(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 774 921**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.06.2011 PCT/US2011/040777**

(87) Fecha y número de publicación internacional: **22.12.2011 WO11159952**

(96) Fecha de presentación y número de la solicitud europea: **16.06.2011 E 11757437 (6)**

(97) Fecha y número de publicación de la concesión europea: **01.01.2020 EP 2583479**

(54) Título: **Procedimiento y aparato para vincular la autenticación de abonados y la autenticación de dispositivos en sistemas de comunicación**

(30) Prioridad:

15.06.2011 US 201113161336
16.06.2010 US 355423 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.07.2020

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121-1714 , US

(72) Inventor/es:

ESCOTT, ADRIAN EDWARD y
PALANIGOUNDER, ANAND

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Procedimiento y aparato para vincular la autenticación de abonados y la autenticación de dispositivos en sistemas de comunicación

Reivindicación de prioridad en virtud de 35 U.S.C. apartado 119

[0001] La presente solicitud de patente reivindica la prioridad de la solicitud provisional estadounidense n.º 61/355.423 titulada "Apparatus and Method for Device Authentication in 3GPP Systems [Aparato y procedimiento para la autenticación de dispositivos en sistemas 3GPP]", presentada el 16 de junio de 2010.

ANTECEDENTES

Campo

[0002] Diversas características se refieren a los sistemas de comunicaciones y, más en particular, a la autenticación de dispositivos, tales como nodos de retransmisión y dispositivos de máquina a máquina, empleados en un sistema de comunicaciones alámbricas o inalámbricas.

Antecedentes

[0003] Las redes inalámbricas modernas pueden incluir nodos de retransmisión y/o terminales de acceso, denominados conjuntamente en el presente documento dispositivos. Para que dicho dispositivo funcione correctamente, el dispositivo a menudo se dota/configura con credenciales de seguridad operativas y de abonado antes de que el dispositivo se ponga en funcionamiento. Dichas credenciales de seguridad de abonado se pueden usar para, por ejemplo, autenticar el dispositivo antes de proporcionar servicio o acceso inalámbrico y, en algunos casos, pueden almacenarse en un módulo que se acopla de manera inamovible a su dispositivo anfitrión. Existe el riesgo de que las credenciales de seguridad de abonado puedan eliminarse de un dispositivo autenticado e introducirse en un dispositivo no autorizado. En el caso de un nodo de retransmisión, esto puede permitir que un nodo de retransmisión no autorizado acceda subrepticiamente a las transmisiones, por ejemplo, entre un nodo de acceso y uno o más terminales de acceso y/u obtenga acceso libre a servicios de red. Este riesgo o vulnerabilidad también existe en el caso de dispositivos de máquina a máquina (M2M) en donde las credenciales de abonado válidas (por ejemplo, parámetros de acuerdo de autenticación de claves (AKA) en una tarjeta de circuito integrado universal (UICC) extraíble) en un dispositivo M2M podrían transferirse a otro dispositivo para obtener acceso gratuito a la red. Existe una vulnerabilidad relacionada en el sentido de que no es necesario tener acceso físico al propio dispositivo M2M. El acceso a los datos (por ejemplo, las claves de seguridad resultantes de la autenticación) que se realiza en una interfaz de dispositivo M2M (por ejemplo, de dispositivo anfitrión a interfaz de UICC) es suficiente para obtener acceso a las claves de seguridad y exponer los datos protegidos por dichas claves.

[0004] Existe un problema similar si un operador desea controlar qué dispositivos pueden acceder a su red.

[0005] En consecuencia, existe la necesidad de proporcionar seguridad adicional para que los dispositivos aborden estas y otras vulnerabilidades y riesgos.

[0006] También se hace referencia al documento WO 2007/121 190 A2, en el que se describen técnicas para vincular múltiples autenticaciones para un igual. En un diseño, se pueden vincular múltiples autenticaciones para el igual en base a un identificador único para el igual. El igual puede realizar una primera autenticación con un primer servidor de autenticación y obtener una primera clave criptográfica y también puede realizar una segunda autenticación con el primer servidor de autenticación o un segundo servidor de autenticación y obtener una segunda clave criptográfica. El igual puede, a continuación, intercambiar datos de forma segura usando las dos claves que usan seguridad anidada.

