(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 554 671**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.01.2011 E 11701966 (1)**

(97) Fecha y número de publicación de la concesión europea: **16.09.2015 EP 2529566**

(54) Título: **Autenticación eficaz de terminal en redes de telecomunicaciones**

(30) Prioridad:

28.01.2010 EP 10151964

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.12.2015

(73) Titular/es:

KONINKLIJKE KPN N.V. (50.0%)
Maanplein 55
2516 CK The Hague, NL y
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO (50.0%)

(72) Inventor/es:

FRANSEN, FRANK

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Autenticación eficaz de terminal en redes de telecomunicaciones

CAMPO DE LA INVENCIÓN

En general, la invención se refiere al campo de la autenticación de terminales en redes de telecomunicaciones de acceso inalámbrico. Más en particular, la invención se refiere al campo de la autenticación de terminales en redes de telecomunicaciones para la comunicación de máquina a máquina.

ANTECEDENTES DE LA INVENCIÓN

En las redes de transmisión de datos existentes, terminales y nodos particulares (p.ej., un HLR/AuC o HSS/AuC) de una red cooperan con el fin de efectuar la autenticación de los terminales en la red y para encriptar datos por intermedio de la parte de radio de la red. Una descripción detallada se da a conocer en la recomendación de GSM 03.20 para redes 2G, 3GPP TS 33.102 para redes 3G y 3GPP TS 33.401 para redes 4G.

En resumen, para redes GSM/GPRS, una clave secreta K_i constituye la parte esencial para los mecanismos de seguridad. La clave secreta K_i se memoriza en el terminal (normalmente en la tarjeta SIM) y en el HLR/AuC de la red. El HLR/AuC genera un número aleatorio RAND en respuesta a la demanda de autenticación procedente de un terminal que contiene un identificador de abonado IMSI para una sesión de terminal particular. El número aleatorio RAND y la clave secreta K_i se utilizan para derivar una clave de encriptación K_c que utiliza un algoritmo de generación de claves y para derivar una respuesta prevista XRES bajo un algoritmo de autenticación. La combinación (RAND, XRES, K_c) forma un vector de autenticación de GSM (triplete) transmitido desde el HLR/AuC a un MSC o SGSN. El MSC/SGSN transmite luego el número aleatorio RAND al terminal y la clave de encriptación K_c a una estación base o SGSN en caso de GPRS. El terminal y la red se comunican de forma inalámbrica por intermedio de una ruta de radio entre la estación base y el terminal.

A la recepción del número aleatorio RAND, el terminal deriva la clave de encriptación K_c utilizando el algoritmo de generación de claves, el número aleatorio RAND y la clave secreta K_i y también deriva una respuesta RES utilizando el algoritmo de autenticación, el número aleatorio RAND y la clave secreta K_i.

Para la autenticación, el terminal envía la respuesta RES por intermedio de la ruta de radio al MSC/SGSN en donde la respuesta RES derivada del terminal se compara con la respuesta prevista generada por la red XRES memorizada en el MSC/SGSN. Cuando la respuesta RES derivada del terminal coincide con la respuesta XRES generada por la red, el terminal es objeto de autenticación en la red para la sesión del terminal particular.

Después de la autenticación, la clave de encriptación K_c puede utilizarse para encriptar datos transmitidos por intermedio de la ruta de radio entre el terminal y la estación base que había memorizado la clave de encriptación K_c generada por la red. La encriptación de los datos en la ruta de radio se realiza utilizando la clave de encriptación K_c en combinación con un algoritmo de encriptación.

Cuando se termina la sesión del terminal, el terminal debe, en condiciones normales, seguir de nuevo el procedimiento de autenticación para una sesión de terminal posterior.

Para las redes UMTS, se recibe de nuevo una demanda de autenticación en el HLR/AuC que contiene el indicador de abonado IMSI. En lugar de un vector de autenticación de triplete, se genera un vector de autenticación de quinteto que contiene de nuevo un número aleatorio RAND y la respuesta prevista XRES junto con una clave de cifrado CK, una clave de integridad IK y una ficha de autenticación AUTN. AUTN se genera en una manera conocida como tal. El vector de autenticación de quinteto se envía a un nodo de red adicional, tal como VLR/SGSN. Tanto el número aleatorio RAND como la ficha de autenticación AUTN se transmiten por intermedio de la interfaz de radio al terminal. En el terminal, se verifica AUTN para autenticación de la red en una manera conocida y se establece una respuesta RES y se reenvía a la red para la autenticación del terminal en la red. Claves CK e IK pueden derivarse también en el terminal utilizando la clave secreta K_i y el número aleatorio RAND recibido.

Cuando se termina la sesión del terminal, el terminal debe seguir normalmente de nuevo el procedimiento de autenticación para una sesión de terminal posterior.

Para los Sistemas de Paquetes Evolucionados 4G (EPS), el procedimiento de autenticación es similar al de las redes UMTS, aunque se utiliza una nueva jerarquía de claves. La clave secreta K_i memorizada en la tarjeta USIM en el lado del terminal y la AuC en el lado de la red se utiliza para derivar las claves CK e IK. Las claves CK e IK, en combinación con un identificador ID de red de servicio se utilizan para derivar una nueva clave, $KASME_.$ A partir de esta nueva clave, $KASME_,$ otras claves de encriptación y de integridad para protección de la señalización entre el terminal y la red base (clave KNASenc), una protección de integridad entre el terminal y la red base (clave KNASint), la señalización de RRC y la transmisión de datos del usuario por intermedio de la interfaz de radio, incluyendo esta última la clave de encriptación K_{UPenc}.

Los procedimientos de encriptación y autenticación, generalmente conocidos como Acuerdo de Autenticación y Claves (AKA) integran un intercambio de mensajes considerable. Este intercambio de mensajes puede constituir una carga en casos particulares, p.ej., para las comunicaciones máquina a máquina (M2M) que se normalizan actualmente en 3GPP (véase p.ej., TS 22.368). Las aplicaciones de M2M suelen implicar a centenares, miles o millones de módulos de comunicaciones. Algunas aplicaciones solamente requieren, en casos raros, el acceso a una red de telecomunicaciones. Una realización, a modo de ejemplo, implica la recogida de información por un servidor desde, p.ej., medidores de electricidad inteligentes en las viviendas de una base de clientes amplia. Otras realizaciones, a modo de ejemplo, incluyen sensores, medidores, máquinas dispensadoras de café, etc., que pueden estar previstas de módulos de comunicación que permiten informar del estado operativo a un centro de procesamiento de datos por intermedio de la red de telecomunicaciones. Dichos dispositivos pueden supervisarse también desde un servidor. El centro de procesamiento de datos puede memorizar, a modo de ejemplo, los datos y/o proporcionar una relación para los encargados del mantenimiento con el fin de reparar una máquina, medidor, sensor, etc.

El documento titulado “Reducción de los retrasos de reautenticación durante las transferencias verticales UMTS/WLAN” por Ali Al Shidhani et al, IEEE 19º Simposio Internacional sobre Radiocomunicaciones Personales, en Interiores y Móviles 2008, da a conocer un método para realizar una reautenticación rápida en transferencias verticales y describe un método en el que un protocolo de UMTS-AKA modificado se realiza inicialmente seguido por una secuencia de protocolos FUAR recientemente descritos.

El documento US 2010/0017603 describe un método de generación de una identidad de pseudónimo temporal para un abonado que aumenta la flexibilidad en la autenticación al mismo tiempo que proporciona las ventajas de una reautenticación rápida.

El documento US 2007/0178885 describe un método de autenticación para permitir a un abonado acceder a una red de telecomunicaciones por intermedio de una red WiFi actuando como portal.

SUMARIO DE LA INVENCIÓN

Es un objetivo de la invención dar a conocer un sistema de autenticación y/o acuerdo de claves (AKA) más eficientes para los terminales en una red de telecomunicación.

La invención se define en las reivindicaciones independientes 1, 9, 16 y 20.

Un método para habilitar la autenticación y/o acuerdo de claves para un terminal en una red se da a conocer en esta invención. El método implica la transmisión de al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) desde una red a un dispositivo de destino, tal como un terminal, durante una sesión *n* del terminal. El parámetro de AKA permite un procedimiento de autenticación y/o acuerdo de claves del terminal en la red para una posterior sesión del terminal n+m.

El dispositivo de destino puede ser también otro nodo de red u otra entidad receptora.

Un programa informático o conjunto de programas en cooperación que comprenden partes de código de software configuradas para, cuando se ejecuta por un procesador, realizar las etapas del método se da a conocer también en la presente invención.

Además, una red o un nodo de red que está configurado para la autenticación y/o acuerdo de claves (AKA) para un terminal en la red se dan a conocer en esta invención. La red o nodo de red comprende una interfaz de recepción configurada para recibir un identificador (IMSI) del terminal durante una sesión *n* del terminal. La red contiene también un generador configurado para generar al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) que permite la autenticación y/o acuerdo de claves para el terminal identificado en la red o nodo de red para una sesión de terminal posterior n+m. La red o el nodo de red tiene una interfaz de transmisión configurada para transmitir el al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) destinado para el terminal.

Además, una señal de vector de AKA para una red se da a conocer en esta invención. La señal de vector de AKA contiene al menos un parámetro para una sesión de terminal *n* y al menos un parámetro para una sesión de terminal posterior n+m del mismo terminal en la red. Para redes 2G, este vector de AKA puede comprender [$RAND_{n+m}$, $XRES_n$, Kc_n]; para redes 3G [$RAND_{n+m}$, $AUTN_{n+m}$, $XRES_n$, IK_n, CK_n] y para redes 4G [$RAND_{n+m}$, $AUTN_{n+m}$, $XRES_n$, $KASME_n$].

Además, se da a conocer un método para permitir la autenticación y/o acuerdo de claves (AKA) para un terminal y una red. El terminal recibe durante una sesión de terminal *n* al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$). Con el fin de establecer una sesión de terminal posterior n+m, el terminal utiliza el parámetro de AKA recibido durante la sesión del terminal anterior *n* para la autenticación y/o acuerdo de claves del terminal con la red.

Un programa informático o conjunto de programas en cooperación comprende partes de código de software

configuradas para, cuando se ejecuta por un procesador, realizar las etapas de este método que se dan también a conocer en esta descripción.

De forma adicional, un terminal configurado para la autenticación y/o acuerdo de claves (AKA) en una red se da a conocer en la presente invención. El terminal comprende una interfaz de recepción configurada para recibir, durante una sesión de terminal *n*, al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) para una sesión de terminal posterior n+m procedente de la red. El terminal contiene un procesador configurado para derivar un mensaje de autenticación (RES_{n+m}) y/o una clave que utiliza el al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) recibido durante la sesión del terminal *n*. El terminal tiene una interfaz de transmisión configurada para transmitir, durante la SIP/IP de terminal posterior n+m, el mensaje de autenticación derivado (RES_{n+m}) y/o los datos encriptados bajo la clave derivada a la red para la autenticación y/o acuerdo de claves para el terminal en la red.

Por último, un sistema que comprende al menos un terminal y un nodo de red de una red de telecomunicación se dan a conocer en la presente invención. El nodo de red comprende una interfaz de recepción, un generador y una interfaz de transmisión. La interfaz de recepción está configurada para recibir un identificador (IMSI) del terminal durante una sesión *n* del terminal. El generador está configurado para generar al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) que permite la autenticación y/o acuerdo de claves (AKA) para el terminal identificado en la red o nodo de red para una sesión de terminal n+m posterior. La interfaz de transmisión está configurada para transmitir el al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) destinado para el terminal.

El sistema comprende también un terminal con una interfaz de recepción, un procesador y una interfaz de transmisión. La interfaz de recepción está configurada para recibir, durante la sesión de terminal *n*, el al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) para la sesión del terminal posterior n+m (p.ej., m = 1) desde la red. El procesador está configurado para derivar un mensaje de autenticación (RES_{n+m}) y/o una clave utilizando el al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) recibido durante la sesión de terminal *n*. La interfaz de transmisión está configurada para transmitir, durante la sesión de terminal posterior n+m, el mensaje de autenticación derivado (RES_{n+m}) y/o datos bajo la clave derivada hacia la red para la autenticación y/o acuerdo de claves para el terminal en la red para la sesión de terminal posterior n+m.

En la presente invención, se define una sesión como un intercambio de información interactiva entre el terminal y la red que se establece en un determinado momento y se abandona en un momento posterior. Los parámetros de AKA son parámetros utilizados para al menos una de entre la autenticación del terminal en la red y el acuerdo de claves entre el terminal y la red. Estos parámetros se utilizan para derivar respuestas de autenticación y/o claves en el terminal.

Utilizando los parámetros de AKA, obtenidos en una sesión de terminal anterior *n* por el terminal, en una sesión de terminal n+m posterior, puede omitirse una demanda por separado de estos parámetros de AKA para fines de autenticación y/o acuerdo de claves para la sesión n+m, con lo que se mejora la eficiencia de AKA. El AKA desplazado en el tiempo da lugar a que un terminal cuando se desea su conexión a la red, tenga acceso inmediato a los parámetros de AKA o a mensajes de autenticación memorizados y/o claves derivadas de estos parámetros de AKA y puede enviar de inmediato el mensaje de autenticación a la red. Los parámetros de AKA pueden incluirse en un mensaje (señalización) desde la red para terminar la sesión de terminal anterior *n* y el mensaje de autenticación puede incluirse en un mensaje (señalización) desde el terminal para iniciar la sesión del terminal n+m posterior.

Debe apreciarse que, en general, cualquier etapa durante la sesión de terminal *n* puede utilizarse para proporcionar al terminal los parámetros de AKA aplicables para los fines de autenticación y/o acuerdo de claves para una sesión de terminal n+m posterior.

En la presente invención, los mensajes de autenticación RES suelen ser mensajes de respuesta de autenticación, que dan respuesta a una demanda exigida (RAND). Estos mensajes suelen comprender o consistir en un código.

Una forma de realización, a modo de ejemplo, implica la recepción de una primera demanda de autenticación desde el terminal que contiene un primer mensaje de autenticación (RES_n) derivado en el terminal utilizando la clave secreta K_i y al menos un primer parámetro de autenticación ($RAND_n$) para la primera sesión del terminal *n* y la transferencia de al menos un segundo parámetro de autenticación ($RAND_{n+m}$) al terminal durante la primera sesión de terminal *n*. El al menos un segundo parámetro de autenticación ($RAND_{n+m}$) permite al terminal derivar un segundo mensaje de autenticación (RES_{n+m}) y, de forma opcional, memorizar el segundo parámetro de autenticación. Cuando el terminal establece una sesión de terminal n+m, posterior en el tiempo a la primera sesión de terminal *n*, la red decide una segunda demanda de autenticación desde el terminal para esta sesión de terminal posterior. La segunda demanda de autenticación contiene entonces el segundo mensaje de autenticación (RES_{n+m}) y la red está configurada para realizar la autenticación del terminal para la sesión del terminal posterior sin necesitar primero suministrar el segundo parámetro de autenticación ($RAND_{n+m}$).

Una forma de realización de la invención implica la recepción de una demanda de incorporación desde el terminal en la red para la sesión de terminal posterior n+m, en donde la demanda de incorporación contiene un mensaje de solicitud (UD) destinado a un servidor de aplicación en, o conectado a, la red y un mensaje de autenticación

(RES_{n+m}) derivado en el terminal utilizando el al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) recibido durante la sesión de terminal *n*. La forma de realización implica, asimismo, en el lado del terminal, la etapa de transmitir una demanda de incorporación a la red para la sesión de terminal n+m posterior, en donde la demanda de incorporación contiene un mensaje de solicitud (UD) destinado para un servidor de aplicación en, o conectado a, la red y un mensaje de autenticación (RES_{n+m}), derivado en el terminal utilizando el al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) recibido durante la sesión del terminal *n*.

Estas formas de realización son especialmente ventajosas para aplicaciones de M2M, en donde los datos de aplicaciones y el mensaje de autenticación están ambos contenidos en la demanda de incorporación. La demanda de incorporación permite la autenticación del terminal en la red en un nodo particular y la transmisión de los datos de aplicación sin requerir el establecimiento de una conexión, tal como un contexto de PDP. La demanda de incorporación puede desde el terminal puede rechazarse por la red mientras que se sigue permitiendo que los datos de los usuarios se transmitan desde el terminal a la red en la demanda de incorporación, con lo que se economizan recursos del terminal y de la red.

Aunque sea de forma convencional, la encriptación de datos solamente se proporciona después de la autenticación de un terminal, una forma de realización de la presente invención implica la etapa de recepción de los datos de aplicación (UD) en la red en forma encriptada durante la sesión de terminal n+m posterior, en donde la forma encriptada se obtiene en el terminal mediante la encriptación del mensaje de solicitud utilizando al menos una calve (Kc_{n+m}; $CK_{n+m,}$ $KNASenc_{n+m}$) que se deriva utilizando al menos el parámetro de AKA ($RAND_{n+m}$) recibido durante la sesión de terminal *n*. Asimismo, en el lado del terminal, la forma de realización implica la etapa de encriptar el mensaje de solicitud transmitido con la demanda de incorporación de la sesión de terminal posterior n+m utilizando al menos una clave (Kc_{n+m}; CK_{n+m}; $KNASenc_{n+m}$) derivada utilizando al menos un parámetro de autenticación ($RAND_{n+m}$) recibido durante la sesión del terminal *n*.

Estas formas de realización permiten la encriptación de datos de usuarios (el mensaje de solicitud) antes de la autenticación del terminal con la red, con lo que se mejora la seguridad de la transmisión de datos. El mensaje de solicitud puede ser desencriptado en un nodo en la red que tenga acceso al algoritmo de encriptación y las una o más claves de encriptación. Los datos de solicitud pueden desencriptarse también en el servidor de aplicación.

En una forma de realización de la invención, el método en el lado de la red implica, además, la etapa de recepción de una demanda de incorporación desde el terminal en la red para la sesión de terminal posterior n+m, en donde la extrema de incorporación contiene un código de autenticación de mensaje (MAC) para la protección de la integridad de al menos una parte del mensaje de demanda de incorporación, obteniéndose el código MAC en el terminal utilizando un algoritmo de MAC criptográfico y al menos una clave (Kc_{n+m}; IK_{n+m}; $KNASint_{n+m}$) derivada utilizando al menos el al menos un parámetro de AKA ($RAND_{n+m}$) recibido durante la sesión del terminal *n*. Asimismo, el método en el lado del terminal implica la etapa de generar un código de autenticación de mensajes (MAC) para protección de la integridad de al menos una parte de un al menos un mensaje de demanda para la sesión de terminal n+m utilizando al menos una clave (Kc_{n+m}; IK_{n+m}; $KNASint_{n+m}$) derivada utilizando al menos el al menos un parámetro de AKA ($RAND_{n+m}$) recibido durante la sesión de terminal *n* y transmitiendo el código de autenticación de mensaje en la red en la demanda de incorporación.

