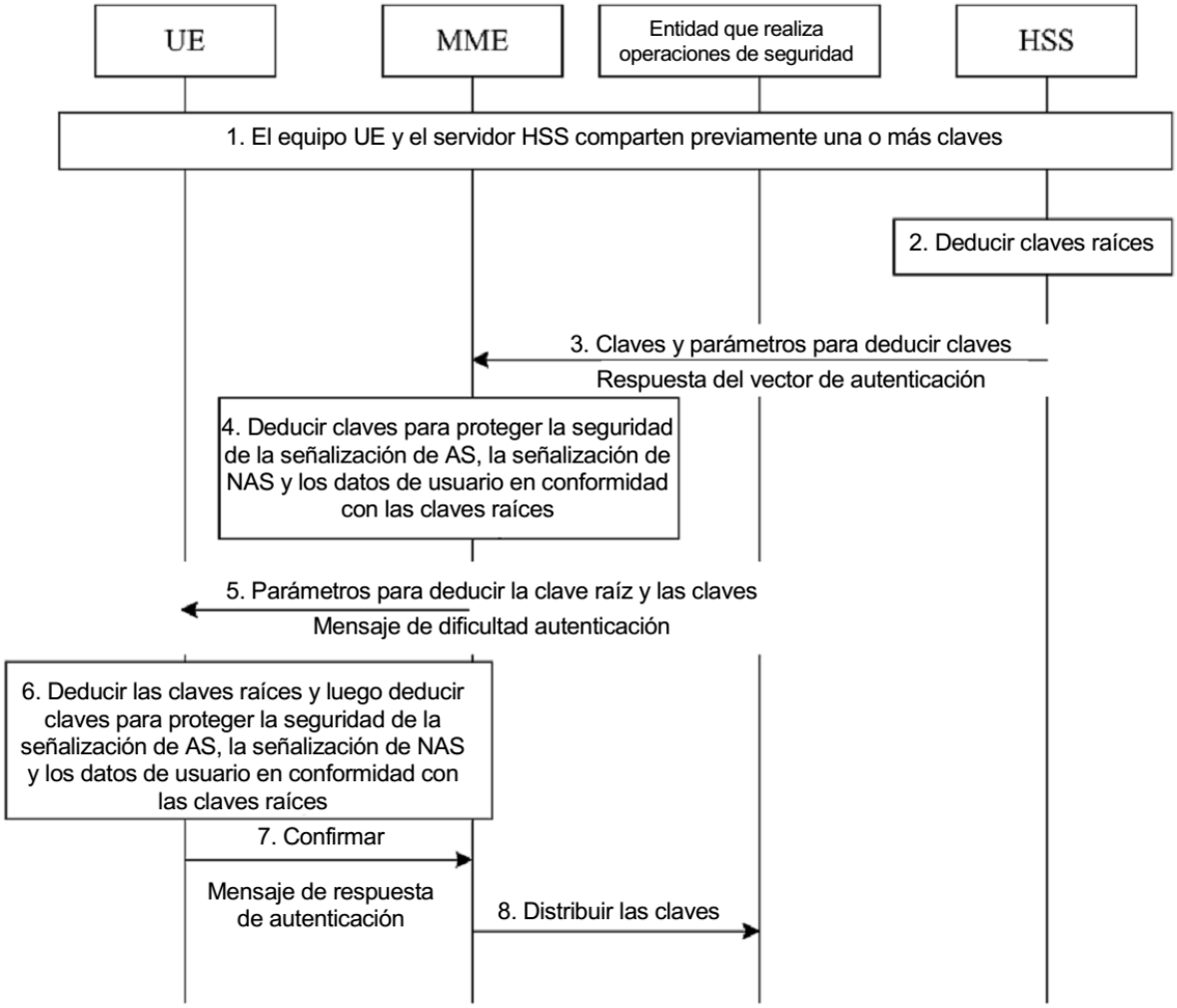

Figura 4

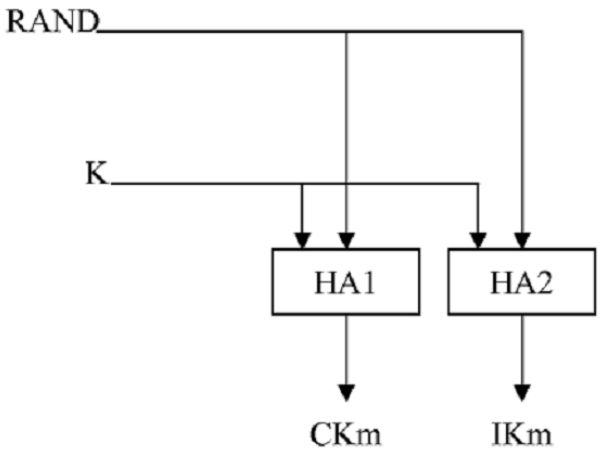