[0007] El documento 3GPP: "3rd Generation Partnership Project; Technical Specification Group Service and Systems Aspects: Security of H(e)NB; Release 8", describe las amenazas especiales de seguridad de H(e)NB y las contramedidas a estas amenazas. El estudio incluye análisis de amenazas de H(e)NB, autenticación mutua y protección de seguridad entre H(e)NB y el resto de la red, mantenimiento del contexto de seguridad entre H(e)NB y el resto de la red, requisitos de seguridad en el H(e)NB, dotación de credenciales de seguridad en el H(e)NB, solución de seguridad para verificar la ubicación del H(e)NB, etc.

[0008] El documento EP 1 739 903 A1 describe un procedimiento y sistema de autenticación en un sistema de comunicación. Una MS, una BS y un servidor AAA adquieren una primera MSK mediante una primera autenticación de EAP para la MS en un esquema EAP-en-EAP. Después de la primera autenticación de EAP, adquieren una segunda MSK mediante una segunda autenticación de EAP para la MS en el esquema EAP-en-EAP.

SUMARIO

[0009] De acuerdo con la presente invención, se proporciona un procedimiento como se expone en la reivindicación 1, un aparato como se expone en la reivindicación 8, un procedimiento como se expone en la reivindicación 10, un aparato como se expone en la reivindicación 14 y un medio legible por procesador como se expone en la reivindicación 15. Otros modos de realización de la invención se reivindican en las reivindicaciones dependientes.

[0010] Se proporcionan un procedimiento y un aparato para dotar de seguridad a un dispositivo vinculando la autenticación de abonado y la autenticación de dispositivo para generar una clave de seguridad.

[0011] De acuerdo con un primer aspecto, se proporciona un procedimiento operativo en un dispositivo que vincula la autenticación de dispositivo y de abonado. El dispositivo puede comenzar enviando una solicitud de conexión a la entidad de red, incluyendo la solicitud de conexión una indicación de las capacidades de autenticación de dispositivo del dispositivo. La autenticación de abonado puede ser realizada por el dispositivo con una entidad de red. Por ejemplo, la autenticación de abonado puede basarse en un intercambio de acuerdo de autenticación de claves entre el dispositivo y la entidad de red. El dispositivo también puede realizar la autenticación de dispositivo con la entidad de red. Por ejemplo, la autenticación de dispositivo puede basarse en un intercambio pregunta-respuesta entre el dispositivo y la entidad de red.

[0012] A continuación, se puede generar una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo. La clave de seguridad puede generarse en función de al menos una primera clave obtenida de la autenticación de abonado y una segunda clave obtenida de la autenticación de dispositivo. Además, la clave de seguridad también puede depender de un nonce de red y un nonce de dispositivo. La clave de seguridad se puede usar después para dotar de seguridad a las comunicaciones entre el dispositivo y una red de servicio. Cabe destacar que la clave de seguridad puede ser generada por separado por el dispositivo y la entidad de red, por lo que no se transmite de manera inalámbrica.

[0013] De acuerdo con una implementación, la autenticación de abonado se puede realizar por un primer servidor de autenticación que es parte de la entidad de red, mientras que la autenticación de dispositivo se puede realizar por un segundo servidor de autenticación que es parte de la entidad de red.

[0014] En un ejemplo, la autenticación de dispositivo se puede realizar usando una clave secreta compartida para cifrar/descifrar determinados intercambios entre el dispositivo y la entidad de red. En otro ejemplo, la autenticación de dispositivo se puede realizar: (a) recibiendo datos desde de la entidad de red que está cifrada con una clave pública del dispositivo; (b) usando una clave privada correspondiente para descifrar los datos cifrados; y/o (c) posteriormente demostrando a la entidad de red que el dispositivo tiene conocimiento de los datos.

[0015] De acuerdo con un aspecto, puede dotarse de seguridad a la autenticación de dispositivo mediante al menos una clave generada durante la autenticación de abonado.

[0016] En diversas implementaciones, la autenticación de abonado y la autenticación de dispositivo se pueden realizar simultáneamente en intercambios de mensajes combinados, o la autenticación de abonado se puede realizar en un intercambio de seguridad anterior y separado de la autenticación de dispositivo.