Estas formas de realización permiten la protección de la integridad del mensaje de demanda de incorporación completo o solamente de los datos de los usuarios (el mensaje de aplicación) para una sesión de terminal n+m. Después de haber recibido los parámetros de AKA durante la sesión de terminal n, puede derivarse una clave para generar un Código de Autenticación de Mensaje (MAC) a transmitirse durante la sesión de terminal n+m sin tener primero que realizar un procedimiento de AKA para la sesión de terminal n+m. La protección de la integridad se suele aplicar para verificar la corrección del mensaje y de la fuente de origen del mensaje. La verificación del Código de Autenticación de Mensaje puede realizarse en la red o en el servidor de aplicación, dependiendo de la disponibilidad de las claves de encriptación y de los algoritmos de MAC aplicados.

En una forma de realización de la invención, el método en el lado de la red implica la etapa de transmitir, durante la sesión de terminal *n*, el al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTH_{n+m}$) desde la red al terminal en forma encriptada. Asimismo, el método en el lado del terminal implica las etapas de:

- recibir, durante la sesión de terminal *n*, el al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTH_{n+m}$) desde la red al terminal en forma encriptada; y

- desencriptar el al menos un parámetro de AKA encriptado ($RAND_{n+m}$; $RAND_{n+m}$, $AUTH_{n+m}$) para derivar un mensaje de autenticación (RES_{n+m}).

Puesto que el intervalo temporal entre la sesión de terminal *n* y la sesión de terminal posterior n+m puede ser considerable, la intercepción de los parámetros de AKA y el uso posterior de estos parámetros para derivar mensajes de autenticación y/o claves puede realizarse a este respecto. Aunque el uso de la autenticación adecuada y de los algoritmos de generación de claves pueden retrasar la derivación de los mensajes de autenticación y/o claves por partes no autorizadas, la encriptación de los parámetros de AKA, en conformidad con esta forma de

realización, puede resultar ventajosa para impedir el denominado sniffing que efectúa una captura de paquetes de datos. El nodo de red configurado para la encriptación de los parámetros de AKA para la sesión de terminal posterior tiene acceso a la clave de encriptación para la sesión de terminal actual y al algoritmo de encriptación.
En una forma de realización de la invención, el nodo de red está configurado, además, para transmitir al menos uno de un mensaje de autenticación prevista ($XRES_n$), al menos una clave de encriptación/desencriptación (Kc_n; IK_n, CK_n; $KASME_n$) para un nodo de red adicional para la sesión de terminal *n* en combinación con al menos un parámetro de AKA ($RAND_{n+m}$; $RAND_{n+m}$, $AUTN_{n+m}$) para la sesión de terminal posterior n+m. La forma de realización permite a la red realizar la autenticación del terminal en la red para la sesión de terminal *n* y para proporcionar los parámetros de AKA al terminal para la sesión de terminal posterior n+m.

En adelante, las formas de realización de la invención se describirán con más detalle. Debe apreciarse, sin embargo, que esta forma de realización no puede interpretarse como limitadora del alcance de protección de la presente invención.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

En los dibujos:

La Figura 1 es una ilustración esquemática de una red de telecomunicación que conecta terminales a un servidor de aplicación;

Las Figuras 2A y 2B son ilustraciones esquemáticas de un terminal 3 y un HLR/AuC de una red 2G en conformidad con una forma de realización de la invención;

Las Figuras 3A-3D proporcionan ilustraciones esquemáticas de procedimientos de AKA para una red de telecomunicación 2G en conformidad con formas de realización de la invención;

Las Figuras 4A a 4D proporcionan ilustraciones esquemáticas de procedimientos de AKA para una red de telecomunicación 3G en conformidad con las formas de realización de la invención;

La Figura 5 da a conocer una ilustración esquemática de un procedimiento de AKA para una red de telecomunicación 4G en conformidad con una forma de realización de la invención;

La Figura 6 es un diagrama de estados para un terminal y un nodo de red en conformidad con una forma de realización de la invención; y

La Figura 7 proporciona una ilustración esquemática de otra forma de realización en conformidad con la invención para una red 2G.

DESCRIPCIÓN DETALLADA DE LOS DIBUJOS

La Figura 1 muestra una ilustración esquemática de una red de telecomunicación 1. La red de telecomunicación 1 permite las sesiones de datos entre el servidor de aplicación 2 y un terminal 3 por intermedio de una red de datos 4, en donde el acceso del terminal 3 a la red de telecomunicación 1 es de tipo inalámbrico.

En la red de telecomunicaciones ilustrada en la Figura 1, tres generaciones de redes de telecomunicaciones se ilustran esquemáticamente juntas para fines de mayor brevedad. Una descripción más detallada de la arquitectura y una visión general pueden encontrarse en 3GPP TS 23.002 que está incluida en la presente solicitud de patente por referencia en su integridad.

La bifurcación inferior ilustrada en la Figura 1 representa una red de telecomunicaciones GPRS o UMTS que comprende un nodo de soporte de GPRS de pasarela (GGSN), un nodo de soporte de GPRS de servicio (SGSN) y una red de acceso a radio (GERAN o UTRAN). Para una red de acceso de radio de GSM/EDGE (GERAN), la red RAN comprende un controlador de estación base (BSC) conectado a una pluralidad de transceptores de estaciones base (BTSs), ambos no ilustrados. Para una red de acceso de radio de UMTS (UTRAN), la red RAN comprende un controlador de red de radio (RNC) conectado a una pluralidad de nodos eNodeBs, tampoco ilustrados. Los nodos GGSN y SGSN están convencionalmente conectados a un denominado Registro de Localización Base (HLR) que contiene información de suscripción de los terminales 3. En las Figuras, el registro HLR está combinado con un centro de autenticación (AuC) para terminales de autenticación 3 en la red.

La bifurcación superior en la Figura 1 representa una red de telecomunicaciones de la siguiente generación, normalmente indicada como de Evolución a Largo Plazo (LTE) o Sistema de Paquetes Evolucionado (EPS). Dicha red comprende una pasarela PDN (P-GW) y una pasarela de servicio (S-GW). La red E-UTRAN del EPS comprende nodos NodeBs (eNodeBs o eNBs) evolucionados que proporcionan un acceso inalámbrico para un terminal 3 que está conectado a la S-GW por intermedio de una red de paquetes. La S-GW está conectada a un servidor de abonado base HSS y una entidad de gestión de la movilidad MME para fines de señalización. El servidor HSS

incluye un depósito de perfiles de suscripción y un centro de autenticación (AuC).

Información adicional de la arquitectura general de una red EPS puede encontrarse en 3GPP TS 23.401.
En un entorno de M2M, un servidor único 2 se utiliza normalmente para la comunicación con un gran número de terminales 3. Los terminales individuales 3 pueden identificarse mediante identificadores individuales, tales como una dirección IP, una IMSI u otro identificador de terminal.

Formas de realización de la presente invención se describirán a condición con más detalle para redes de acceso inalámbricas 2G, 3G y 4G. En estas formas de realización, se considerará la sucesión de sesiones de terminales n-1, *n*, n+1. La presente invención, sin embargo, es aplicable igualmente para sesiones de terminales n-m, n, n+m para sesiones de terminales n-k, n, n+m o secuencias más avanzadas de sesiones de terminales en tanto que al menos un parámetro de AKA recibido durante una sesión de terminal anterior puede utilizarse para futuras sesiones de terminales.

Las Figuras 2A y 2B son ilustraciones esquemáticas de un terminal 3 y un HLR/AuC de una red 2G en conformidad con una forma de realización de la invención.

El HLR/AuC comprende una interfaz de recepción 20 y una interfaz de transmisión 21. La interfaz de recepción 20 está configurada para recibir una demanda de autenticación desde un terminal 3 cuando se establece una sesión de terminal *n*. La demanda de autenticación contiene al menos el identificador de abonado, el identificador IMSI (Identidad de Abonado Móvil Internacional) memorizada en la tarjeta SIM. El subíndice *n* para IMSI en la Figura 2B es indicativo de la sesión de terminal ilustrada pero, en general, la IMSI tendrá lo mismo que para una sesión de terminal anterior n-1 y una sesión de terminal posterior n+1.

El HLR/AuC comprende una clave secreta K_i y un número aleatorio $RAND_n$ para el terminal 3, siendo este último normalmente distinto para cada sesión de terminal *n*. La clave secreta K_i y el número aleatorio $RAND_n$ se utilizan en combinación con el algoritmo de autenticación A_3 y el algoritmo de generación de claves A_8 para derivar un mensaje de autenticación prevista $XRES_n$ y la clave de encriptación Kc_n utilizando el procesador 22 en una manera conocida por sí misma. Además, sin embargo, la demanda de autenticación da lugar también a la generación de un número aleatorio $RAND_{n+1}$ por el generador 23. $RAND_{n+1}$ puede utilizarse también para derivar un mensaje de respuesta de autenticación prevista $XRES_{n+1}$ y la clave de encriptación Kc_{n+1} por anticipado, esto es, antes de que se reciba la demanda de una sesión de terminal posterior n+1. $XRES_{n+1}$ y la clave de encriptación Kc_{n+1} pueden memorizarse luego en una memoria (no ilustrada). El HLR/AuC está configurado para transmitir el triplete de parámetros de AKA [$RAND_{n+1}$, $XRES_n$, Kc_n] por intermedio de la interfaz de transmisión 21 a un nodo de red adicional, p.ej., nodo SGSN ilustrado en la Figura 1.

Conviene señalar que no todos los componentes del triplete están destinados para el terminal 3. En el nodo SGSN (véase Figura 1), los componentes del triplete recibidos desde el HLR/AuC son objeto de proceso. $XRES_n$ se utiliza para la autenticación del terminal 3 en la red para la sesión de terminal *n*, mientras la clave de encriptación Kc_n puede utilizarse para desencriptar los datos de usuario UD recibidos en el nodo SGSN durante la sesión de terminal *n*. La clave de encriptación Kc_n puede, sin embargo, utilizarse también para la encriptación de $RAND_{n+1}$, después de lo cual puede reenviarse el número $RAND_{n+1}$ encriptado al terminal 3 por intermedio de la red de acceso de radio RAN. La encriptación y la desencriptación pueden realizarse durante el algoritmo de encriptación A_5 en combinación con la clave de encriptación Kc_n.

El terminal 3 comprende una interfaz de recepción 30 y una interfaz de transmisión 31. En alguna etapa durante la sesión de terminal *n*, la interfaz de recepción 30 recibe el parámetro $RAND_{n+1}$ de AKA posiblemente encriptado utilizando el algoritmo de encriptación A_5 y la clave de encriptación Kc_n. El algoritmo de encriptación A_5 es conocido y la clave de encriptación Kc_n se deriva en el terminal 3, lo que permite al terminal 3 desencriptar el parámetro $RAND_{n+1}$ de AKA.

El parámetro $RAND_{n+1}$ de AKA permite al terminal 3, utilizando el procesador 32, derivar un mensaje de autenticación RES_{n+1} y una clave de encriptación Kc_{n+1} para una sesión de terminal posterior n+1, utilizando el algoritmo de autenticación A_3 y el algoritmo de generación de claves A_8 en un tiempo arbitrario después de haber terminado la sesión de terminal *n* y sin tener primero que demandar $RAND_{n+1}$ desde la red 1 para la sesión de terminal posterior n+1. El mensaje de autenticación RES_{n+1} y una clave de encriptación Kc_{n+1} pueden memorizarse temporalmente en la memoria 33 en el terminal 3. Los datos de usuario UD, a transmitirse durante la sesión de terminal posterior n+1 pueden encriptarse utilizando la clave Kc_{n+1} y el algoritmo de encriptación A_5. Cuando se inicia la sesión de terminal posterior n+1, la interfaz de transmisión 31 puede utilizarse para transmitir el identificador IMSI (que tiene la suscripción n+1 en la Figura 2A para indicar la sesión de terminal posterior; en general $IMSI_{n+1}$ es igual a $IMSI_n$), el mensaje de autenticación RES_{n+1} y, de forma opcional, los datos de usuario UD encriptados destinados para el servidor de aplicación 2.

Conviene señalar que formas de realización similares pueden considerarse por un experto en terminales de 3G/4G y nodos de red 3G/4G sobre la base de las Figuras 2A y 2B y la explicación anterior.

Aunque en la presente descripción de las formas de realización, el procedimiento implica la autenticación y el acuerdo de claves, debe entenderse que la invención es también aplicable para otra autenticación o acuerdo de claves a nivel individual.

Las Figuras 3A a 3D proporcionan ilustraciones esquemáticas de procedimientos de autenticación y acuerdo de claves (AKA) para una red de telecomunicaciones 2G 1 en conformidad con las formas de realización de la invención.

La Figura 3A es una ilustración esquemática de un procedimiento de AKA en donde los datos de usuario UD se transmiten en mensajes de señalización desde un terminal UE 3 a una red 1.

En la etapa 1a, el terminal UE 3 transmite una demanda de incorporación que contiene al menos uno o la totalidad de los identificadores de terminales IMSI, UD de mensaje de solicitud o un mensaje de autenticación RES_n utilizando, a modo de ejemplo, la interfaz de transmisión 31, con el fin de demandar una sesión de terminal *n*. El mensaje de autenticación RES_n puede ser un mensaje de 32 bits. RES_n se obtiene, a modo de ejemplo, mediante una ejecución posterior de la forma de realización de la invención, según se explicará más adelante haciendo referencia a la Figura 6. La demanda de incorporación puede recibirse de forma inalámbrica en la red RAN de la Figura 1 reenviarse al MSC/SGSN en la etapa 1b.

En la etapa 2a, el MSC/SGSN emite una demanda de autenticación al HLR, conteniendo dicha demanda de autenticación el identificador IMSI del equipo UE 3. La demanda de autenticación se recibe por intermedio de la interfaz de recepción 20 en el HLR. El HLR recupera el mensaje de respuesta de autenticación $XRES_n$ prevista y la clave de encriptación Kc_n y además, genera un parámetro de AKA $RAND_{n+1}$ para fines de AKA para una sesión de terminal posterior n+1, utilizando el generador 23, mediante el mismo terminal UE 3. $RAND_{n+1}$ puede ser un mensaje de 128 bits. El HLR puede calcular ya los valores de $XRES_{n+1}$ y de Kc_{n+1} para la sesión de terminal posterior n+1 y memorizar estos parámetros. En la etapa 2b, el HLR informa el triplete [$RAND_{n+1}$, $XRES_n$, Kc_n] al MSC/SGSN. En el MSC/SGSN, la autenticación del terminal 3 en la red 1 para la sesión de terminal *n* puede procesarse comparando RES_n, recibida en la etapa 1b, con $XRES_n$ del triplete recibida en la etapa 2b. Si la autenticación tiene un resultado satisfactorio, el terminal UE 3 y la red pueden conmutarse a un modo de seguridad (etapas 2c, 2d), en donde se conviene en que toda comunicación adicional se realice bajo la clave de encriptación Kc_n.

Los datos de usuario UD, recibidos en la etapa 1b, pueden reenviarse luego al servidor M2M 2. En la forma de realización ilustrada en la Figura 3A, esta operación se realiza utilizando mensajes SMS por intermedio de las etapas 3a, 3b, pero se pueden aplicar otros métodos de reenvío de los datos de usuario desde el MSC/SGSN al servidor de aplicación 2. En la presente forma de realización, de nuevo de forma opcional, una confirmación de recibo de un mensaje de entrega de los datos de usuarios en el servidor de aplicación 2 se recibe en la etapa 3c en el MSC/SGSN.

Puesto que los datos de usuario están incluidos ya en el mensaje de señalización, esto es, la demanda de incorporación de IMSI en la presente forma de realización, no es necesario establecer una conexión de datos completa entre el terminal UE 3 y la red 1. Por lo tanto, en las etapas 4a y 4b, un mensaje de rechazo de incorporación de IMSI se reenvía al terminal UE 3 desde la red 1 para evitar el establecimiento de una conexión completa y, en consecuencia, para economizar recursos de red. El mensaje de rechazo de incorporación de IMSI contiene, sin embargo, el parámetro $RAND_{n+1}$ de AKA que se recibe por el terminal UE 3 por intermedio de la interfaz de recepción 30 como la etapa final de la sesión de terminal *n*.

Según se explica haciendo referencia a la Figura 2A, el parámetro de AKA $RAND_{n+1}$ puede utilizarse para derivar un mensaje de autenticación RES_{n+1} y/o una clave de encriptación Kc_{n+1} que puede memorizarse en la memoria 33 para una sesión de terminal posterior n+1.

Las etapas 5a, 5b y 6 ilustran el uso de RES_{n+1} para una sesión de terminal posterior n+1 para demandar de inmediato la autenticación en la red para esta sesión.

La Figura 3B es una ilustración esquemática de un procedimiento de AKA en donde datos de usuario UD se transmiten en mensajes de señalización desde un terminal UE 3 a una red 1 en una forma encriptada.

En la etapa 1a, el terminal UE 3 transmite una demanda de incorporación que contiene el identificador de abonado IMSI, el mensaje de solicitud de UD y un mensaje de autenticación RES_n, que utiliza la interfaz de transmisión 31, con el fin de demandar una sesión de terminal *n*. El mensaje de autenticación RES_n puede ser un mensaje de 32 bits. Los datos de usuario UD se encriptan ahora utilizando la clave de encriptación Kc_n y el algoritmo de encriptación A_5 según se describe haciendo referencia a la Figura 2A. La demanda de incorporación se recibe, de forma inalámbrica, en la red RAN según se ilustra en la Figura 1 y se reenvía al MSC/SGSN en la etapa 1b.

En la etapa 2a, el MSC/SGSN emite una demanda de autenticación al HLR, conteniendo dicha demanda de autenticación el identificador IMSI del terminal UE 3. La demanda de autenticación se recibe por intermedio de la interfaz de recepción 20 en el HLR. El HLR recupera el mensaje de respuesta de autenticación $XRES_n$ prevista y la clave de encriptación Kc_n y además, genera un parámetro de AKA $RAND_{n+1}$ para fines de AKA para una sesión de

terminal posterior n+1, utilizando el generador 23, mediante el mismo terminal UE 3. $RAND_{n+1}$ puede ser un mensaje de 128 bits. El HLR puede calcular ya $XRES_{n+1}$ y Kc_{n+1} para la sesión de terminal posterior n+1 y memorizar estos parámetros. En la etapa 2b, el HLR informa del triplete [$RAND_{n+1}$, $XRES_n$, Kc_n] al MSC/SGSN.

En el MSC/SGSN, la autenticación del terminal 3 en la red 1 para la sesión de terminal *n* puede procesarse comprando RES_n que se recibe en la etapa 1b, con $XRES_n$ del triplete recibido en la etapa 2b. Si la autenticación tiene un resultado satisfactorio, el terminal UE 3 y la red pueden conmutarse a un modo de seguridad (etapas 2c, 2b), en donde se conviene en que toda comunicación adicional se realice bajo la clave de encriptación Kc_n.