Figura 5

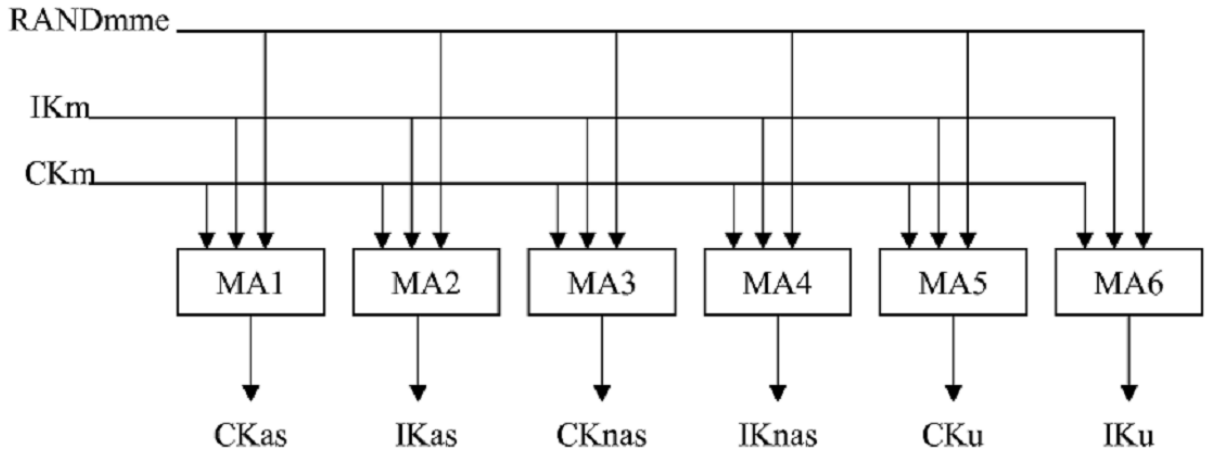

Figura 6

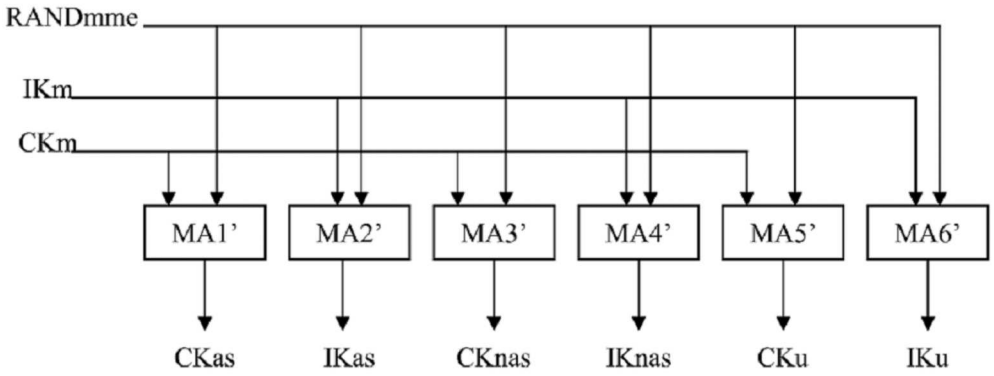