[0017] De acuerdo con una característica, una clave específica de abonado puede proporcionarse en el dispositivo como parte de un acuerdo de servicio, donde la clave específica de abonado se usa para la autenticación de abonado. De manera similar, una clave específica de dispositivo puede proporcionarse en el dispositivo durante la fabricación, donde la clave específica de dispositivo se usa para la autenticación de dispositivo.

[0018] En una implementación, el dispositivo puede ser un nodo de retransmisión que aparece como un terminal de acceso para la entidad de red y aparece como un dispositivo de red para uno o más terminales de acceso. En otra implementación, el dispositivo puede ser un terminal de acceso.

[0019] De acuerdo con un ejemplo, el dispositivo puede incluir una interfaz de comunicación acoplada a un circuito de procesamiento. El circuito de procesamiento se puede adaptar para: (a) realizar la autenticación de abonado con una entidad de red; (b) realizar la autenticación de dispositivo del dispositivo con la entidad de red; (c) generar una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo; y/o (d) usar la clave de seguridad para dotar de seguridad a las comunicaciones entre el dispositivo y una red de servicio.

[0020] De acuerdo con aún otro ejemplo, se puede proporcionar un medio legible por procesador que comprende instrucciones operativas en un dispositivo. Cuando son ejecutadas por un procesador, estas instrucciones pueden hacer que el procesador: (a) realice la autenticación de abonado con una entidad de red; (b) realice la autenticación de dispositivo del dispositivo con la entidad de red; (c) genere una clave de seguridad que vincule la autenticación de abonado y la autenticación de dispositivo; y/o (d) use la clave de seguridad para dotar de seguridad a las comunicaciones entre el dispositivo y una red de servicio.

[0021] De acuerdo con otro aspecto, se proporciona un procedimiento operativo en una entidad de red. La entidad de red puede recibir una solicitud de conexión desde el dispositivo, incluyendo la solicitud de conexión una indicación

de las capacidades de autenticación de dispositivo del dispositivo. La entidad de red puede realizar la autenticación de abonado con un dispositivo. Del mismo modo, la entidad de red puede realizar la autenticación de dispositivo del dispositivo. A continuación, se puede generar una clave de seguridad por la entidad de red que vincula la autenticación de abonado y la autenticación de dispositivo. La clave de seguridad se puede usar entonces para dotar de seguridad a las comunicaciones entre la entidad de red y el dispositivo. Cabe destacar que, para evitar la transmisión inalámbrica de la clave de seguridad, la clave de seguridad puede ser generada por separado por el dispositivo y la entidad de red.

[0022] En un ejemplo, la autenticación de abonado puede basarse en un intercambio de acuerdo de autenticación de claves entre la entidad de red y el dispositivo. La autenticación de dispositivo puede basarse en un intercambio de pregunta-respuesta entre la entidad de red y el dispositivo.

[0023] En una implementación, la autenticación de dispositivo puede incluir: (a) recibir un certificado desde el dispositivo; y (b) verificar que el certificado asociado al dispositivo no ha sido revocado.

[0024] En una implementación, para evitar espionaje durante el proceso de autenticación de dispositivo, puede dotarse de seguridad a la autenticación de dispositivo mediante al menos una clave generada durante una autenticación de abonado anterior.

[0025] De acuerdo con diversos ejemplos, la autenticación de abonado y la autenticación de dispositivo pueden realizarse simultáneamente en intercambios de mensajes combinados, o la autenticación se realiza en un intercambio de seguridad anterior y separado de la autenticación de dispositivo.

[0026] En otro ejemplo, la clave de seguridad puede generarse en función de al menos una primera clave obtenida de la autenticación de abonado y una segunda clave obtenida de la autenticación de dispositivo.

[0027] En una implementación, la entidad de red puede obtener una clave específica de abonado como parte de un acuerdo de servicio, donde la clave específica de abonado se usa para la autenticación de abonado. De manera similar, la entidad de red puede obtener una clave específica de dispositivo para el dispositivo, donde la clave específica de dispositivo se usa para la autenticación de dispositivo.