Los datos de usuarios UD del mensaje de solicitud, recibidos en la etapa 1b, pueden reenviarse luego al servidor M2M 2. En la forma de realización ilustrada en la Figura 3A, esta operación se realiza utilizando mensajes SMS por intermedio de las etapas 3a, 3b, pero se pueden aplicar otros métodos de reenvío de los datos de usuario desde el MSC/SGSN al servidor de aplicación 2. En la presente forma de realización, de nuevo de forma opcional, un acuse de recibo del mensaje de entrega de los datos de usuarios en el servidor de aplicación 2 se recibe en la etapa 3c en el MSC/SGSN. Además, los datos de usuario UD del mensaje de solicitud se desencriptan utilizando la clave de encriptación Kc_n y el algoritmo de encriptación A_5 conocido en el MSC/SGSN. De forma alternativa, los datos de usuario UD del mensaje de solicitud se reenvían hacia el servidor de aplicación 2 en forma encriptada y desencriptada en un nodo de red adicional o el servidor de aplicación 2 que tenga acceso a la clave de encriptación Kc_n y al algoritmo de encriptación A_5.

De nuevo, puesto que los datos de usuarios UD del mensaje de solicitud están ya incluidos en el mensaje de señalización, esto es, la demanda de incorporación de IMSI en la presente forma de realización, no es necesario establecer una conexión de datos completa entre el terminal UE 3 y la red 1. Por lo tanto, en las etapas 4a y 4b, se reenvía un mensaje de rechazo de incorporación de IMSI al terminal UE 3 desde la red 1 para evitar el establecimiento de una conexión completa y, en consecuencia, economizar recursos de la red. El mensaje de rechazo de incorporación de IMSI contiene, sin embargo, el parámetro $RAND_{n+1}$ de AKA que se recibe por el terminal UE 3 por intermedio de la interfaz de recepción 30 en la etapa final de la sesión de terminal *n*.

Según se explica haciendo referencia a la Figura 2A, el parámetro $RAND_{n+1}$ de AKA puede utilizarse para derivar un mensaje de autenticación RES_{n+1} y/o una clave de encriptación Kc_{n+1} que puede memorizarse en la memoria 33 para una sesión de terminal posterior n+1.

Las etapas 5a, 5b y 6 ilustran el uso de RES_{n+1} para una sesión de terminal posterior n+1 para demandar, de inmediato, la autenticación en la red para esta sesión. Los datos de usuario UD del mensaje de solicitud a enviarse en esta sesión de terminal pueden encriptarse utilizando el algoritmo de encriptación A_5 y la clave de encriptación Kc_{n+1} siendo esta última derivada del parámetro $RAND_{n+1}$ de AKA recibido durante la sesión de terminal anterior *n*, K_i y el algoritmo de generación de claves A_8.

Puesto que el intervalo temporal entre la sesión de terminal *n* y la sesión de terminal posterior n+1 puede ser considerable, puede realizarse la intercepción del parámetro $RAND_{n+1}$ de AKA y el uso posterior de este parámetro para derivar el mensaje de autenticación RES_{n+1} y/o clave Kc_{n+1}. Aunque el uso de algoritmos adecuados de autenticación y generación de claves puede retardar la derivación del mensaje de autenticación y/o la clave por partes no autorizadas, la encriptación del parámetro de AKA $RAND_{n+1}$ puede ser ventajosa para impedir la captura denominada sniffing de paquete de datos. Dicha forma de realización se ilustra en la Figura 3C.

La Figura 3C es una ilustración esquemática de un procedimiento de AKA en donde los datos de usuarios UD se transmiten en mensajes de señalización desde un terminal UE 3 a una red 1 en forma encriptada y en donde el parámetro de AKA $RAND_{n+1}$ transmitido al terminal UE 3 durante la sesión de terminal *n* es también objeto de encriptación. Conviene señalar que aunque la Figura 3C ilustra la opción combinada, no es necesario encriptar los datos UD de mensaje de solicitud cuando se realiza la encriptación del parámetro de AKA $RAND_{n+1}$.

En la etapa 1a, el terminal UE 3 transmite de nuevo una demanda de incorporación que contiene el identificador de abonado IMSI, los datos UD del mensaje de solicitud y un mensaje de autenticación RES_n, que utiliza la interfaz de transmisión 31, con el fin de demandar una sesión de terminal *n*. El mensaje de autenticación RES_n puede ser un mensaje de 32 bits. Los datos de usuario UD pueden encriptarse utilizando la clave de encriptación Kc_n y el algoritmo de encriptación A_5 según se describe haciendo referencia a la Figura 2A. La demanda de incorporación se recibe, de forma inalámbrica, en la red RAN ilustrada en la Figura 1 y se reenvía al MSC/SGSN en la etapa 1b.

En la etapa 2a, el MSC/SGSN emite una demanda de autenticación al HLR, conteniendo dicha demanda de autenticación el IMSI de terminal UE 3. La demanda de autenticación se recibe por intermedio de la interfaz de recepción 20 en el HLR. El HLR recupera el mensaje de respuesta de autenticación prevista $XRES_n$ y la clave de encriptación Kc_n y genera, además, un parámetro de AKA $RAND_{n+1}$ para fines de AKA para una sesión de terminal posterior n+1, utilizando el generador 23 por el mismo terminal UE 3. $RAND_{n+1}$ puede ser un mensaje de 128 bits. El HLR puede calcular ya $XRES_{n+1}$ y Kc_{n+1} para la sesión de terminal posterior n+1 y memorizar estos parámetros. En la etapa 2b, el HLR informa del triplete [$RAND_{n+1}$, $XRES_n$, Kc_n] al MSC/SGSN.

En el MSC/SGSN, la autenticación del terminal 3 en la red 1 para sesión de terminal *n* puede procesarse comparando RES_n que se recibe en la etapa 1b, con $XRES_n$ del triplete que se recibe en la etapa 2b.

Los datos UD del mensaje de solicitud, recibido en la etapa 1b pueden reenviarse luego al servidor M2M 2. En la forma de realización ilustrada en la Figura 3C, esta operación se realiza utiliza mensajes SMS por intermedio de las etapas 3a, 3b pero se pueden aplicar otros métodos de reenvío de los datos de usuario desde el MSC/SGSN al servidor de aplicación 2. En la presente forma de realización, de nuevo de forma opcional, una confirmación de recibo del mensaje de entrega de los datos de usuarios en el servidor de aplicación 2 se recibe en la etapa 3c en el MSC/SGSN. Además, cuando los datos de usuario UD del mensaje de aplicación son objeto de encriptación, los datos UD del mensaje de aplicación pueden desencriptarse utilizando la clave de encriptación Kc_n y el algoritmo de encriptación A_5 conocidos en el MSC/SGSN. Como alternativa, los datos de usuario UD del mensaje de solicitud se reenvían hacia el servidor de aplicación 2 en una forma encriptada y desencriptada en un nodo de red adicional o el servidor de aplicación 2 que tiene acceso a la clave de encriptación Kc_n y al algoritmo de encriptación A_5.

De nuevo, puesto que los datos UD del mensaje de solicitud están ya incluidos en el mensaje de señalización, esto es, la demanda de incorporación de IMSI en la presente forma de realización, no es necesario establecer una conexión de datos completa entre el terminal UE 3 y la red 1. Por lo tanto, en las etapas 4a y 4b, un mensaje de rechazo de incorporación de IMSI se reenvía al terminal UE 3 desde la red 1 para evitar el establecimiento de una conexión completa y, en consecuencia, economizar recursos de red. El mensaje de rechazo de incorporación de IMSI contiene, sin embargo, el parámetro de AKA $RAND_{n+1}$ que se recibe por el terminal UE 3 por intermedio de la interfaz de recepción 30 en la etapa final de la sesión de terminal *n*. En la forma de realización ilustrada en la Figura 3C, el parámetro de AKA $RAND_{n+1}$ es objeto de encriptación utilizando la clave de encriptación Kc_n a partir del triplete y el algoritmo de encriptación A_5 para complicar la captura (sniffing) de este parámetro en la interfaz de aire inalámbrica.

Según se explica haciendo referencia a la Figura 2A, el parámetro $RAND_{n+1}$ de AKA puede utilizarse para derivar un mensaje de autenticación de respuesta RES_{n+1} y/o una clave de encriptación Kc_{n+1} que puede memorizarse en la memoria 33 para una sesión de terminal posterior n+1.

De nuevo, las etapas 5a, 5b y 6 ilustran el uso de RES_{n+1} para una sesión de terminal posterior n+1 para una sesión de terminal posterior n+1 para demandar, de forma inmediata, la autenticación en la red para esta sesión. Los datos UD del mensaje de solicitud a enviarse en esta sesión de terminal pueden encriptarse utilizando el algoritmo de encriptación A_5 y la clave de encriptación Kc_{n+1}, derivándose está última del parámetro $RAND_{n+1}$ de AKA, recibida durante la sesión de terminal anterior *n*, K_i y el algoritmo de generación de claves A_8.

En general, cualquier etapa durante la sesión de terminal *n* puede utilizarse para proporcionar al terminal los parámetros de AKA aplicables para fines de autenticación y/o acuerdo de claves para una sesión de terminal posterior n+1.

En las formas de realización ilustradas en las Figuras 3A a 3C, la demanda de incorporación de IMSI fue rechazada para economizar recursos puesto que el mensaje de solicitud estaba ya transmitido a la red por esta demanda. Sin embargo, en conformidad con una forma de realización de la invención, la demanda de incorporación de IMSI puede aceptarse también con el fin de permitir la transmisión desde la red al terminal UE 3.

La Figura 3D es una ilustración de un sesión de terminal *n* en donde la demanda de incorporación de IMSI es aceptada (etapas 4a, 4b) con el fin de enviar el acuse de recibo del informe de entrega de los datos UD del mensaje de solicitud en el servidor de aplicación 2 en la etapa 5d. La inclusión de los parámetros de AKA no se ilustra en la Figura 3D. El terminal UE 3 puede, después de la recepción del informe de entrega en la etapa 5d, demandar la desincorporación desde la red en la etapa 6a, 6b que es aceptada por la red 1 en las etapas 7a, 7b. El parámetro $RAND_{n+1}$ de AKA puede transmitirse al terminal UE 3 durante las etapas 4a; 4b, etapa 5d o etapas 7a; 7b.

Las Figuras 4A a 4D proporcionan ilustraciones esquemáticas de procedimientos de AKA para una red de telecomunicaciones 3G en conformidad con las formas de realización de la invención.

La Figura 4A es una ilustración esquemática de un procedimiento de AKA en donde los datos de usuarios UD se transmiten en el mensaje de señalización desde un terminal UE 3 a una red 1.

En la etapa 1a, el terminal UE 3 transmite una demanda de incorporación que contiene el identificador de abonado IMSI los datos de usuarios UD del mensaje de solicitud y un mensaje de autenticación RES_n con el fin de demandar una sesión de terminal *n*. El mensaje de autenticación RES_n puede ser un mensaje de 128 bits. RES_n se obtiene, a modo de ejemplo, mediante una ejecución anterior de la forma de realización de la invención, según se explicará con más detalle haciendo referencia a la Figura 6. La demanda de incorporación se reenvía al RNC de la RAN de la Figura 1 y se reenvía al SGSN en la etapa 1b.

En la etapa 2a, el nodo SGSN emite una demanda de autenticación al HLR, conteniendo la demanda de autenticación el IMSI del UE 3. La demanda de autenticación se recibe en el HLR. El HLR recupera el mensaje de

respuesta de autenticación prevista $XRES_n$ y las claves criptográficas IK_n para protección de la integridad y CK_n para encriptación. Además, los parámetros $RAND_{n+1}$ y $AUTH_{n+1}$ de AKA se generan en el HLR para fines de AKA para una sesión de terminal posterior n+1 por el mismo terminal UE 3. Los parámetros $RAND_{n+1}$ y $AUTN_{n+1}$ tienen ambos una longitud de 128 bits. El HLR puede calcular ya $XRES_{n+1}$ e IK_{n+1} y CK_{n+1} para la sesión de terminal posterior n+1 y memorizar estos parámetros. En la etapa 2b, el HLR informa del quinteto [$RAND_{n+1}$, $AUTN_{n+1}$, $XRES_n$, IK_n, CK_n] al nodo SGSN. En el nodo SGSN, la autenticación del terminal 3 en la red 1 para la sesión de terminal *n* puede procesarse comparando RESn recibido en la etapa 1b, con $XRES_n$ del quinteto que se recibe en la etapa 2b. Si la autenticación tiene resultado satisfactorio, el terminal UE 3 y la red pueden conmutarse a un modo de seguridad (etapas 2c, 2d), en donde se conviene en que toda comunicación de señalización y datos posterior sea objeto de protección utilizando las claves IK_n y CK_n, respectivamente.

Los datos de usuarios UD, recibidos en la etapa 1b, pueden reenviarse luego al servidor M2M 2. En la forma de realización ilustrada en la Figura 4A, esta operación se realiza utilizando mensajes SMS por intermedio de las etapas 3a, 3b pero pueden aplicarse otros métodos de reenvío de los datos de usuario dentro de SGSN al servidor de aplicación 2. En la presente forma de realización, de nuevo de forma opcional, un acuse de recibo del mensaje de entrega de los datos de usuarios en el servidor de aplicación 2 se recibe en la etapa 3c en el nodo SGSN.

Puesto que los datos de usuarios están ya incluidos en el mensaje de señalización, esto es, la demanda de incorporación de IMSI en la presente forma de realización, no es necesario establecer una conexión de datos completa entre el terminal UE 3 y la red 1. Por lo tanto, en las etapas 4a, y 4b, un mensaje de rechazo de incorporación de IMSI se reenvía al terminal UE 3 desde la red 1 para evitar el establecimiento de una conexión completa y, en consecuencia, economizar recursos de red. El mensaje de rechazo de incorporación de IMSI contiene, sin embargo, los parámetros $RAND_{n+1}$ y $AUTN_{n+1}$ de AKA que se reciben por el terminal UE 3 como la etapa final de la sesión de terminal *n*.

El parámetro $RAND_{n+1}$ de AKA puede utilizarse para derivar un mensaje de autenticación de respuesta RES_{n+1} y/o las claves IK_{n+1} y CK_{n+1} que pueden memorizarse para una sesión de terminal posterior n+1. $AUTN_{n+1}$ se utiliza para la autenticación de red de una sesión de terminal posterior n+1 para determinar que $RAND_{n+1}$ fue recibido desde la red correcta.

Las etapas 5a, 5b y 6 ilustran el uso de RES_{n+1} para una sesión de terminal posterior n+1 para la demanda inmediata de la autenticación en la red para esta sesión.

La Figura 4B es una ilustración esquemática de un procedimiento de AKA en donde los datos de usuarios UD se transmiten en mensaje de señalización desde un terminal UE 3 a una red 1 en una forma encriptada.

En la etapa 1a, el terminal UE 3 transmite una demanda de incorporación que contiene el identificador de abonado IMSI, los datos de usuarios UD del mensaje de solicitud y un mensaje de autenticación RES_n con el fin de demandar una sesión de terminal *n*. El mensaje de autenticación RES_n puede ser un mensaje de 128 bits. RES_n se obtiene, a modo de ejemplo, mediante una ejecución anterior de la forma de realización de la invención, según se explicará más adelante haciendo referencia a la Figura 6. La demanda de incorporación se reenvía al RNC de la RAN que se ilustra en la Figura 1 y se reenvía al nodo SGSN en la etapa 1b. Los datos de usuarios UD se encriptan utilizando la clave de encriptación CK_n y un algoritmo de encriptación UMTS (p.ej., UEA1 o UEA2).

En la etapa 2a, el nodo SGSN emite una demanda de autenticación al HLR, conteniendo dicha demanda de autenticación el IMSI del UE 3. La demanda de autenticación se recibe en el HLR. El HLR recupera el mensaje de respuesta de autenticación prevista $XRES_n$ y las claves de encriptación IK_n para la encriptación de la señalización y CK_n para la encriptación de los datos de usuarios. Además, los parámetros de AKA $RAND_{n+1}$ y $AUTH_{n+1}$ se generan en el HLR para fines de AKA para una sesión de terminal posterior n+1 por el mismo terminal UE 3. $RAND_{n+1}$ y $AUTN_{n+1}$ tienen ambos una longitud de 128 bits. El HLR puede calcular ya $XRES_{n+1}$ e IK_{n+1} y CK_{n+1} para la sesión de terminal posterior n+1 y memorizar estos parámetros. En la etapa 2b, el HLR informa del quinteto [$RAND_{n+1}$, $AUTN_{n+1}$, $XRES_n$, IK_n, CK_n] al nodo SGSN. En el nodo SGSN, la autenticación del terminal 3 en la red 1 para la sesión de terminal *n* puede procesarse comparando RES_n que se recibe en la etapa 1b, con $XRES_n$ del quinteto que se recibe en la etapa 2b. Si la autenticación tiene un resultado satisfactorio, el terminal UE 3 y la red pueden conmutarse a un modo de seguridad (etapas 2c, 2d) en donde se conviene en que toda señalización posterior y la comunicación de datos sean objeto de protección utilizando las claves IK_n y CK_n, respectivamente.

Los datos de usuarios UD, recibidos en la etapa 1b pueden reenviarse luego al servidor M2M 2. De una u otra manera, los datos de usuarios UD se desencriptan en el RNC utilizando la clave de encriptación CK_n recibida en el quinteto y un algoritmo de encriptación con los datos de usuarios se reenvía en forma encriptada para su desencriptación en un nodo de red adicional o servidor de aplicación 2 que tenga acceso a la clave de encriptación CK_n y al algoritmo de encriptación. En la forma de realización ilustrada en la Figura 4B, el reenvío de los datos de usuarios UD se realiza utilizando mensajes SMS por intermedio de las etapas 3a, 3b pero se pueden aplicar otros métodos de reenvío de los datos de usuarios desde el nodo SGSN al servidor de aplicación 2. En la presente forma de realización, de nuevo de forma opcional, una confirmación de recibo de un mensaje de entrega de los datos de usuarios en el servidor de aplicación 2 se recibe en la etapa 3c en el nodo SGSN.

Puesto que los datos de usuarios están ya incluidos en el mensaje de señalización, esto es, la demanda de incorporación de IMSI en la presente forma de realización, no es necesario establecer una conexión de datos completa entre el terminal UE 3 y la red 1. Por lo tanto, en las etapas 4a y 4b, un mensaje de rechazo de incorporación de IMSI se reenvía al terminal UE 3 desde la red 1 para evitar el establecimiento de una conexión completa y, en consecuencia, economizar recursos de la red. El mensaje de rechazo de incorporación de IMSI contiene, sin embargo, los parámetros $RAND_{n+1}$ y $AUTN_{n+1}$ de AKA que se reciben por el terminal UE 3 como la etapa final de la sesión de terminal *n*.
El parámetro $RAND_{n+1}$ de AKA puede utilizarse para derivar un mensaje de respuesta de autenticación RES_{n+1} y/o las claves de encriptación IK_{n+1} y CK_{n+1} que pueden memorizarse para una sesión de terminal posterior n+1. $AUTN_{n+1}$ se utiliza para la autenticación de red de una sesión de terminal posterior n+1 para determinar que el $RAND_{n+1}$ fue recibido desde la red correcta.