Figura 7

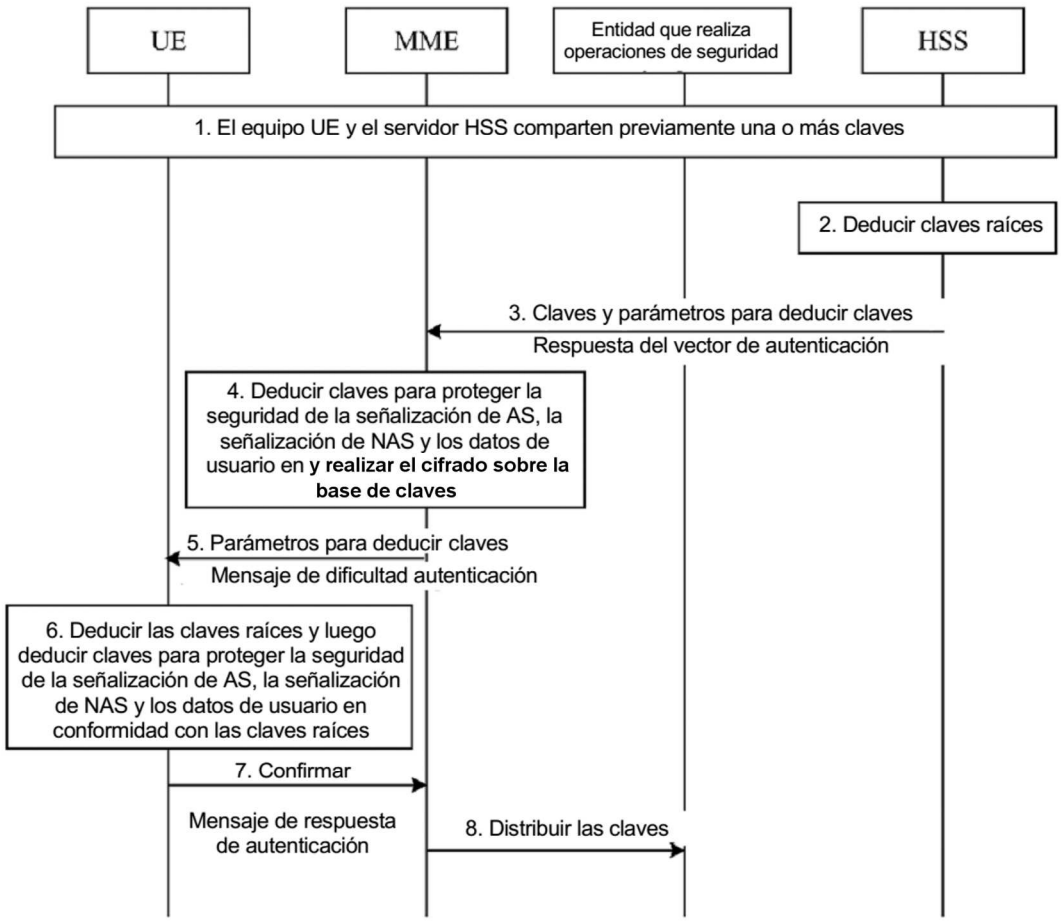

Figura 8

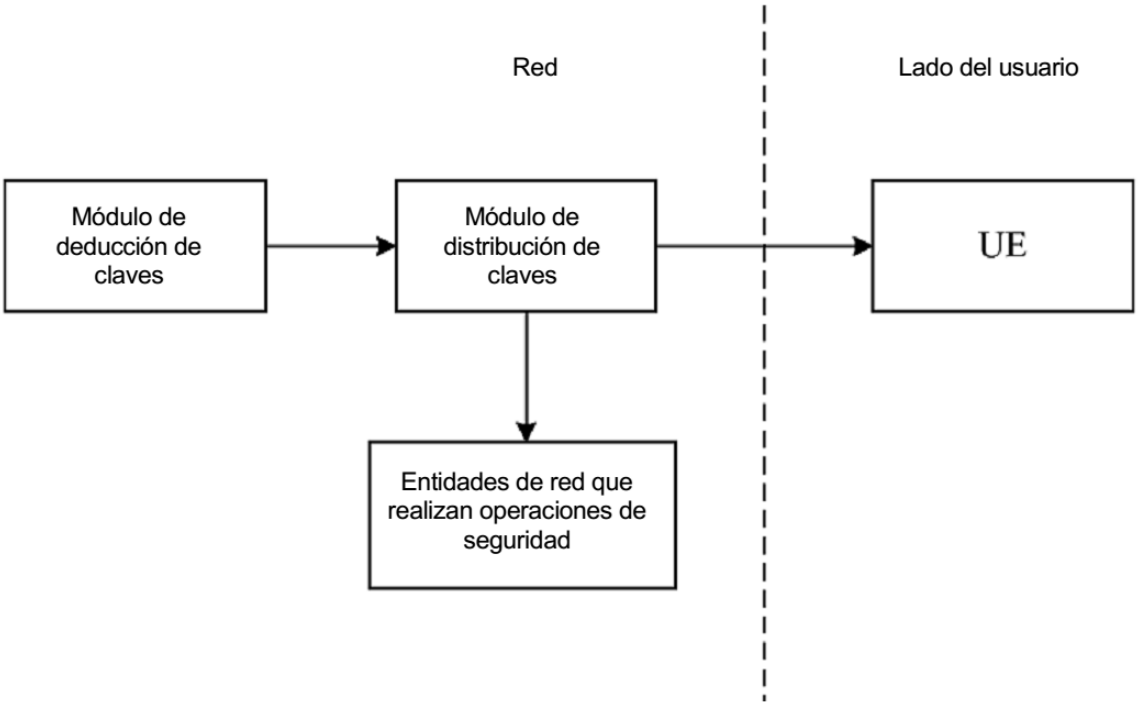