[0028] En una implementación, la entidad de red puede comprender una interfaz de comunicaciones acoplada a un circuito de procesamiento. El circuito de procesamiento se puede adaptar para: (a) realizar la autenticación de abonado con un dispositivo; (b) realizar la autenticación de dispositivo del dispositivo; (c) generar una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo; y/o (d) usar la clave de seguridad para dotar de seguridad a las comunicaciones entre la entidad de red y el dispositivo.

[0029] En una implementación, se proporciona un medio legible por procesador que comprende instrucciones operativas en una entidad de red. Cuando son ejecutadas por un procesador, estas instrucciones pueden hacer que el procesador: (a) realice la autenticación de abonado con un dispositivo; (b) realice la autenticación de dispositivo del dispositivo; (c) genere una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo; y/o (d) use la clave de seguridad para dotar de seguridad a las comunicaciones entre la entidad de red y el dispositivo.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0030]

La FIG. 1 es un diagrama de bloques que ilustra un sistema de comunicación inalámbrica en el que una red central puede autenticar diversos tipos de dispositivos inalámbricos para obtener servicio.

La FIG. 2 ilustra un enfoque general para vincular una autenticación de dispositivo y una autenticación de abonado.

La FIG. 3 (que comprende la FIG. 3A y la FIG. 3B) ilustra un ejemplo de cómo se puede modificar una jerarquía de claves basada en la autenticación de abonado para añadir la autenticación de dispositivo.

La FIG. 4 ilustra una pila de protocolos ejemplar que puede implementarse en un dispositivo que funciona en una red de conmutación de paquetes.

La FIG. 5 es un diagrama de bloques que ilustra un sistema de red en el que pueden generarse las diversas claves de autenticación y/o seguridad ilustradas en las FIGS. 3 y 4.

La FIG. 6 es un diagrama de bloques que ilustra componentes seleccionados de un dispositivo inalámbrico que pueden adaptarse para vincular la autenticación de abonado y la autenticación de dispositivo.

La FIG. 7 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en un dispositivo inalámbrico para generar una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo.

La FIG. 8 es un diagrama de bloques que ilustra componentes seleccionados de una entidad de red que pueden adaptarse para vincular la autenticación de abonado y la autenticación de dispositivo.

La FIG. 9 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una entidad de red para generar una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo.

La FIG. 10 ilustra un primer procedimiento ejemplar para generar una clave de seguridad mediante la vinculación de la autenticación de abonado y de dispositivo.

La FIG. 11 ilustra un segundo procedimiento ejemplar para generar una clave de seguridad mediante la vinculación de la autenticación de abonado y de dispositivo.

La FIG. 12 ilustra un tercer procedimiento ejemplar para generar una clave de seguridad mediante la vinculación de la autenticación de abonado y de dispositivo.

DESCRIPCIÓN DETALLADA

[0031] En la siguiente descripción, se dan detalles específicos para proporcionar un entendimiento exhaustivo de las implementaciones descritas. Sin embargo, un experto en la técnica entenderá que pueden llevarse a la práctica diversas implementaciones sin estos detalles específicos. Por ejemplo, pueden mostrarse circuitos en diagramas de bloques para no complicar las implementaciones con detalles innecesarios. En otros casos, pueden mostrarse en detalle circuitos, estructuras y técnicas bien conocidos para no complicar las implementaciones descritas.

[0032] El término "ejemplar" se usa en el presente documento en el sentido de "que sirve de ejemplo, caso o ilustración". Cualquier implementación o modo de realización descrito en el presente documento como "ejemplar" no debe considerarse necesariamente preferente o ventajoso con respecto a otros modos de realización o implementaciones. Asimismo, el término "modos de realización" no requiere que todos los modos de realización incluyan la característica, ventaja o modo de funcionamiento analizados.

Visión general

[0033] Se proporciona un procedimiento de autenticación entre un dispositivo (por ejemplo, un dispositivo cliente o terminal de acceso) y una entidad de red. Un dispositivo de almacenamiento extraíble se puede acoplar al dispositivo, que almacena una clave específica de abonado que se puede usar para la autenticación de abonado. Un dispositivo de almacenamiento seguro se puede acoplar al dispositivo, que almacena una clave específica de dispositivo usada para la autenticación de dispositivo. La autenticación de abonado se puede realizar entre el dispositivo y una entidad de red. La autenticación de dispositivo también se puede realizar del dispositivo con la entidad de red. A continuación, se puede generar una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo. Es decir, una clave, datos y/o información del proceso de autenticación de abonado y una clave, datos y/o información del proceso de autenticación de dispositivo pueden combinarse para generar la clave de seguridad (compuesta). La clave de seguridad se puede usar para dotar de seguridad a las comunicaciones entre el dispositivo y una red de servicio.