Las etapas 5a, 5b y 6 ilustran el uso de RES_{n+1} para una sesión de terminal posterior n+1 para demandar inmediatamente la autenticación en la red para esta sesión. Los datos de usuario UD del mensaje de solicitud a envirarse en esta sesión de terminal pueden encriptarse utilizando un algoritmo de encriptación y la clave de encriptación $CK_{n+1,}$ derivándose esta última del parámetro $RAND_{n+1}$ de AKA recibido durante la sesión de terminal anterior *n*, K_i y un algoritmo de generación de claves.

La Figura 4C es una ilustración esquemática de un procedimiento de AKA en donde los datos de usuario UD se transmiten en mensajes de señalización desde un terminal UE 3 a una red 1 en forma encriptada y en donde los parámetros $RAND_{n+1}$ y $AUTN_{n+1}$ de AKA se transmiten al terminal UE 3 durante la sesión de terminal *n* que están también encriptados. Conviene señalar que, aunque la Figura 4C ilustra la opción combinada, no es necesario encriptar los datos de usuario UD del mensaje de solicitud cuando se encripta el parámetro $RAND_{n+1}$ de AKA.

En la etapa 1a, el terminal UE 3 transmite una demanda de incorporación que contiene el identificador de abonado IMSI, los datos de usuarios UD del mensaje de solicitud y un mensaje de autenticación RES_n con el fin de demandar una sesión de terminal *n*. El mensaje de autenticación RES_n puede ser un mensaje de 128 bits. RES_n se obtiene, a modo de ejemplo, mediante una ejecución anterior de la forma de realización anterior, según se explicará con más detalle haciendo referencia a la Figura 6. La demanda de incorporación se reenvía al RNC de la red RAN de la Figura 1 y se reenvía al nodo SGSN en la etapa 1b. Los datos de usuarios UD pueden encriptarse utilizando la clave de encriptación CK_n y el algoritmo de encriptación $A_{5.}$

En la etapa 2a, el nodo SGSN emite una demanda de autenticación al HLR, conteniendo dicha demanda de autenticación la IMSI del UE 3. La demanda de autenticación se recibe en el HLR. El HLR recupera el mensaje de respuesta de autenticación prevista $XRES_n$ y las claves de encriptación IK_n para la encriptación de la señalización y CK_n para la encriptación de datos de usuarios. Además, los parámetros $RAND_{n+1}$ y $AUTH_{n+1}$ de AKA se generan en el HLR para fines de AKA para una sesión de terminal posterior n+1 por el mismo terminal UE 3. $RAND_{n+1}$ y $AUTN_{n+1}$ tienen ambos una longitud de 128 bits. El HLR puede calcular ya $XRES_{n+1}$ e IK_{n+1} y CK_{n+1} para la sesión de terminal posterior n+1 y memorizar estos parámetros. En la etapa 2b, el HLR informa del quinteto [$RAND_{n+1,}$ $AUTN_{n+1,}$ $XRES_{n,}$ $IK_{n,}$ CK_n] al nodo SGSN. En el nodo SGSN, la autenticación del terminal 3 en la red 1 para la sesión de terminal *n* puede procesarse comparando el RES_n que se recibe en la etapa 1b con el $XRES_n$ del quinteto que se recibe en la etapa 2b.

Los datos de usuarios UD, recibidos en la etapa 1b, pueden reenviarse luego al servidor M2M 2. Cuando se encriptan los datos de usuarios, los datos de usuarios UD pueden desencriptarse en el RNC utilizando la clave de encriptación CK_n recibida en el quinteto y un algoritmo de encriptación de UMTS o los datos de usuarios se reenvían en forma encriptada para su desencriptación en un nodo de red adicional o el servidor de aplicación 2 que tenga acceso a la clave de encriptación CK_n y el algoritmo de encriptación. En la forma de realización ilustrada en la Figura 4C, el reenvío de los datos de usuarios UD se realiza utilizando mensajes SMS por intermedio de las etapas 3a, 3b, pero se pueden aplicar otros métodos de reenvío de los datos de usuarios desde el nodo SGSN al servidor de aplicación 2. En la presente forma de realización, de nuevo de forma opcional, una confirmación de recibo del mensaje de entrega de los datos de usuarios en el servidor de aplicación 2 se recibe en la etapa 3c en el nodo SGSN.

Puesto que los datos de usuarios están ya incluidos en el mensaje de señalización, esto es, la demanda de incorporación de IMSI en la presente forma de realización, no es necesario establecer una conexión de datos completa entre el terminal UE 3 y la red 1. Por lo tanto, en las etapas 4a y 4b un mensaje de rechazo de incorporación de IMSI se reenvía al terminal UE 3 desde la red 1 para evitar el establecimiento de una conexión completa y en consecuencia, economizar recursos de red. El mensaje de rechazo de incorporación de IMSI contiene, sin embargo, los parámetros $RAND_{n+1}$ y $AUTN_{n+1}$ de AKA que se reciben por el terminal UE 3 como la etapa final de la sesión de terminal *n*. En la forma de realización ilustrada en la Figura 4C, los parámetros $RAND_{n+1}$ y $AUTN_{n+1}$ de AKA están encriptados utilizando la clave de encriptación CK_n a partir del quinteto recibido en la etapa 2b y un algoritmo de encriptación para complicar la captura denominada *sniffing* de estos parámetros en la interfaz de aire inalámbrica.

El parámetro $RAND_{n+1}$ de AKA puede utilizarse para derivar un mensaje de autenticación RES_{n+1} y/o las claves criptográficas IK_{n+1} y CK_{n+1} que pueden memorizarse para una sesión de terminal posterior n+1. $AUTN_{n+1}$ se utiliza para la autenticación de red de una sesión de terminal posterior n+1 para determinar que $RAND_{n+1}$ fue recibido desde la red correcta.

Las etapas 5a, 5b y 6 ilustran el uso de RES_{n+1} para una sesión de terminal posterior n+1 para la demanda inmediata de la autenticación en la red para esta sesión. Los datos de usuarios UD del mensaje de solicitud a enviarse en esta sesión de terminal pueden encriptarse utilizando un algoritmo de encriptación y la clave de encriptación $CK_{n+1,}$ siendo esta última derivada del parámetro $RAND_{n+1}$ de AKA, recibido durante la sesión de terminal anterior *n*, K_i y un algoritmo de generación de claves.
Conviene señalar que, según se describió anteriormente para las redes 2G con referencia a la Figura 3D, no se requiere rechazar la demanda de incorporación de IMSI para la sesión de terminal *n* y para proporcionar los parámetros de AKA para la sesión de terminal posterior n+1 con el rechazo de incorporación de IMSI. La conexión para la sesión de terminal *n* puede establecerse y, durante cualquiera de las etapas de esta sesión, los parámetros de AKA pueden reenviarse desde la red 1 al terminal UE 3.

La Figura 4D es una ilustración esquemática de un procedimiento de AKA en donde los datos de usuarios UD se transmiten en mensajes de señalización desde un terminal UE 3 a una red 1 y en donde también un código de autenticación de mensaje MAC para los datos de usuarios UD, indicado como MAC_key(UD) en donde el término *key* indica la clave utilizada para generar MAC. Conviene señalar que el código de autenticación de mensajes puede aplicarse también a otros elementos de datos dentro de la demanda de incorporación o incluso la demanda de incorporación completa, con lo que se permite la protección de la integridad de otros elementos de datos (p.ej., IMSI, RES) de la demanda de incorporación.

En la etapa 1a, el terminal UE 3 transmite una demanda de incorporación que contiene el identificador de abonado IMSI, los datos de usuarios UD del mensaje de solicitud y un mensaje de autenticación RES_n con el fin de demandar una sesión de terminal *n*, de forma similar a la que se ilustra en la Figura 4A. El mensaje de autenticación RES_n puede ser un mensaje de 128 bits. RES_n es, p.ej., obtenido mediante una ejecución anterior de la forma de realización de la invención, según se explicará más adelante haciendo referencia a la Figura 6.

Además, la demanda de incorporación contiene un código de autenticación de mensaje MAC para la sesión de terminal *n*. El código de autenticación de mensaje MAC ha sido generado en el terminal UE 3 utilizando una clave de integridad IK_n obtenida durante una ejecución anterior de la presente forma de realización en donde los parámetros de AKA para la sesión de terminal *n* fueron ya recibidos.

La demanda de incorporación se reenvía a un nodo de red adicional, p.ej., el RNC o el nodo eNodeB de la red RAN de la Figura 1 y se reenvían al nodo SGSN en la etapa 1b.

En la etapa 2a, el nodo SGSN emite una demanda de autenticación al HLR, conteniendo la demanda de autenticación el IMSI del UE 3. La demanda de autenticación se recibe en el HLR. El HLR recupera el mensaje de respuesta de autenticación prevista $XRES_n$ y las claves criptográficas IK_n para protección de la integridad y CK_n para la encriptación. Además, los parámetros $RAND_{n+1}$ y $AUTH_{n+1}$ de AKA se generan en el HLR para fines de AKA para una sesión de terminal posterior n+1 por el mismo terminal UE 3. $RAND_{n+1}$ y $AUTN_{n+1}$ tienen ambos una longitud de 128 bits. El HLR puede calcular ya $XRES_{n+1}$ e IK_{n+1} y CK_{n+1} para la sesión de terminal posterior n+1 y memorizar estos parámetros. En la etapa 2b, el HLR informa del quinteto [$RAND_{n+1,}$ $AUTN_{n+1,}$ $XRES_n$, $IK_{n,}$ CK_n] al nodo SGSN. En el nodo SGSN, la autenticación del terminal 3 en la red 1 para la sesión de terminal *n* puede procesarse comparando RES_n que se recibe en la etapa 1b, con $XRES_n$ del quinteto que se recibe en la etapa 2b. Además, la integridad de los datos de usuarios UD puede verificarse en el nodo SGSN generando el código de autenticación de mensaje $XMAC\_IK_n$ (UD) prevista utilizando la clave de integridad IK_n procedente del quinteto y un algoritmo de MAC adecuado. $XMAC\_IK_n$ (UD) puede compararse luego con MAC_IK_n (UD) que se recibe en la etapa 1b. Si la autenticación tiene un resultado satisfactorio, el terminal UE 3 y la red pueden conmutarse a un modo de seguridad (etapas 2c, 2d), en donde se conviene en que toda señalización y comunicación de datos adicionales esté protegida utilizando las calves IK_n y CK_n, respectivamente.

Conviene señalar que la integridad de los datos de usuarios UD puede verificarse también por el servidor de aplicación 2. En ese caso, el nodo SGSN del HLR debe enviar la clave de protección de integridad IK_n al servidor de aplicación 2 y el servidor de aplicación 2 debe tener acceso al algoritmo de MAC.

Los datos de usuarios UD recibidos en la etapa 1b, pueden reenviarse al servidor M2M 2. En la forma de realización ilustrada en la Figura 4D, esta operación se realiza utilizando mensajes SMS por intermedio de las etapas 3a, 3b, pero pueden aplicarse otros métodos de reenvío de los datos de usuarios desde el nodo SGSN al servidor de aplicación 2. En la presente forma de realización, de nuevo de forma opcional, una confirmación de recibo del mensaje de entrega de los datos de usuarios en el servidor de aplicación 2 se recibe en la etapa 3c en el nodo SGSN.

Puesto que los datos de usuarios están ya incluidos en el mensaje de señalización, esto es, la demanda de

incorporación de IMSI en la presente forma de realización, no es necesario establecer una comunicación de datos completa entre el terminal UE 3 y la red 1. Por lo tanto, en las etapas 4a y 4b, un mensaje de rechazo de incorporación de IMSI se reenvía al terminal UE 3 desde la red 1 para evitar el establecimiento de una conexión completa y, en consecuencia, economizar recursos de red. El mensaje de rechazo de incorporación de IMSI contiene, sin embargo, los parámetros $RAND_{n+1}$ y $AUTN_{n+1}$ de AKA que se reciben por el terminal UE 3 como la etapa final de la sesión de terminal *n*.

El parámetro $RAND_{n+1}$ de AKA puede utilizarse para derivar un mensaje de autenticación RES_{n+1} y/o las claves criptográficas IK_{n+1} y CK_{n+1} que pueden memorizarse para una sesión de terminal posterior n+1. $AUTN_{n+1}$ se utiliza para la autenticación de red de una sesión de terminal posterior n+1 para determinar que el $RAND_{n+1}$ fue recibido desde la red correcta.

Las etapas 5a, 5b y 6 ilustran el uso de RES_{n+1} para una sesión de terminal posterior n+1 para la demanda inmediata de la autenticación en la red para esta sesión, incluyendo también un mensaje de verificación de integridad encriptada MAC_ IK_{n+1} (UD) encriptado bajo la clave de integridad derivada IK_{n+1}.

Conviene señalar que la forma de realización de la verificación de integridad para la red 3G de la Figura 4D es también aplicable para las redes 2G y 4G. Para las redes 2G modernas, en donde puede aplicarse un USIM, una clave de integridad está disponible en la tarjeta USIM después del procesamiento de la orden de autenticación AUTHENTICATE. Cuando se utiliza una tarjeta SIM, es posible utilizar la clave de encriptación Kc para generar el código de integridad de mensaje MAC. Para las redes 4G se puede aplicar un procedimiento similar como el que se ilustra en la Figura 4D, utilizando p.ej., la clave de integridad $KNASint_n$ para la encriptación del mensaje de verificación de integridad MAC_n.

La Figura 5 proporciona una ilustración esquemática de un procedimiento de AKA para una red de telecomunicaciones 4G en conformidad con una forma de realización de la invención utilizando la encriptación de los datos de usuarios UD del mensaje de aplicación y los parámetros $RAND_{n+1}$ y $AUTN_{n+1}$ de AKA. Conviene señalar que estas etapas de encriptación son opcionales.

En la etapa 1a, el terminal UE 3 transmite una demanda de incorporación que contiene el indicador de abonado IMSI, los datos de usuarios UD del mensaje de solicitud y un mensaje de autenticación RES_n con el fin de demandar una sesión de terminal *n*. El mensaje de autenticación RES_n puede ser un mensaje de 128 bits de longitud. RES_n se obtiene, a modo de ejemplo, mediante una ejecución anterior de la forma de realización de la invención, según se explicará más adelante con referencia a la Figura 6. La demanda de incorporación se reenvía al nodo NodeB de la red E-UTRAN según se ilustra en la Figura 1 y se reenvía a la entidad MME en la etapa 1b. Los datos de usuarios UD pueden encriptarse utilizando la clave de encriptación $KNASenc_n$ y un algoritmo de encriptación. Otra clave, derivada de KASME puede, sin embargo, utilizarse para esta finalidad.

En la etapa 2a, la entidad MME emite una demanda de autenticación al servidor HSS, conteniendo dicha demanda de autenticación el IMSI del UE 3. La demanda de autenticación se recibe en el servidor HSS. El servidor HSS recupera el mensaje de respuesta de autenticación prevista $XRES_n$ y la clave de encriptación $KASME_n$. Además, los parámetros de encriptación $RAND_{n+1}$ y $AUTH_{n+1}$ de AKA se generan en el servidor HSS para fines de AKA para una sesión de terminal posterior n+1 por el mismo terminal UE 3, equivalente como para las redes 3G. $RAND_{n+1}$ y $AUTN_{n+1}$ tienen ambos una longitud de 128 bits. El servidor HSS puede calcular ya $XRES_{n+1}$ y $KASME_{n+1}$ para la sesión de terminal posterior n+1 y memorizar estos parámetros. En la etapa 2b, el servidor HSS informa del cuarteto [$RAND_{n+1}$, $AUTN_{n+1}$, $XRES_n$, $KASME_n$] a la entidad MME. En la entidad MME, la autenticación de terminal 3 en la red 1 para la sesión de terminal *n* puede procesarse comparando RES_n que se recibe en la etapa 1b con $XRES_n$ del cuarteto que se recibe en la etapa 2b. Si la autenticación tiene un resultado satisfactorio, el terminal UE 3 y la red pueden conmutarse a un modo de seguridad, en donde se conviene en que toda comunicación de datos y señalización adicional se realice bajo claves de encriptación, respectivamente.

Conviene señalar que para los sistemas de EPC, existen dos órdenes del modo de seguridad, una entre el terminal UE 3 y la entidad MME (la orden del modo de seguridad NAS) para iniciar protecciones de integridad y/o la encriptación de la señalización en la red base (el estrato de no acceso NAS) y otro entre el terminal UE 3 y el nodo (la orden del módulo de seguridad AS) para iniciar la protección de integridad y la encriptación de la señalización de RRC y la encriptación en el plano del usuario para la red de acceso de radio (el estrato de acceso AS).

Los datos de usuarios UD recibidos en la etapa 1b, pueden reenviarse luego al servidor M2M 2. Cuando se encriptan los datos de usuarios, los datos de usuarios UD pueden desencriptarse en la entidad MME utilizando la clave de encriptación derivada de $KASME_n$ tal como $KNASenc_n$ que se recibe en el cuarteto y un algoritmo de encriptación o los datos de usuarios se reenvían en forma encriptada para su desencriptación en un nodo de red adicional o servidor de aplicación 2 que tiene acceso a la clave de encriptación y al algoritmo de encriptación. En la forma de realización ilustrada en la Figura 5, el reenvío de los datos de usuarios UD se realiza utilizando mensajes SMS, por intermedio de las etapas 3a, 3b, pero se pueden aplicar otros métodos de reenvío de datos de usuarios desde la entidad MME al servidor de aplicación 2. En la presente forma de realización, de nuevo de forma opcional, una confirmación de recibo de un mensaje de entrega de los datos de usuarios en el servidor de aplicación 2 se

recibe en la etapa 3c en la entidad MME.

Puesto que los datos de usuarios están ya incluidos en el mensaje de señalización, esto es, la demanda de incorporación de IMSI en la presente forma de realización, no es necesario establecer una conexión de datos completa entre el terminal UE 3 y la red 1. Por lo tanto, en las etapas 4a y 4b, un mensaje de rechazo de incorporación de IMSI se reenvía al terminal UE 3 desde la red 1 para evitar el establecimiento de una conexión completa y, en consecuencia, economizar recursos de red. El mensaje de rechazo de incorporación de IMSI contiene, sin embargo, los parámetros $RAND_{n+1}$ y $AUTN_{n+1}$ de AKA que se reciben por el terminal UE 3 como la etapa final de la sesión de terminal n. En la forma de realización ilustrada en la Figura 5, los parámetros $RAND_{n+1}$ y $AUTN_{n+1}$ de AKA son objeto de encriptación utilizando la clave de encriptación $KNASenc_n$ que se deriva de $KASME_n$ a partir del cuarteto recibido en la etapa 2b y un algoritmo de encriptación complican la captura del tipo sniffing de este parámetro en la interfaz de aire inalámbrica.