Figura 9

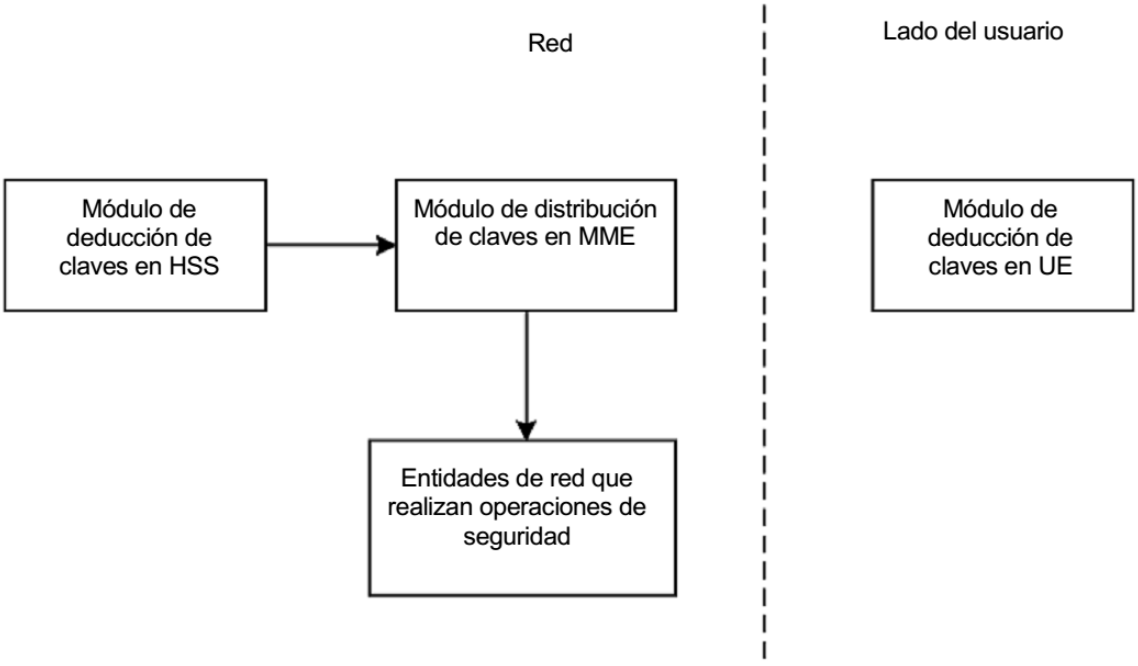

Figura 10