Entorno de red ejemplar

[0034] La FIG. 1 es un diagrama de bloques que ilustra un sistema de comunicación inalámbrica en el que una red central puede autenticar diversos tipos de dispositivos inalámbricos para obtener servicio. Este sistema de comunicación inalámbrica puede ser, por ejemplo, una red compatible con o que se ajusta al Sistema Universal de Telecomunicaciones Móviles (UMTS) o una red compatible con el Sistema Global para Comunicaciones Móviles (GSM) o una red compatible con el Sistema Global para Comunicaciones Móviles (GSM). Si bien algunos de los ejemplos descritos en el presente documento pueden pertenecer a una red de evolución a largo plazo (LTE), las diversas características descritas en el presente documento también pueden implementarse en otras redes.

[0035] El sistema puede incluir uno o más dispositivos 101, tales como terminales de acceso 103/104 y un nodo de retransmisión 102, que se comunican con un nodo de acceso 106. El nodo de retransmisión 102 puede facilitar las transmisiones inalámbricas entre una red de comunicación inalámbrica 106/108 y uno o más terminales de acceso 104. El sistema de comunicaciones inalámbricas (por ejemplo, una red de evolución a largo plazo (LTE), una red LTE-avanzada, etc.) puede comprender una red central 108 y uno o más nodos de acceso 106. El nodo de acceso 106 se puede acoplar a la red central 108 a través de un enlace de retorno (por ejemplo, una conexión por cable). La red central 108 puede incluir, por ejemplo, una entidad de gestión de movilidad (MME) 110, un servidor de abonado propio (HSS) 112 y/u otros componentes.

[0036] En un ejemplo, una entidad de gestión de movilidad (MME) 110 puede participar en la activación/desactivación de portadoras para el dispositivo 101, el nodo de retransmisión 102 y/o los terminales de acceso 103/104 (en lo sucesivo, denominado genéricamente "dispositivo") y ayudar con la autenticación interactuando

con el servidor de abonado propio (HSS) 112. La MME 110 también puede generar y/o asignar identidades temporales a los dispositivos (por ejemplo, dispositivo 101, nodo de retransmisión 102, terminales de acceso 103/104, etc.). Puede verificar la autorización del dispositivo para establecerse en (por ejemplo, obtener servicio de, conectarse a, configurar un enlace de comunicación con) la red móvil pública terrestre (PLMN) de un proveedor de servicios y puede hacer cumplir las restricciones de itinerancia del dispositivo. La MME 110 puede ser el punto de terminación en la red para el cifrado/protección de integridad para la señalización de estrato de no acceso (NAS) y se encarga de la gestión de claves de seguridad. La MME 110 también puede realizar procedimientos de seguimiento y/o radiolocalización (incluidas retransmisiones) para los dispositivos acoplados a la red central 108.

[0037] El servidor de abonado propio (HSS) 112 es una base de datos maestra de abonados que admite las entidades de red que realmente gestionan dispositivos. Puede contener información relacionada con la suscripción (perfiles de abonado), ayudar a realizar la autenticación y autorización de la suscripción y puede proporcionar información sobre la ubicación del abonado. Es similar al registro de posiciones propio GSM (HLR) y al centro de autenticación (AuC). El registro de posiciones propio (HLR) puede ser una base de datos que contiene detalles de cada abonado que está autorizado para usar la red central. El HLR puede ayudar al AuC a autenticar a los abonados (es decir, que usan los terminales de usuario).