El parámetro $RAND_{n+1}$ de AKA puede utilizarse para derivar un mensaje de autenticación de respuesta RES_{n+1} y/o claves de encriptación IK_{n+1} y CK_{n+1} que pueden memorizarse para una sesión de terminal posterior n+1. $AUTN_{n+1}$ se utiliza para la autenticación de red de una sesión de terminal posterior n+1 para determinar que el $RAND_{n+1}$ fue recibido desde la red correcta.

Las etapas 5a, 5b y 6 ilustran el uso de RES_{n+1} para una sesión de terminal posterior n+1 para la demanda inmediata de la autenticación en la red para esta sesión. Los datos de usuarios UD del mensaje de solicitud a enviarse en esta sesión pueden encriptarse utilizando un algoritmo de encriptación y la clave de encriptación derivada de $KASME_{n+1}$ siendo esta última derivada del parámetro $RAND_{n+1}$ de AKA que se recibe durante la sesión de terminal anterior *n*, K_i y un algoritmo de generación de claves.

La Figura 6 proporciona un diagrama de estados para el terminal 3 y un nodo de red, tal como el HLR o HSS de la Figura 1, ilustrando los dados (los círculos) y las transiciones de estados.

La flecha I ilustra la situación en donde ni el terminal 3 ha recibido un parámetro de AKA durante una sesión de terminal anterior para una sesión de terminal siguiente ni el HLR ha memorizado información de AKA. Por lo tanto, una demanda de incorporación de IMSI no puede contener un mensaje de respuesta RES_n y el procedimiento de AKA normal según se describe en la sección precedente se realiza a este respecto.

La flecha II ilustra la situación en donde la demanda de incorporación de IMSI para la sesión de terminal *n* contiene RES_n. Sin embargo, el HLR no ha memorizado la información de AKA para esta sesión de terminal *n* incluyendo el parámetro de AKA para la sesión de terminal n+1. Por lo tanto, RES_n es rechazada y se seguirá el procedimiento de AKA convencional.

De forma similar, según se ilustra por la flecha III, el procedimiento de AKA convencional se sigue si el mensaje de demanda de incorporación de IMSI no contiene RES_n por lo que el HLR/HSS habría memorizado el vector AKA. A continuación, HLR/HSS elimina la información de AKA para la sesión de terminal *n*.

La flecha IV ilustra la situación en donde los parámetros $RAND_{n+1}$ / $AUTN_{n+1}$ de AKA se transmiten desde la red al terminal 3, p.ej., en un mensaje de rechazo de incorporación de IMSI, un informe de entrega o un mensaje de aceptación de la desincorporación de IMSI desde la red. Tanto el HLR/HSS como el terminal 3 pueden calcular ahora y memorizar la información de AKA, esto es, (X) RES_{n+1} y/o las claves para la sesión de terminal n+1.

Por último, la flecha V ilustra la situación ilustrada en las Figuras 3A-3D, Figuras 4A-4C y Figura 5, en donde el (primer) mensaje de señalización desde el terminal 3 a la red contiene ya el mensaje de respuesta de autenticación RES_n y el mensaje (final) desde la red para la sesión de terminal *n* contiene los parámetros $RAND_{n+1}$, $AUTN_{n+1}$ de AKA que permiten al terminal 3 y al HLR/HSS calcular y memorizar al menos un mensaje de autenticación RES_{n+1} y/o la clave para una sesión de terminal posterior n+1.

Las formas de realización anteriores permiten reducir el número de mensajes en la red de telecomunicación. Debe entenderse que la idea inventiva puede aplicarse también fuera del campo de las comunicaciones máquina a máquina y no requiere que los mensajes de solicitud/datos de usuarios se incorporen en el mismo mensaje (señalización) como el mensaje de autenticación de respuesta RES.

Una realización muy esquemática, a modo de ejemplo de dicha forma de realización se proporciona en la Figura 7 para una red 2G. Una demanda de conexión para una sesión de terminal *n* incluye ya un mensaje de autenticación de respuesta RES_n que puede utilizarse para la autenticación del terminal en la red después de recibir la respuesta de autenticación $XRES_n$ desde el HLR. Después de la autenticación, puede realizarse un intercambio de información entre el terminal 3 y un dispositivo de destino.

El triplete recibido desde el HLR contiene también el parámetro $RAND_{n+1}$ de AKA que se comunica al terminal 3, a modo de ejemplo, durante la aceptación de la demanda de conexión según se ilustra en la Figura 7 o en otra etapa (p.ej., durante la terminación de la sesión *n*). El parámetro $RAND_{n+1}$ de AKA comunicado puede utilizarse en el

terminal 3 para la autenticación y/o generación de claves en el lado del terminal de la misma manera que se examinó con anterioridad. El dispositivo de destino de la Figura 7 puede ser un servidor o un terminal de otro usuario.

Conviene señalar que, aunque en las formas de realización anteriormente descritas se aplican claves existentes, nuevas claves especiales pueden aplicarse, como alternativa, y que pueden derivarse de las claves ya existentes.

Conviene señalar también que, aunque en las formas de realización anteriores, el terminal recibe el al menos un par de AKA durante la sesión de terminal *n* para autenticación o acuerdo de claves para un terminal, otros dispositivos de destino, tales como los nodos de red SGSN, NodeB, MSC, MME según se ilustra en la Figura 1 pueden recibir también el al menos un parámetro de AKA y proporcionar información para el terminal para autenticación o utilización de claves durante una sesión de terminal posterior n+m.

REIVINDICACIONES

1. Un método para permitir la autenticación o acuerdo de claves por un terminal (3) en una red (1) que comprende las etapas de:

derivar en el terminal (3), durante una sesión de terminal *n*, un primer mensaje de autenticación RES_n;

caracterizado por cuanto que el método incluye además:

transmitir, durante la sesión de terminal *n*, un mensaje de rechazo de incorporación de IMSI que contiene al menos un parámetro de autenticación $RAND_{n+m}$ o parámetros de aplicación $RAND_{n+m}$, $AUTN_{n+m}$, al terminal (3) en donde RAND es un número aleatorio y AUTN es una ficha de autenticación y en donde el al menos un parámetro de autenticación permite la autenticación o el acuerdo de claves por el terminal en la red para una sesión de terminal posterior n+m.

2. El método según la reivindicación 1 en donde el primer mensaje de autenticación RES_n se deriva en el terminal utilizando al menos un primer parámetro de autenticación $RAND_n$.

3. El método según la reivindicación 2, en donde el primer mensaje de autenticación RES_n se deriva en el terminal utilizando al menos un primer parámetro de autenticación, $RAND_n$ y una clave secreta K_i.

4. El método según la reivindicación 1 que comprende, además, la etapa de recibir una demanda de incorporación procedente del terminal (3) en la red (1) para la sesión de terminal posterior n+m, conteniendo dicha demanda de incorporación datos de usuarios UD, de un mensaje de solicitud destinados para un servidor de aplicación en o conectado a la red.

5. El método según la reivindicación 4, en donde la demanda de incorporación contiene uno o más de entre un identificador de terminal IMSI, datos de usuarios UD de mensaje de solicitud o el primer mensaje de autenticación RES_n.

6. El método según la reivindicación 4, que comprende, además la etapa de la recepción de los datos de solicitud (UD) en la red (1) en forma encriptada durante la sesión de terminal posterior n+m, obteniéndose la forma encriptada en el terminal mediante la encriptación del mensaje de solicitud utilizando al menos una clave o parámetro de autenticación (Kc_{n+m}; $CK_{n+m;}$ $KNASenc_{n+m}$) derivada utilizando al menos el al menos un segundo parámetro de autenticación $RAND_{n+m}$ recibido durante la sesión de terminal *n*.

7. El método según una o más de las reivindicaciones precedentes, que comprende, además, la etapa de recepción de una demanda de incorporación desde el terminal (3) en la red para la sesión de terminal posterior n+m, conteniendo dicha demanda de incorporación un código de autenticación de mensajes, MAC, para la protección de la integridad de al menos una parte del mensaje de demanda de incorporación, obteniéndose el código MAC en el terminal utilizando un algoritmo de MAC criptográfico y al menos una clave, o parámetro de autenticación (Kc_{n+m}; IK_{n+m}; $KNASint_{n+m}$) derivado utilizando al menos el al menos un segundo parámetro de autenticación, $RAND_{n+m}$, recibido durante la sesión de terminal *n*.

8. El método según una o más de las reivindicaciones precedentes, que comprende la etapa de transmitir, durante la sesión de terminal *n*, el al menos un segundo parámetro de autenticación, $RAND_{n+m}$, o parámetros de autenticación $RAND_{n+m}$, $AUTH_{n+m}$ desde la red al terminal en forma encriptada.

9. Un nodo de red que está configurado para la autenticación o acuerdo de claves para un terminal en una red de telecomunicación que comprende:

- una interfaz de recepción (20) configurada para recibir, durante una sesión de terminal *n*, una primera demanda de autenticación procedente del terminal que contiene un identificador (IMSI) del terminal y un primer mensaje de autenticación, RES_n derivado del terminal utilizando al menos un primer parámetro de autenticación $RAND_n$;

- un generador configurado para generar al menos un parámetro de autenticación $RAND_{n+m}$ o los parámetros de autenticación $RAND_{n+m}$, $AUTN_{n+m}$, que permiten la autenticación y/o el acuerdo de claves para el terminal identificado en la red o nodo de red para una sesión de terminal posterior n+m;

- una interfaz de transmisión (21) configurada para transmitir durante la sesión de terminal *n* un mensaje de rechazo de incorporación de IMSI que contiene el al menos un parámetro de autenticación, $RAND_{n+m}$, o parámetros de autenticación, $RAND_{n+m}$, $AUTN_{n+m}$, destinados para el terminal;

en donde RAND es un número aleatorio y AUTN es una denominada ficha de autenticación.

10. El nodo de red según la reivindicación 9, en donde el nodo de red está configurado, además, para transmitir al

menos uno de entre un mensaje de autenticación prevista, $XRES_n$ al menos una clave de encriptación/desencriptación, o parámetros de autenticación, (Kc_n; IK_n, CK_n; $KASME_n$) a un nodo de red adicional para la sesión de terminal *n* en combinación con el al menos un parámetro de autenticación, $RAND_{n+m}$, o parámetros de autenticación, $RAND_{n+m}$, $AUTN_{n+m}$ para la sesión de terminal posterior n+m.

11. El método según la reivindicación 1, para permitir la autenticación o el acuerdo de claves para el terminal (3) en la red (1) que comprende, además:

- durante la sesión de terminal *n* la realización de las etapas de:

enviar una primera demanda de autenticación desde el terminal (3) que contiene el primer mensaje de autenticación, RES_n derivado en el terminal utilizando al menos un primer parámetro de autenticación $RAND_n$,

la recepción de al menos un segundo parámetro de autenticación, $RAND_{n+m}$, o parámetros de autenticación, $RAND_{n+m}$, $AUTN_{n+m}$;

y

- para la sesión de terminal posterior n+m, la autenticación y/o establecimiento de un acuerdo de claves para el terminal (3) en la red (1) utilizando el al menos un segundo parámetro de autenticación, $RAND_{n+m}$, o parámetros de autenticación, $RAND_{n+m}$, $AUTN_{n+m}$.

12. El método según la reivindicación 11 que comprende, además, la etapa de transmitir una demanda de incorporación a la red para la sesión de terminal posterior n+m, conteniendo dicha demanda de incorporación un mensaje de solicitud, UD, destinado para un servidor de aplicación en o conectado a la red y un mensaje de autenticación RES_{n+m}, derivado en el terminal utilizando el al menos un segundo parámetro de autenticación, $RAND_{n+m}$, o parámetros de autenticación, $RAND_{n+m}$, $AUTN_{n+m}$, recibidos durante la sesión de terminal *n*.

13. El método según la reivindicación 12 que comprende, además, la etapa de encriptación del mensaje de solicitud transmitido con la demanda de incorporación de la sesión de terminal posterior n+m utilizando al menos una clave o parámetros de autenticación (Kc_{n+m}; CK_{n+m}; $KNASenc_{n+m}$) derivados utilizando al menos un segundo parámetro de autenticación, $RAND_{n+m}$, recibido durante la sesión de terminal *n*.

14. El método según una o más de las reivindicaciones precedentes 11 a 13 que comprende la etapa de generar un código de autenticación de mensaje (MAC) para protección de la integridad de al menos una parte de un mensaje de demanda de incorporación para la sesión de terminal n+m que utiliza al menos una clave o parámetros de autenticación (Kc_{n+m}; IK_{n+m}; $KNASint_{n+m}$) derivados utilizando al menos el al menos un segundo parámetro de autenticación, $RAND_{n+m}$, recibido durante la sesión de terminal *n* y transmitir el código de autenticación de mensaje a la red en la demanda de incorporación.

15. El método según una o más de las reivindicaciones precedentes 11 a 14, que comprende las etapas de:

- recibir, durante la sesión de terminal *n*, el al menos un segundo parámetro de autenticación, $RAND_{n+m}$, o parámetros de autenticación, $RAND_{n+m}$, $AUTH_{n+m}$, desde la red al terminal en forma encriptada; y

- la desencriptación de al menos un segundo parámetro de autenticación encriptado, $RAND_{n+m}$, o parámetros de autenticación, $RAND_{n+m}$, $AUTH_{n+m}$, para derivar un mensaje de autenticación, RES_{n+m}.

16. Un terminal, configurado para la autenticación o acuerdo de claves en una red, comprendiendo dicho terminal:

- una interfaz de transmisión configurada para transmitir durante una sesión de terminal *n*, una primera demanda de autenticación desde el terminal que contiene un primer mensaje de autenticación, RES_n, derivado en el terminal utilizando al menos un primer parámetro de autenticación $RAND_n$;

- una interfaz de recepción configurada para recibir, durante una sesión de terminal *n*, un mensaje de rechazo de incorporación de IMSI que contiene al menos un segundo parámetro de autenticación, $RAND_{n+m}$, o parámetros de autenticación, $RAND_{n+m}$, $AUTN_{n+m}$, para una sesión de terminal posterior n+m desde la red;

- un procesador configurado para derivar un mensaje de autenticación, RES_{n+m} o derivar una clave utilizando el al menos un segundo parámetro de autenticación, $RAND_{n+m}$, o parámetros de autenticación, $RAND_{n+m}$, $AUTN_{n+m}$, recibidos durante la sesión de terminal *n*;

en donde RAND es un número aleatorio y AUTN es una ficha de autenticación.

17. El terminal según la reivindicación 16 que comprende, además, una interfaz de transmisión configurada para transmitir, durante la sesión de terminal posterior n+m, el mensaje de autenticación derivado RES_{n+m} y/o datos

encriptados bajo la clave derivada a la red para su autenticación y/o acuerdo de claves para el terminal en la red.

18. El terminal según la reivindicación 16, en donde el terminal está configurado para ejecutar el método según una o más de las reivindicaciones 13 a 17.

19. Un programa informático o conjunto de programas en cooperación caracterizado por cuanto que comprenden partes de código de software configurado para, cuando se ejecuta por un procesador, realizar las etapas del método según una o más de las reivindicaciones 1 a 8 o una o más de las reivindicaciones 11 a 15.

20. Un sistema que comprende al menos un terminal y un nodo de red de una red de telecomunicación, en donde

el nodo de red comprende:

- una interfaz de recepción configurada para recibir, durante una sesión de terminal *n*, un identificador (IMSI) del terminal y una primera demanda de autenticación desde el terminal que contiene un primer mensaje de autenticación, RES_n derivado desde el terminal utilizando al menos un primer parámetro de autenticación $RAND_n$;

- un generador configurado para generar al menos un segundo parámetro de autenticación $RAND_{n+m}$ o los parámetros de autenticación $RAND_{n+m}$, $AUTN_{n+m}$, que permiten la autenticación o el acuerdo de claves para el terminal identificado en la red o nodo de red para una sesión de terminal posterior n+m;

- una interfaz de transmisión configurada para transmitir durante la sesión de terminal *n* un mensaje de rechazo de incorporación de IMSI que contiene el al menos un segundo parámetro de autenticación $RAND_{n+m}$ o parámetros de autenticación $RAND_{n+m}$, $AUTN_{n+m}$, destinados para el terminal y en donde el terminal comprende:

- una interfaz de transmisión configurada para transmitir, durante un sesión de terminal *n*, una primera demanda de autenticación desde el terminal que contiene un primer mensaje de autenticación, RES_n derivado en el terminal utilizando al menos un primer parámetro de autenticación $RAND_n$;

- una interfaz de recepción configurada para recibir, durante la sesión de terminal *n*, el mensaje de rechazo de incorporación de IMSI que contiene el al menos un segundo parámetro de autenticación $RAND_{n+m}$, o parámetros de autenticación $RAND_{n+m}$, $AUTN_{n+m}$ para la sesión de terminal posterior n+m desde la red;

- un procesador configurado para derivar un mensaje de autenticación RES_{n+m} y/o derivar una clave utilizando el al menos un segundo parámetro de autenticación $RAND_{n+m}$ o los parámetros de autenticación $RAND_{n+m}$, $AUTN_{n+m}$, recibidos durante la sesión de terminal *n*;

y en donde RAND es un número aleatorio y AUTN es una ficha de autenticación.

21. El sistema según la reivindicación 20 que comprende, además, una interfaz de transmisión configurada para transmitir, durante la sesión de terminal posterior n+m, el mensaje de autenticación derivado RES_{n+m} y/o datos encriptados bajo la clave derivada a la red para su autenticación o acuerdo de claves para el terminal en la red para la sesión de terminal posterior n+m.