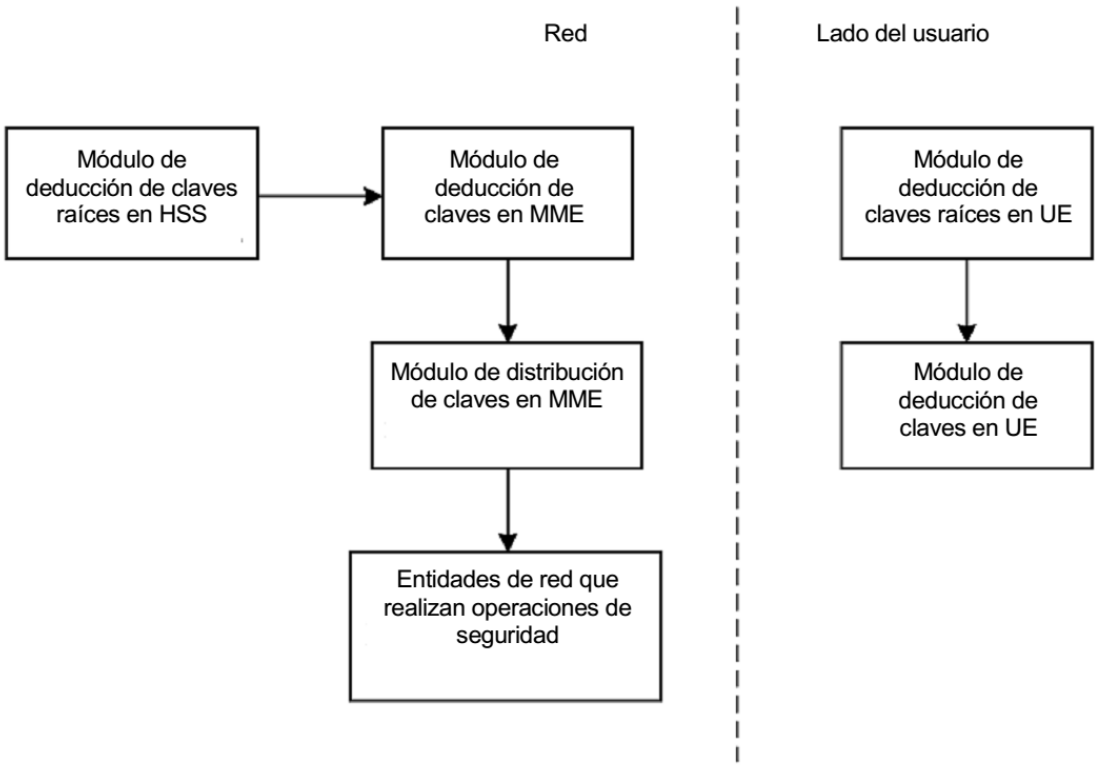

Figura 11

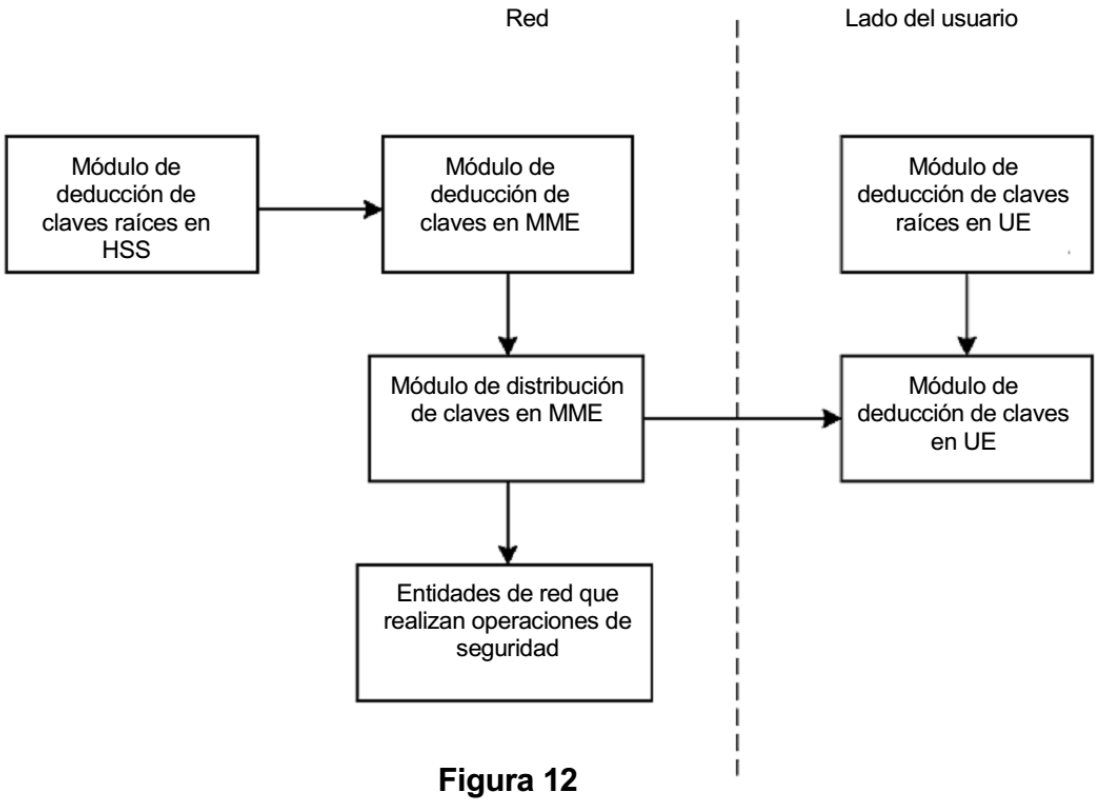

Figura 12