[0038] El nodo de retransmisión 102 puede estar adaptado para amplificar y/o repetir una señal entre el terminal de acceso 104 y el nodo de acceso 106. En general, el nodo de retransmisión 102 puede parecer para el terminal de acceso 104 un nodo de acceso (AN) y puede parecer para el nodo de acceso 106 un terminal de acceso (AT). Por ejemplo, el nodo de retransmisión 102 puede incluir una interfaz de terminal de acceso 105 con la que se comunica con el nodo de acceso 106 y también puede incluir una interfaz de nodo de acceso 107 con la que se comunica con el terminal de acceso 104. Es decir, la interfaz de terminal de acceso 105 puede hacer que el nodo de retransmisión parezca un terminal de acceso para el nodo de acceso 106. De manera similar, la interfaz de nodo de acceso 107 puede hacer que el nodo de retransmisión 102 parezca un nodo de acceso para el terminal de acceso 104. En algunas implementaciones, el nodo de retransmisión 102 puede convertir señales de un primer formato a un segundo formato entre la interfaz de terminal de acceso 105 y la interfaz de nodo de acceso 107. El nodo de retransmisión 102 puede situarse cerca de los bordes de una célula de manera que el terminal de acceso 104 pueda comunicarse con el nodo de retransmisión 102 en lugar de comunicarse directamente con el nodo de acceso 106.

[0039] En sistemas de radio, una célula es un área geográfica de cobertura de recepción y transmisión. Las células pueden solaparse entre sí. En el ejemplo típico, hay un nodo de acceso asociado a cada célula. El tamaño de una célula se determina por factores tales como la banda de frecuencia, el nivel de potencia y las condiciones de canal. Pueden usarse nodos de retransmisión, tales como el nodo de retransmisión 102, para mejorar la cobertura dentro o cerca de una célula, o para ampliar el tamaño de cobertura de una célula. Adicionalmente, el uso de un nodo de retransmisión 102 puede mejorar el rendimiento de una señal dentro de una célula porque el terminal de acceso 104 puede acceder al nodo de retransmisión 102 a una mayor velocidad de transferencia de datos o una potencia de transmisión inferior que la que el terminal de acceso 104 puede usar al comunicarse directamente con el nodo de acceso 106 para esa célula. La transmisión a una mayor velocidad de transferencia de datos crea una mayor eficiencia del espectro, y una potencia inferior beneficia al terminal de acceso 104 al consumir menos potencia de la batería, por ejemplo.

[0040] En algunos ejemplos, un nodo de retransmisión 102 puede implementarse como uno de tres tipos de retransmisor: un nodo de retransmisión monocapa, un nodo de retransmisión bicapa y/o un nodo de retransmisión tricapa. Un nodo de retransmisión monocapa es básicamente un repetidor que puede retransmitir una transmisión sin ninguna modificación distinta de la amplificación y un ligero retardo. Un nodo de retransmisión bicapa puede descodificar una transmisión que recibe, recodificar el resultado de la descodificación y después transmitir los datos recodificados. Un nodo de retransmisión tricapa puede tener capacidades de control de recursos de radio completos y, por lo tanto, puede funcionar de forma similar a un nodo de acceso. Los protocolos de control de recursos de radio usados por un nodo de retransmisión pueden ser los mismos que los usados por un nodo de acceso, y el nodo de retransmisión puede tener una única identidad de célula usada típicamente por un nodo de acceso. Para el propósito de esta divulgación, un nodo de retransmisión 102 se distingue de un nodo de acceso 106 por el hecho de que el nodo de retransmisión 102 puede basarse en la presencia de al menos un nodo de acceso 106 (y la célula asociada a ese nodo de acceso) u otro nodo de retransmisión para acceder a otros componentes en un sistema de telecomunicaciones (por ejemplo, la red 108). Es decir, el nodo de retransmisión 102 puede parecer un dispositivo de abonado, un dispositivo cliente o un terminal de acceso para la red, por lo que se conecta a un nodo de acceso para comunicarse por la red 108. Sin embargo, para otros dispositivos de abonado, dispositivos de usuario y/o terminales de acceso 104, el nodo de retransmisión 102 puede parecer un dispositivo de red (por ejemplo, un nodo de acceso). En consecuencia, el nodo de retransmisión 102 puede implementar una o más interfaces de comunicación para comunicarse con un nodo de acceso y/o uno o más terminales de acceso/abonado/usuario. En un ejemplo, el mismo transmisor/receptor (por ejemplo, en uno o más canales inalámbricos) puede usarse por el nodo de retransmisión 102 para comunicarse con su nodo de acceso y/o uno o más terminales de acceso. En otro ejemplo, el nodo de retransmisión 102 puede utilizar dos o más transmisores/receptores diferentes para comunicarse con el nodo de acceso y/o el uno o más terminales de acceso.