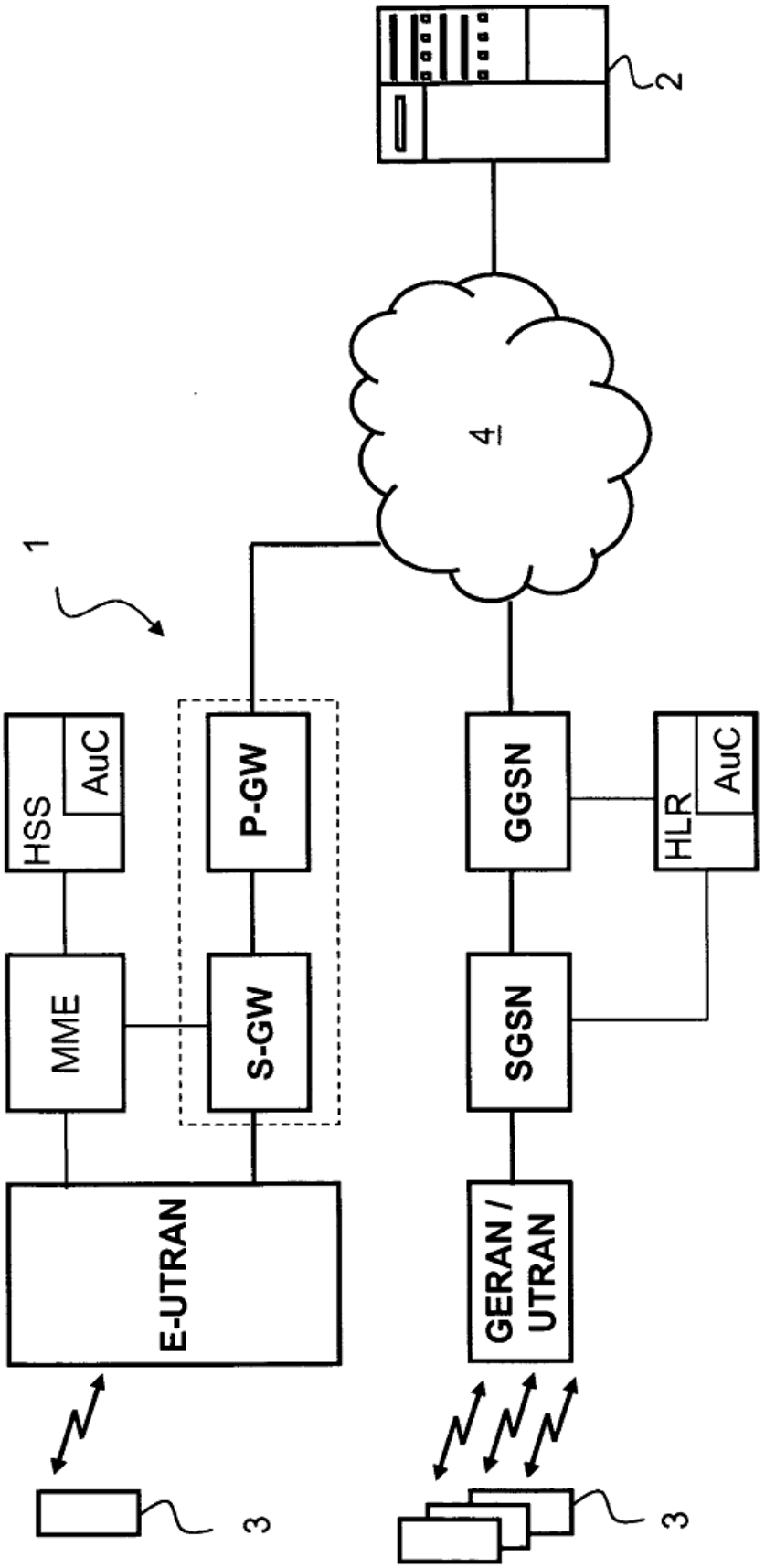
2
4
1
HSS
AuC
P-GW
GGSN
HLR
AuC
MME
S-GW
SGSN
E-UTRAN
GERAN / UTRAN
3
3

FIG. 1

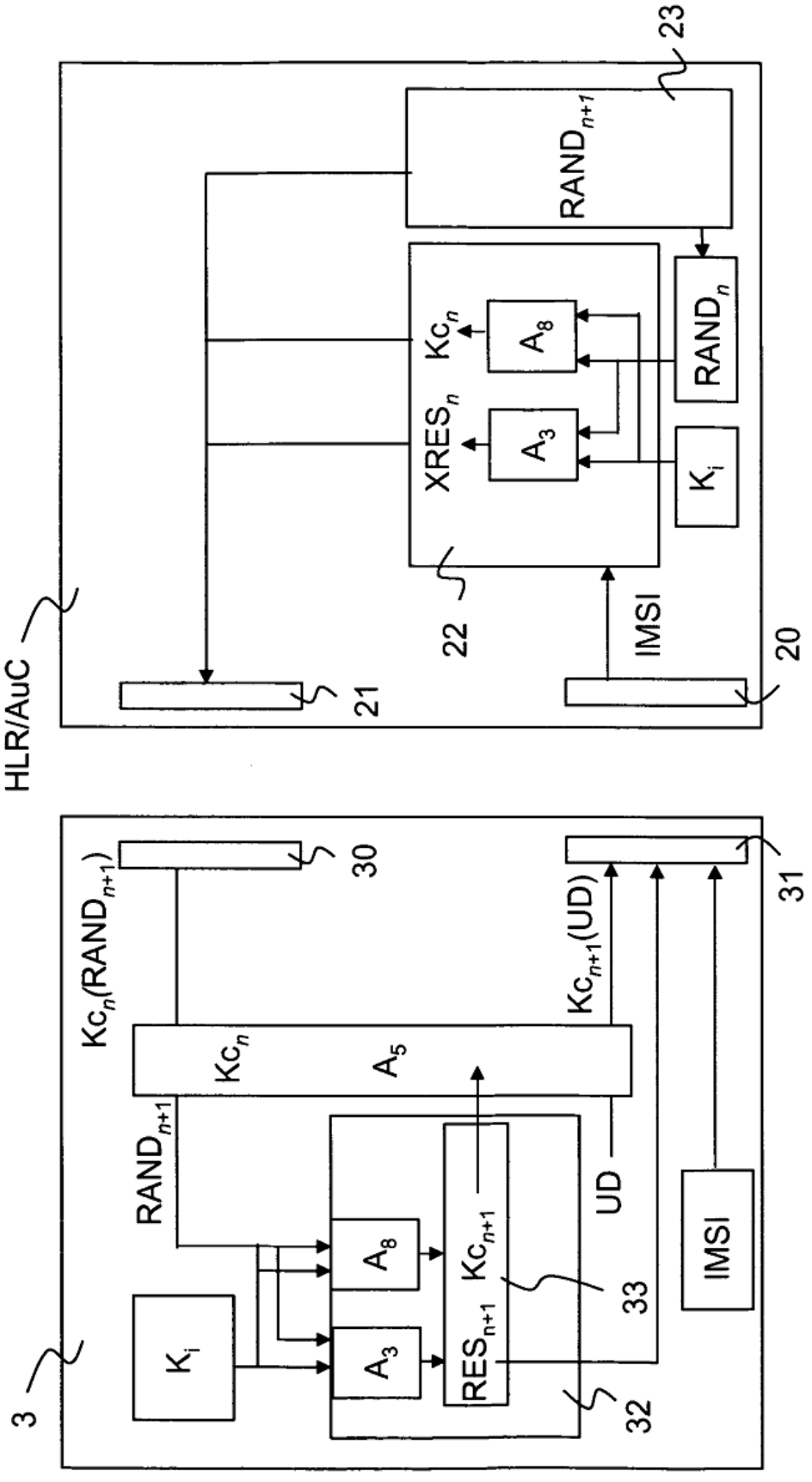
HLR/AuC
23
$RAND_{n+1}$
$RAND_n$
Kc_n
A_8
$XRES_n$
A_3
K_i
22
IMSI
20
21
3
$Kc_n(RAND_{n+1})$
30
31
$Kc_{n+1}(UD)$
Kc_n
A_5
$RAND_{n+1}$
A_8
A_3
K_i
Kc_{n+1}
RES_{n+1}
UD
33
32
IMSI

FIG. 2B

FIG. 2A

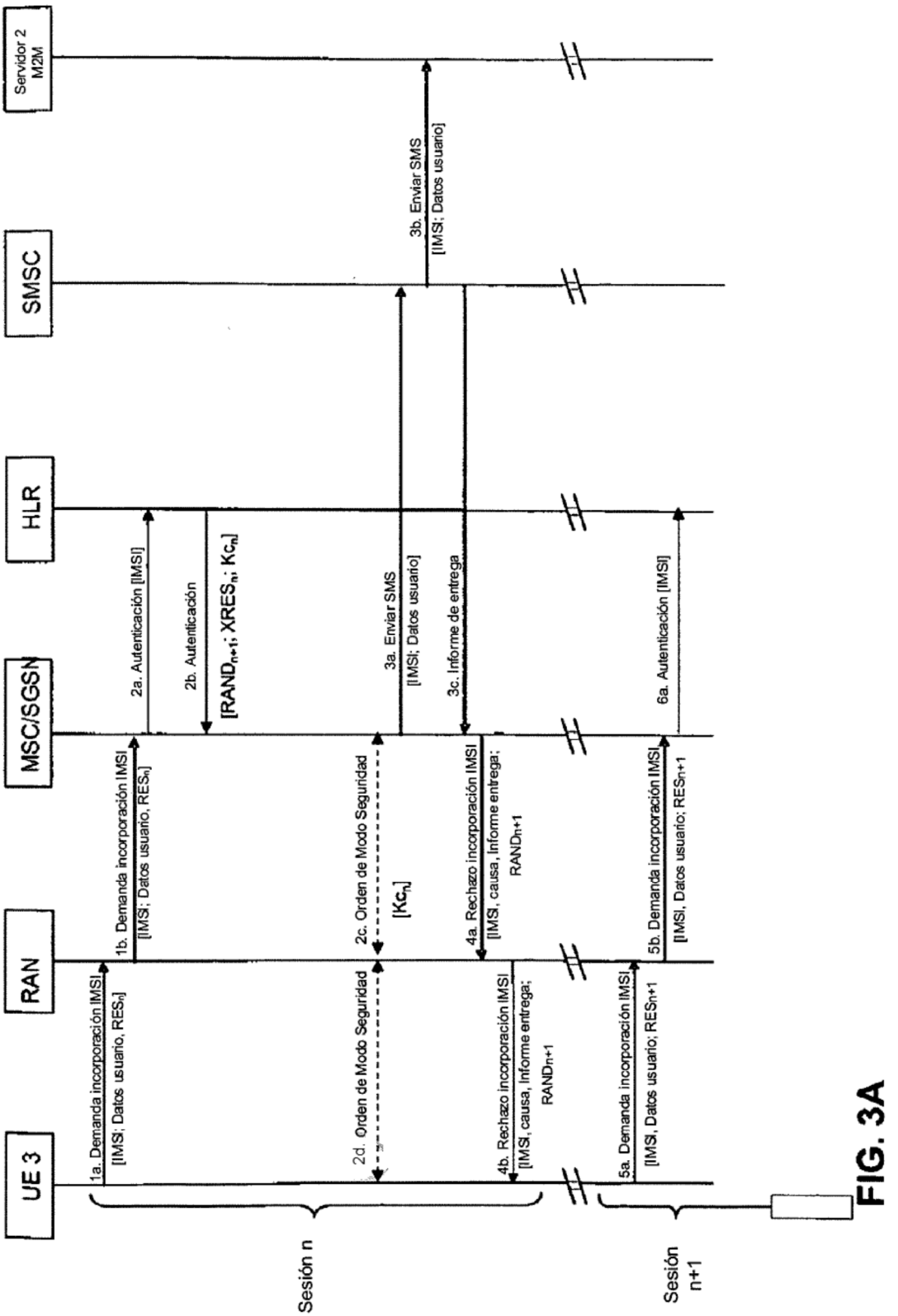
UE 3
RAN
MSC/SGSN
HLR
SMSC
Servidor 2 M2M
1a. Demanda incorporación IMSI [IMSI; Datos usuario, RESn]
1b. Demanda incorporación IMSI [IMSI; Datos usuario, RESn]
2a. Autenticación [IMSI]
2b. Autenticación [RANDn+1; XRESn; Kcn]
2c. Orden de Modo Seguridad [Kcn]
2d. Orden de Modo Seguridad
3a. Enviar SMS [IMSI; Datos usuario]
3b. Enviar SMS [IMSI; Datos usuario]
3c. Informe de entrega
4a. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; RANDn+1
4b. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; RANDn+1
5a. Demanda incorporación IMSI [IMSI, Datos usuario; RESn+1
5b. Demanda incorporación IMSI [IMSI, Datos usuario; RESn+1
6a. Autenticación [IMSI]
Sesión n
Sesión n+1

FIG. 3A

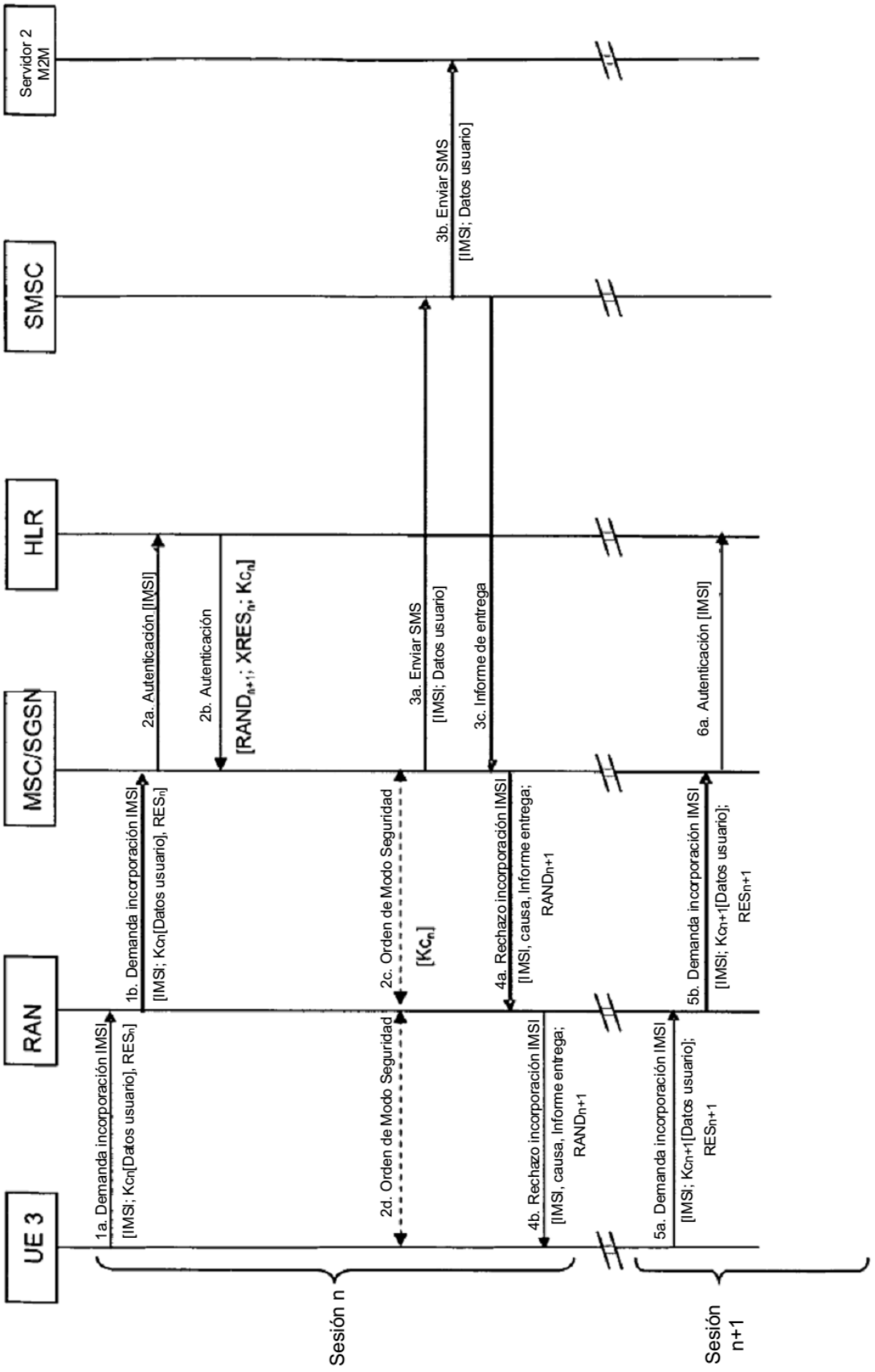
UE 3
RAN
MSC/SGSN
HLR
SMSC
Servidor 2 M2M
1a. Demanda incorporación IMSI [IMSI; Kcn[Datos usuario], RESn]
1b. Demanda incorporación IMSI [IMSI; Kcn[Datos usuario], RESn]
2a. Autenticación [IMSI]
2b. Autenticación [RANDn+1; XRESn; Kcn]
2c. Orden de Modo Seguridad [Kcn]
2d. Orden de Modo Seguridad
3a. Enviar SMS [IMSI; Datos usuario]
3b. Enviar SMS [IMSI; Datos usuario]
3c. Informe de entrega
4a. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; RANDn+1
4b. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; RANDn+1
5a. Demanda incorporación IMSI [IMSI; Kcn+1[Datos usuario]; RESn+1
5b. Demanda incorporación IMSI [IMSI; Kcn+1[Datos usuario]; RESn+1
6a. Autenticación [IMSI]
Sesión n
Sesión n+1

FIG. 3B

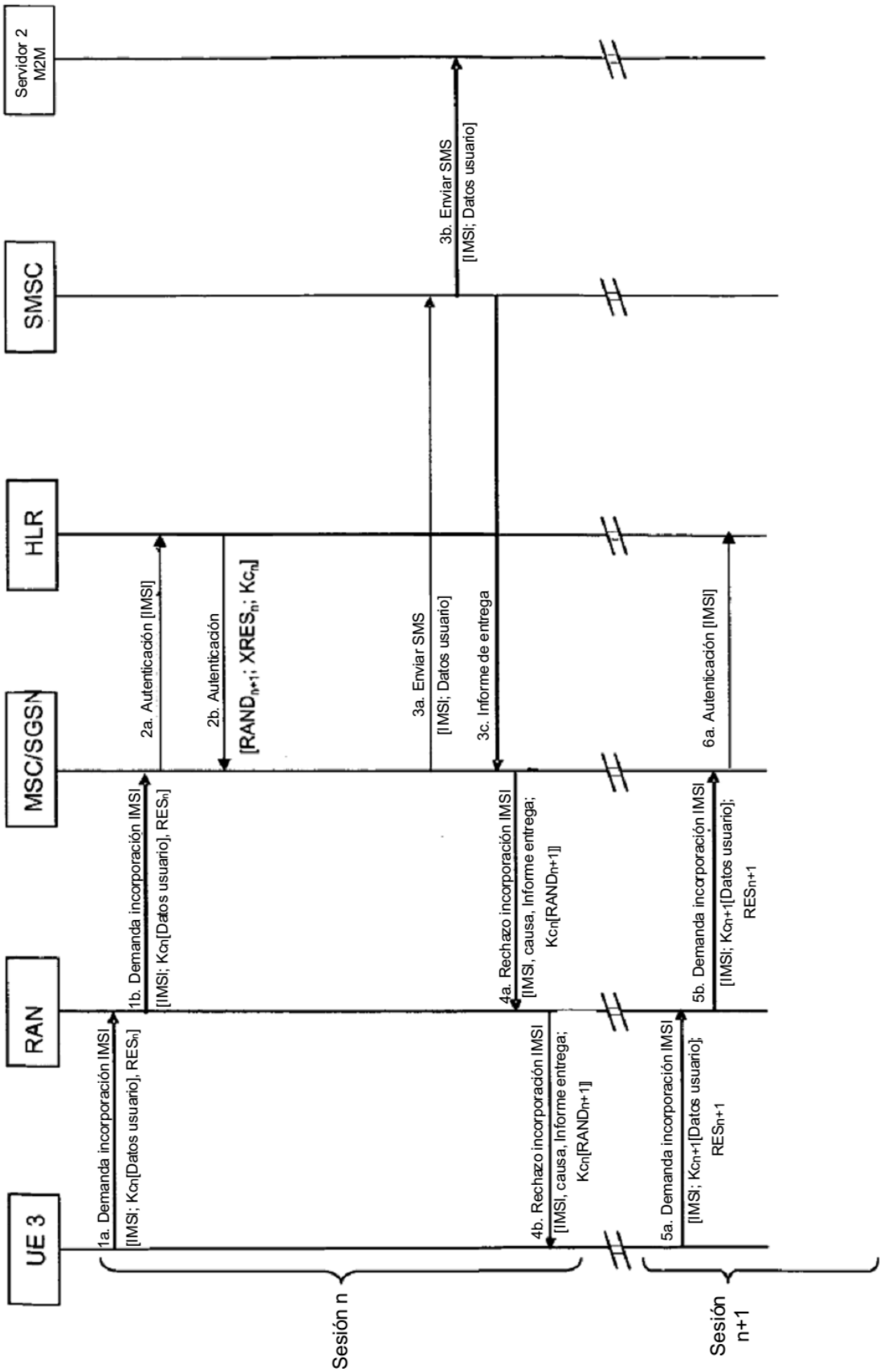
UE 3
RAN
MSC/SGSN
HLR
SMSC
Servidor 2 M2M
1a. Demanda incorporación IMSI
[IMSI; Kcn[Datos usuario], RESn]
1b. Demanda incorporación IMSI
[IMSI; Kcn[Datos usuario], RESn]
2a. Autenticación [IMSI]
2b. Autenticación
[RANDn+1; XRESn; Kcn]
3a. Enviar SMS
[IMSI; Datos usuario]
3b. Enviar SMS
[IMSI; Datos usuario]
3c. Informe de entrega
4a. Rechazo incorporación IMSI
[IMSI, causa, Informe entrega; Kcn[RANDn+1]]
4b. Rechazo incorporación IMSI
[IMSI, causa, Informe entrega; Kcn[RANDn+1]]
5a. Demanda incorporación IMSI
[IMSI; Kcn+1[Datos usuario]; RESn+1
5b. Demanda incorporación IMSI
[IMSI; Kcn+1[Datos usuario]; RESn+1
6a. Autenticación [IMSI]
Sesión n
Sesión n+1

FIG. 3C

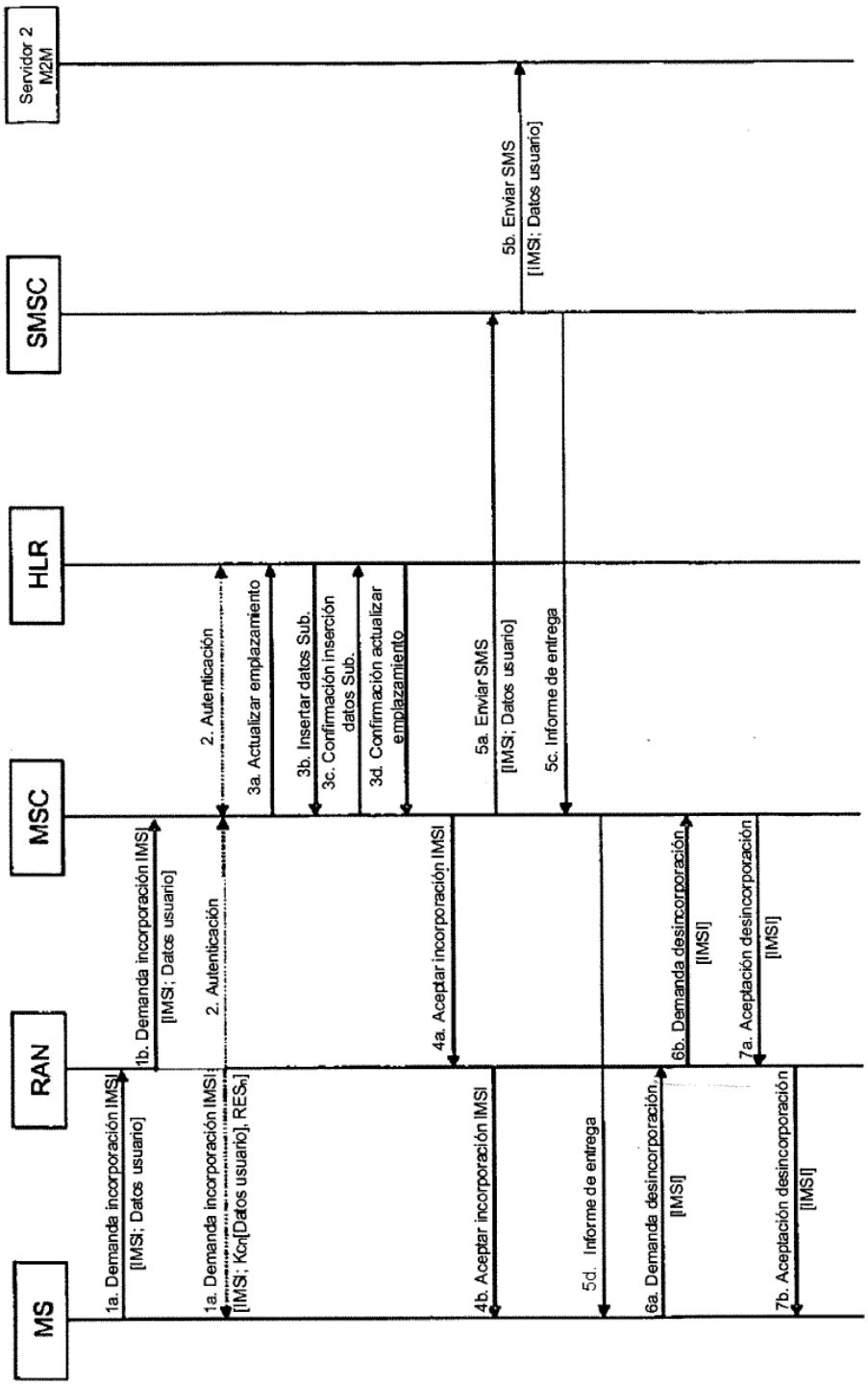
MS
RAN
MSC
HLR
SMSC
Servidor 2 M2M
1a. Demanda incorporación IMSI [IMSI; Datos usuario]
1b. Demanda incorporación IMSI [IMSI; Datos usuario]
2. Autenticación
1a. Demanda incorporación IMSI [IMSI; Kcn[Datos usuario], RESn]
2. Autenticación
3a. Actualizar emplazamiento
3b. Insertar datos Sub.
3c. Confirmación inserción datos Sub.
3d. Confirmación actualizar emplazamiento
4a. Aceptar incorporación IMSI
5a. Enviar SMS [IMSI; Datos usuario]
5b. Enviar SMS [IMSI; Datos usuario]
5c. Informe de entrega
4b. Aceptar incorporación IMSI
5d. Informe de entrega
6a. Demanda desincorporación [IMSI]
6b. Demanda desincorporación [IMSI]
7a. Aceptación desincorporación [IMSI]
7b. Aceptación desincorporación [IMSI]
Sesión n

FIG. 3D

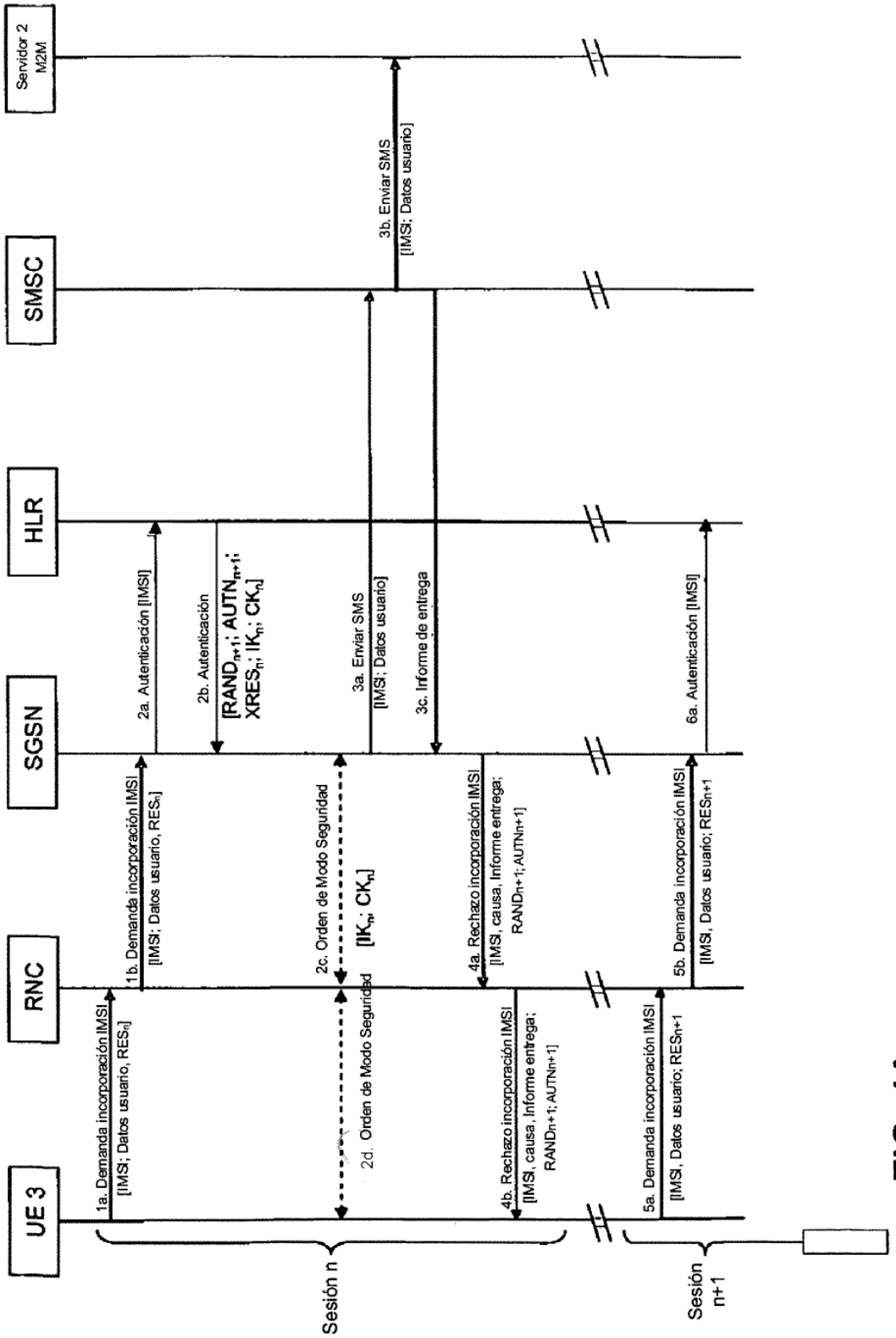
UE 3
RNC
SGSN
HLR
SMSC
Servidor 2 M2M
1a. Demanda incorporación IMSI [IMSI; Datos usuario, RESn]
1b. Demanda incorporación IMSI [IMSI; Datos usuario, RESn]
2a. Autenticación [IMSI]
2b. Autenticación [RANDn+1; AUTNn+1; XRESn; IKn; CKn]
2c. Orden de Modo Seguridad [IKn; CKn]
2d. Orden de Modo Seguridad
3a. Enviar SMS [IMSI; Datos usuario]
3b. Enviar SMS [IMSI; Datos usuario]
3c. Informe de entrega
4a. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; RANDn+1; AUTNn+1]
4b. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; RANDn+1; AUTNn+1]
5a. Demanda incorporación IMSI [IMSI, Datos usuario; RESn+1
5b. Demanda incorporación IMSI [IMSI, Datos usuario; RESn+1
6a. Autenticación [IMSI]
Sesión n
Sesión n+1

FIG. 4A

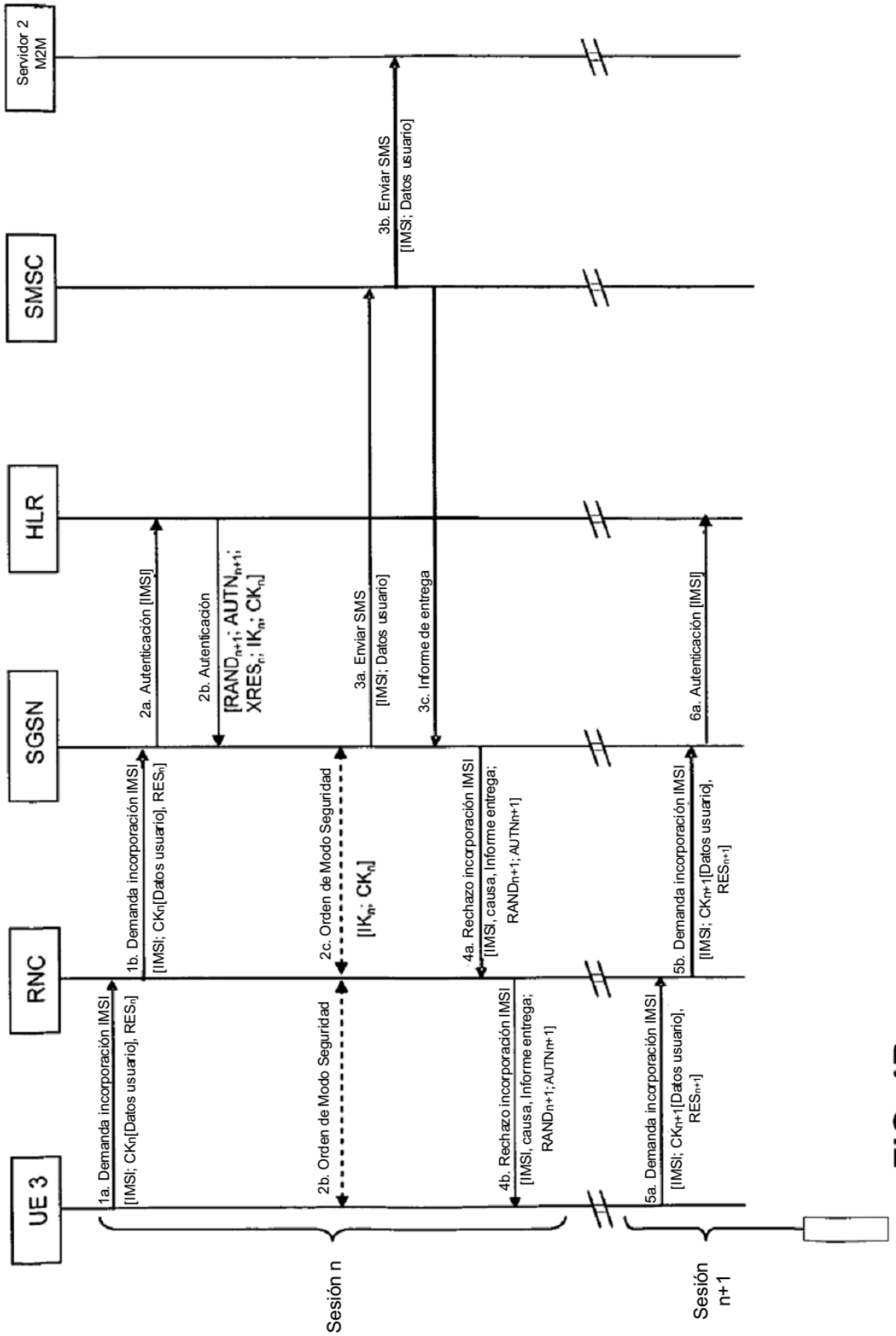
UE 3
RNC
SGSN
HLR
SMSC
Servidor 2 M2M
1a. Demanda incorporación IMSI [IMSI; CKn[Datos usuario], RESn]
1b. Demanda incorporación IMSI [IMSI; CKn[Datos usuario], RESn]
2a. Autenticación [IMSI]
2b. Autenticación [RANDn+1; AUTNn+1; XRESn; IKn; CKn]
2b. Orden de Modo Seguridad
2c. Orden de Modo Seguridad [IKn; CKn]
3a. Enviar SMS [IMSI; Datos usuario]
3b. Enviar SMS [IMSI; Datos usuario]
3c. Informe de entrega
4a. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; RANDn+1; AUTNn+1]
4b. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; RANDn+1; AUTNn+1]
5a. Demanda incorporación IMSI [IMSI; CKn+1[Datos usuario], RESn+1]
5b. Demanda incorporación IMSI [IMSI; CKn+1[Datos usuario], RESn+1]
6a. Autenticación [IMSI]
Sesión n
Sesión n+1

FIG. 4B

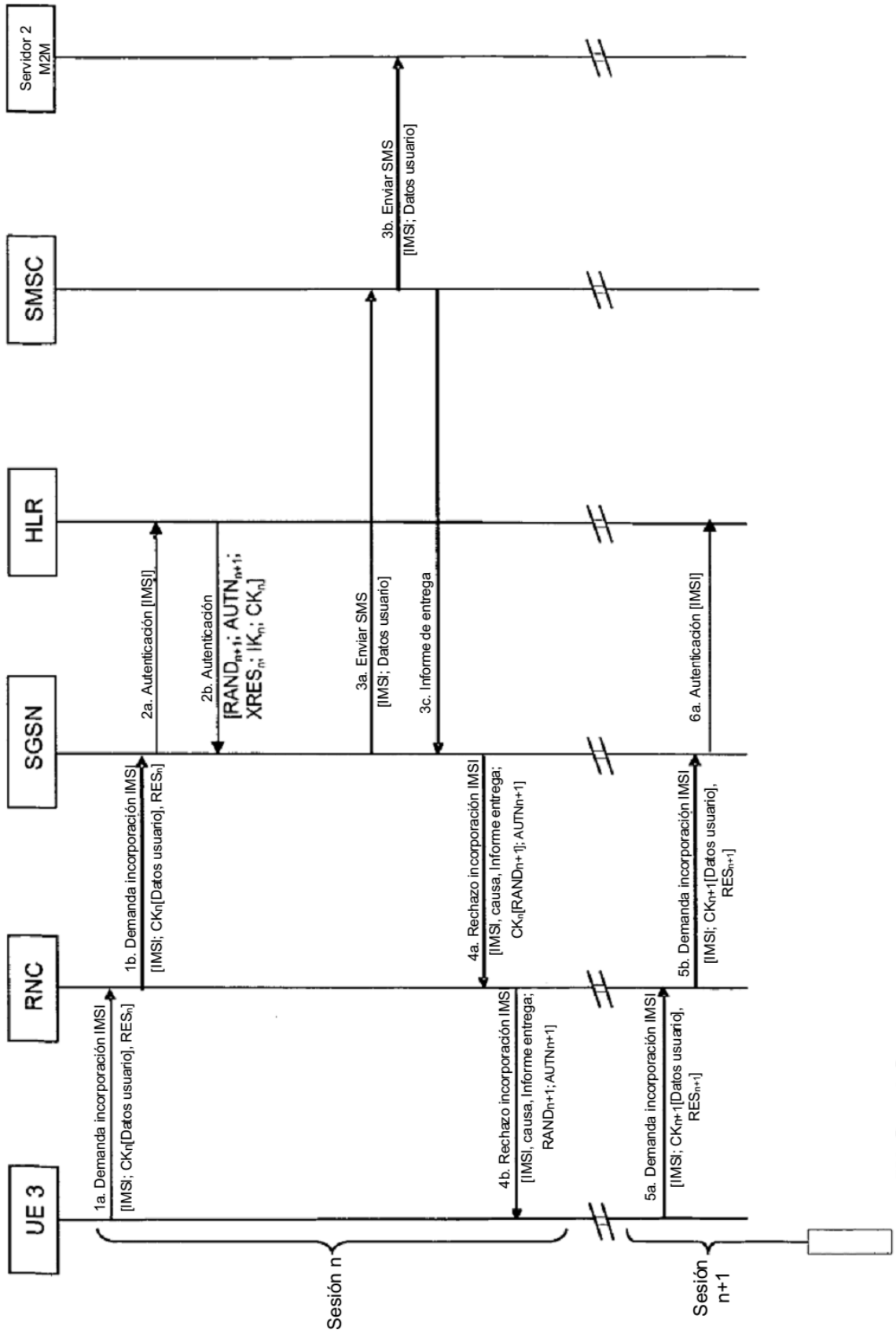
UE 3
RNC
SGSN
HLR
SMSC
Servidor 2 M2M
1a. Demanda incorporación IMSI
[IMSI; CKn[Datos usuario], RESn]
1b. Demanda incorporación IMSI
[IMSI; CKn[Datos usuario], RESn]
2a. Autenticación [IMSI]
2b. Autenticación
[RANDn+1; AUTNn+1; XRESn; IKn; CKn]
3a. Enviar SMS
[IMSI; Datos usuario]
3b. Enviar SMS
[IMSI; Datos usuario]
3c. Informe de entrega
4a. Rechazo incorporación IMSI
[IMSI, causa, Informe entrega; CKn[RANDn+1]; AUTNn+1]
4b. Rechazo incorporación IMSI
[IMSI, causa, Informe entrega; RANDn+1; AUTNn+1]
5a. Demanda incorporación IMSI
[IMSI; CKn+1[Datos usuario], RESn+1]
5b. Demanda incorporación IMSI
[IMSI; CKn+1[Datos usuario], RESn+1]
6a. Autenticación [IMSI]
Sesión n
Sesión n+1