[0041] Para mitigar el mal uso de una suscripción para acceder a los servicios de red, los dispositivos pueden vincular la autenticación de dispositivo con la autenticación de abonado. La autenticación de dispositivo puede funcionar junto con, por ejemplo, una autenticación de acceso AKA (autenticación y acuerdo de claves) 3GPP estándar basada en credenciales (tales como una clave raíz K de abonado) que están almacenadas en una tarjeta de circuito integrado universal (UICC) 109, 111, 113 y 116 o un módulo de identificación de abonado universal (por ejemplo, USIM) acoplados de forma extraíble al dispositivo. En algunos modos de realización, la autenticación de dispositivo puede llevarse a cabo en los mismos mensajes de estrato de no acceso (NAS) que se usan para la autenticación AKA. De esta manera, el dispositivo (por ejemplo, el nodo de retransmisión 102, los terminales de acceso 103/104, etc.) puede estar vinculado a su suscripción (es decir, suscripción de servicio con la red central 108) para evitar que otros usen sus credenciales de abonado (es decir, para un servicio de suscripción) en un dispositivo no autorizado.

[0042] Una solución al riesgo de uso no autorizado de credenciales de abonado es que el dispositivo (por ejemplo, dispositivo 101, nodo de retransmisión 102 o terminales de acceso 103/104) y la UICC 109 se autentiquen mutuamente (por ejemplo, usando un canal seguro entre el dispositivo anfitrión y la UICC), pero eso puede requerir dotar previamente a una UICC 109, 111, 113 y 116 y/o al dispositivo anfitrión (por ejemplo, dispositivo 101, nodo de retransmisión 102 o terminales de acceso 103/104) con información para realizar dicha autenticación mutua.

[0043] Otra solución puede ser requerir que las claves usadas para el acceso a red (por ejemplo, claves usadas para proteger el tráfico entre el dispositivo y la red) dependan tanto de credenciales almacenadas en la UICC 109, 111, 113 y 116 como de las credenciales almacenadas en el dispositivo (por ejemplo, dispositivo 101, nodo de retransmisión 102 o terminales de acceso 103/104). Esto se puede lograr vinculando las claves de autenticación AKA con la autenticación de dispositivo de alguna manera. Esta solución también es útil en el caso de autenticación de identidad de equipo móvil internacional (IMEI) (que, por ejemplo, puede permitir que un operador evite que dispositivos no autorizados se conecten a su red). Esto se debe a que, al vincular la(s) clave(s) resultante(s) de la autenticación AKA usada para el acceso a red con las claves usadas para la autenticación de dispositivo, se garantiza que todos los mensajes que se originan desde el dispositivo a la red 108 se originan realmente desde el dispositivo que fue autenticado. Bajo el supuesto de que las claves vinculadas (y todas las demás claves posteriores derivadas de la clave vinculada) se almacenan de forma segura en el dispositivo (por ejemplo, dispositivo 101, nodo de retransmisión 102 o terminales de acceso 103/104), la vinculación de las claves de la autenticación AKA con la autenticación de dispositivo proporciona una seguridad más sólida que el uso del mecanismo basado en pregunta/respuesta solo para la autenticación de dispositivo. El uso de un mecanismo de pregunta/respuesta solo para la autenticación de dispositivo sólo prueba que el dispositivo estaba presente para generar la respuesta de autenticación, pero no que permanezca presente en un momento posterior.

[0044] La FIG. 2 ilustra un enfoque general para vincular una autenticación de dispositivo y una autenticación de abonado. El dispositivo 202 (por ejemplo, dispositivo 101, nodo de retransmisión 102 o terminales de acceso 103/104) se puede dotar de una *clave_raíz_de_abonado* 206 y/o de una *identidad_de_abonado* 207 que se pueden usar para autenticar una suscripción con la red central 108 y/o generar claves de seguridad usadas para acceder al tráfico cifrado enviado al dispositivo 202. La *clave_raíz_de_abonado* 206 puede estar asociada de forma exclusiva con la *identidad_de_abonado* 207. En un ejemplo, la *clave_raíz_de_abonado* 206 y/o una *identidad_de_abonado* 207 pueden almacenarse en la UICC 204 y/o la autenticación de abonado puede procesarse por la UICC 204. De manera similar, el dispositivo 202 puede dotarse de (o almacenar) una *clave_raíz_de_dispositivo* 208 y/o una *identidad_de_dispositivo* 209 que se pueden usar para autenticar el dispositivo con la red central 108. La *clave_raíz_de_dispositivo* 208 puede estar asociada de forma exclusiva con *la identidad_de_dispositivo* 209.