FIG. 4C

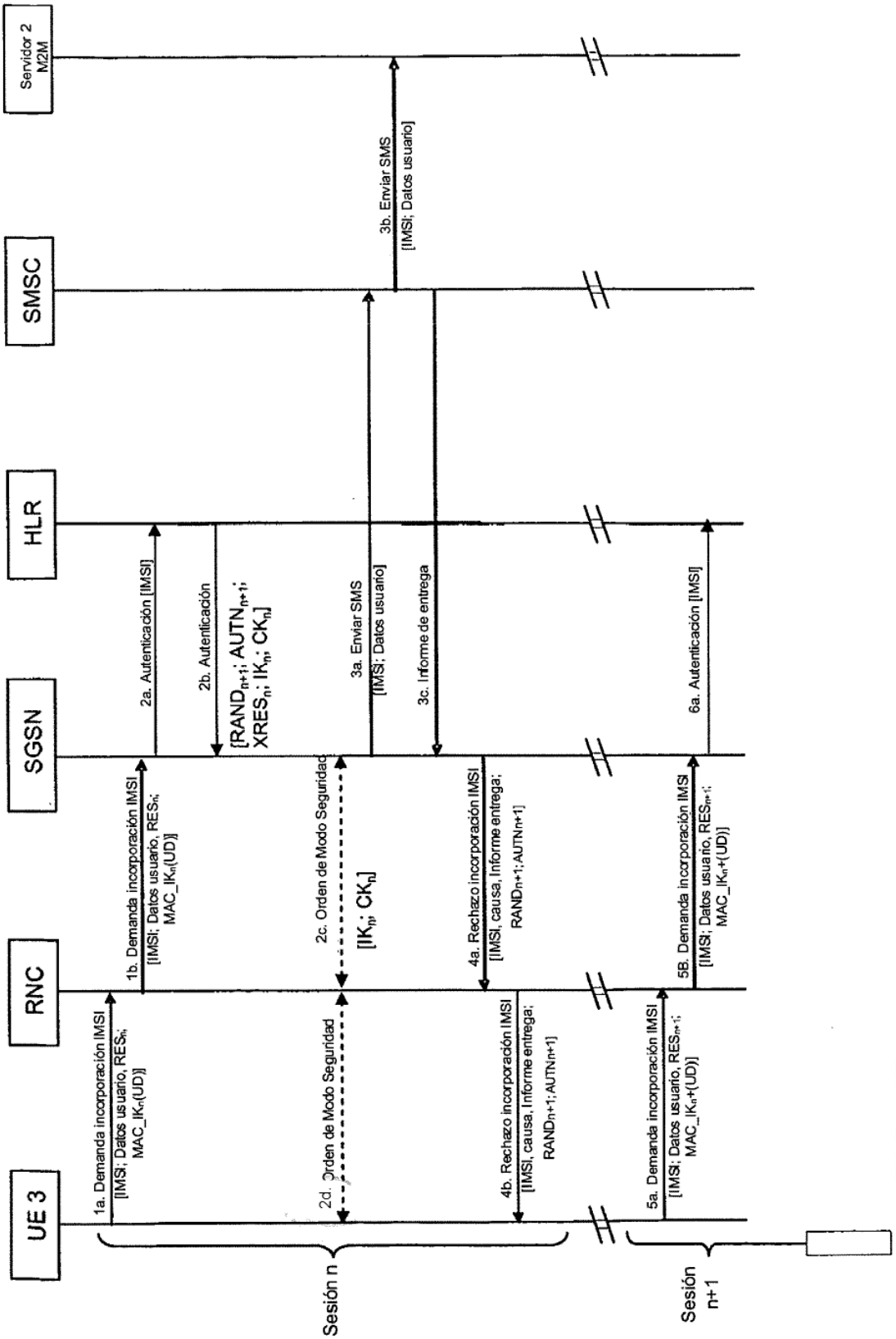
UE 3
RNC
SGSN
HLR
SMSC
Servidor 2 M2M
1a. Demanda incorporación IMSI [IMSI; Datos usuario, RES_n; MAC_IK_n(UD)]
1b. Demanda incorporación IMSI [IMSI; Datos usuario, RES_n; MAC_IK_n(UD)]
2a. Autenticación [IMSI]
2b. Autenticación [RAND_n+1; AUTN_n+1; XRES_n; IK_n; CK_n]
2c. Orden de Modo Seguridad [IK_n; CK_n]
2d. Orden de Modo Seguridad
3a. Enviar SMS [IMSI; Datos usuario]
3b. Enviar SMS [IMSI; Datos usuario]
3c. Informe de entrega
4a. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; RAND_n+1; AUTN_n+1]
4b. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; RAND_n+1; AUTN_n+1]
5a. Demanda incorporación IMSI [IMSI; Datos usuario, RES_n+1; MAC_IK_n+(UD)]
5B. Demanda incorporación IMSI [IMSI; Datos usuario, RES_n+1; MAC_IK_n+(UD)]
6a. Autenticación [IMSI]
Sesión n
Sesión n+1

FIG. 4D

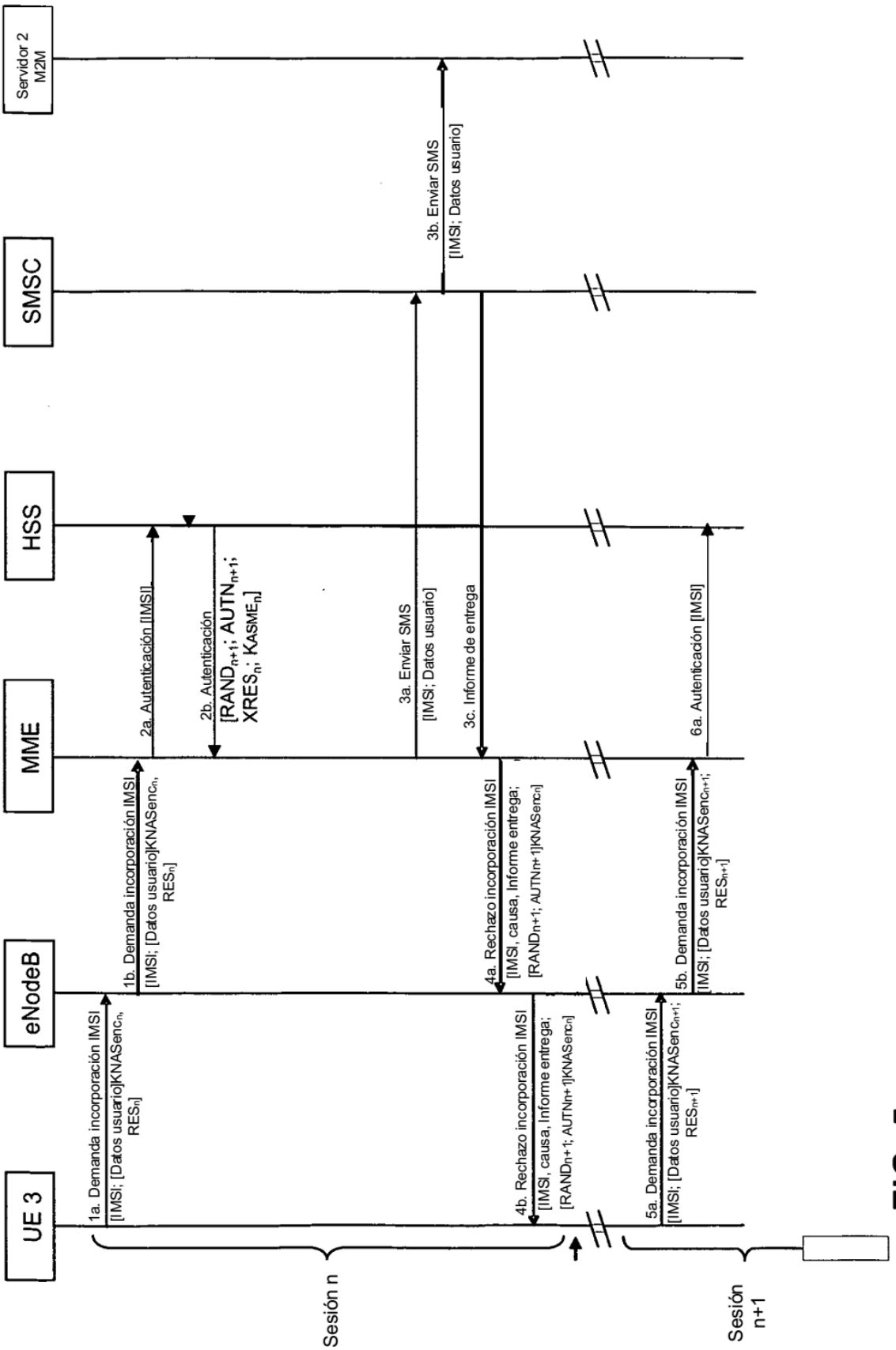
Servidor 2 M2M
SMSC
HSS
MME
eNodeB
UE 3
3b. Enviar SMS [IMSI; Datos usuario]
2a. Autenticación [IMSI]
2b. Autenticación [RAND$_{n+1}$; AUTN$_{n+1}$; XRES$_n$; KASME$_n$]
3a. Enviar SMS [IMSI; Datos usuario]
3c. Informe de entrega
6a. Autenticación [IMSI]
1b. Demanda incorporación IMSI [IMSI; [Datos usuario]KNASenc$_n$, RES$_n$]
4a. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; [RAND$_{n+1}$; AUTN$_{n+1}$]KNASenc$_n$]
5b. Demanda incorporación IMSI [IMSI; [Datos usuario]KNASenc$_{n+1}$; RES$_{n+1}$]
1a. Demanda incorporación IMSI [IMSI; [Datos usuario]KNASenc$_n$, RES$_n$]
4b. Rechazo incorporación IMSI [IMSI, causa, Informe entrega; [RAND$_{n+1}$; AUTN$_{n+1}$]KNASenc$_n$]
5a. Demanda incorporación IMSI [IMSI; [Datos usuario]KNASenc$_{n+1}$; RES$_{n+1}$]
Sesión n
Sesión n+1

FIG. 5

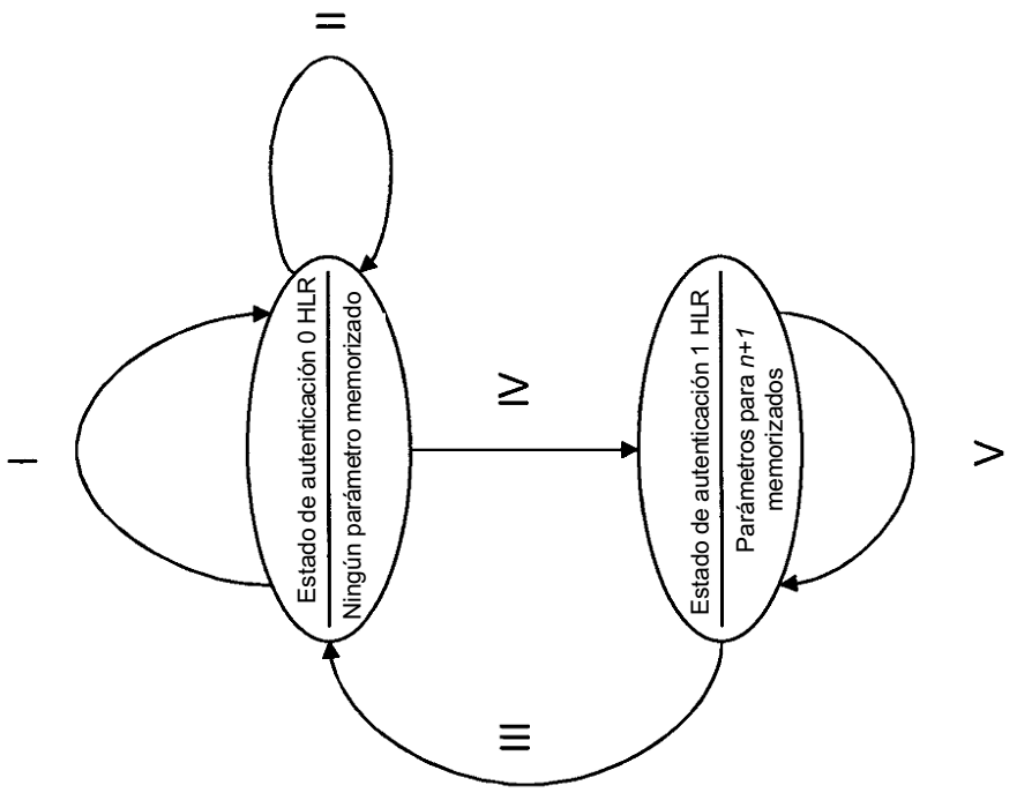
I
II
III
IV
V
Estado de autenticación 0 HLR
Ningún parámetro memorizado
Estado de autenticación 1 HLR
Parámetros para n+1 memorizados

FIG. 6

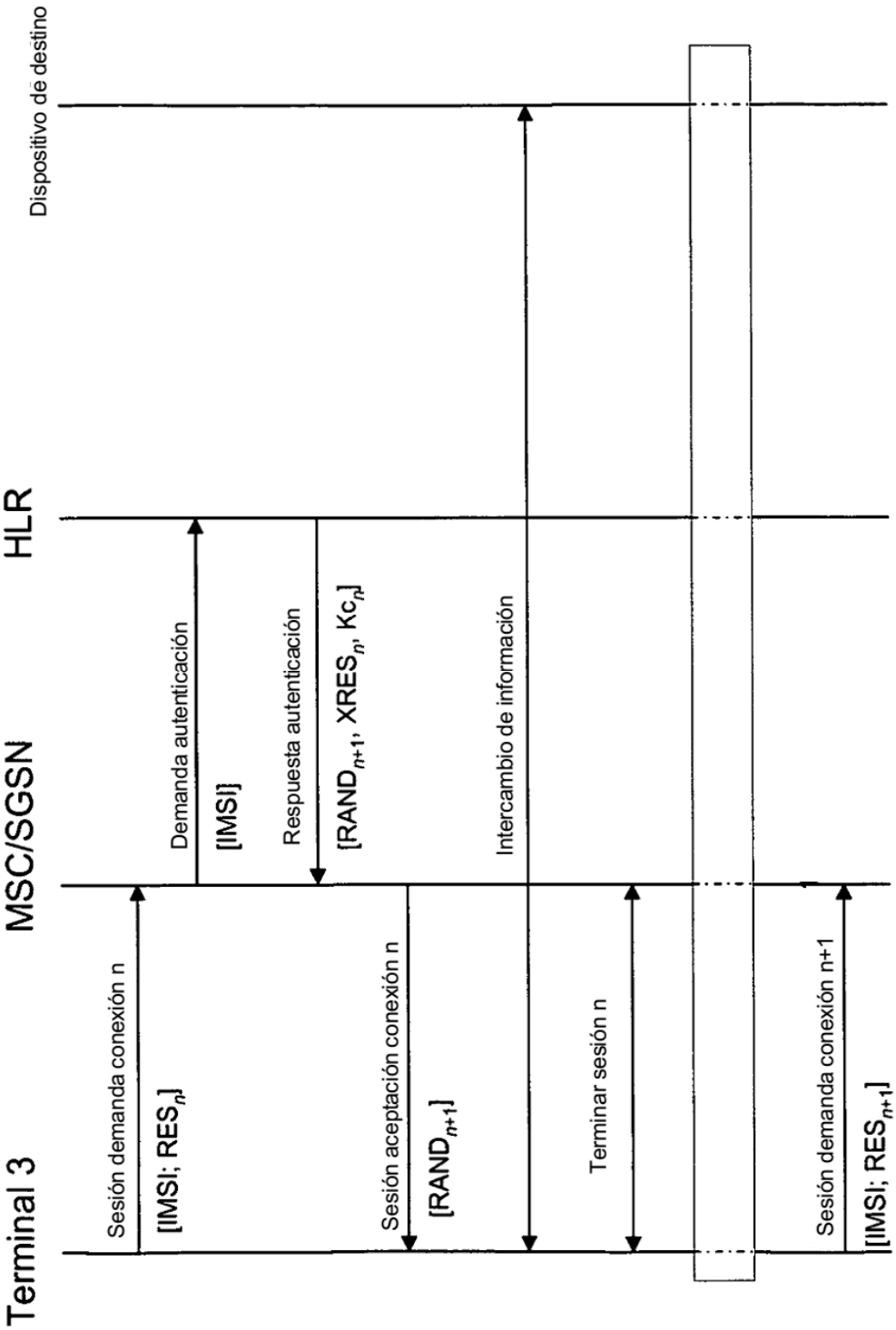
Terminal 3
MSC/SGSN
HLR
Dispositivo de destino
Sesión demanda conexión n
[IMSI; RES$_n$]
Demanda autenticación
[IMSI]
Respuesta autenticación
[RAND$_{n+1}$, XRES$_n$, Kc$_n$]
Intercambio de información
Sesión aceptación conexión n
[RAND$_{n+1}$]
Terminar sesión n
Sesión demanda conexión n+1
[IMSI; RES$_{n+1}$]

FIG. 7