[0045] En un ejemplo, la *identidad_de_dispositivo* 209 puede ser una identidad de equipo móvil internacional (IMEI) del dispositivo 202 (por ejemplo, dispositivo 101, nodo de retransmisión 102 o terminales de acceso 103/104), pero también se pueden usar otras formas de identidad asociadas al dispositivo (por ejemplo, la dirección de hardware IEEE, tal como EUI-48 o EUI-64).

[0046] En algunas implementaciones, la *clave_raíz_de_dispositivo* 208 puede ser una clave secreta compartida por el dispositivo 202 sólo con la red central 108 pero no transmitida de manera inalámbrica. La *identidad_de_dispositivo* 209 puede ser transmitida por el dispositivo 202 a la red central 108 para que pueda obtener la *clave_raíz_de_dispositivo* correcta para ser usada en la autenticación de dispositivo. De forma alternativa, la *clave_raíz_de_dispositivo* 208 puede ser una clave pública de un par de claves pública/privada, donde los certificados se usan para la autenticación de dispositivo. Por ejemplo, el dispositivo puede recibir algunos datos desde la red, donde los datos están cifrados con la clave pública. A continuación, el dispositivo puede usar su clave privada para descifrar los datos cifrados y, posteriormente, demostrar a la red que tiene conocimiento de los datos. El certificado (por ejemplo, *credenciales_de_dispositivo*) puede ser verificado por la red central 108. La clave privada asociada del dispositivo 202 puede almacenarse de forma segura en el dispositivo 202. Las *credenciales_de_dispositivo* pueden hacer referencia al certificado de dispositivo o a un puntero al mismo. Estas *credenciales_de_dispositivo* pueden permitir que la entidad de red pertinente forme la *pregunta_de_dispositivo* y verifique el estado de revocación del dispositivo 202 (por ejemplo, verifique si las credenciales tales como la clave privada o la clave compartida asociada al dispositivo están comprometidas). Además, se supone que una parte segura del dispositivo (como un entorno de confianza o TrE como se define en la especificación técnica 3GPP 33.320) almacena las claves sensibles del

dispositivo, tales como la *clave_raíz_de_ dispositivo* y/o la clave privada asociada al certificado. Además, se supone que el TrE realiza todas las operaciones criptográficas que hacen uso de estas claves.

[0047] Inicialmente, la autenticación de abonado puede tener lugar entre el dispositivo 202 y la red 108. Por ejemplo, un intercambio de acuerdo de autenticación de claves (AKA) 210 entre el dispositivo 202 y la red 108 puede dar como resultado el establecimiento de una clave *K_ASME.* Dicho intercambio AKA 210 se puede basar, por ejemplo, en la *clave_raíz_de_abonado* 206 y/o la *identidad_de_abonado* 207 para autenticar a un abonado asociado al dispositivo 202. Por ejemplo, dicha información o credenciales de suscripción pueden almacenarse de forma segura en la UICC 204 que está acoplada de manera extraíble al dispositivo anfitrión 202.

[0048] La red 108 también puede realizar la autenticación de dispositivo en el dispositivo 202. El dispositivo 202 puede proporcionar la *identidad_de_dispositivo* 209 a la red central 108 para que la red central 108 pueda buscar u obtener la *clave_raíz_de_dispositivo* 208 correspondiente correcta. La red 108 puede crear una *pregunta_de_dispositivo* 212 y la envía al dispositivo 202 (por ejemplo, como parte de un mensaje NAS pertinente). En respuesta, el dispositivo 202 calcula la *respuesta_de_dispositivo* 214 (por ejemplo, basándose en la *pregunta_de_dispositivo* y la *clave_raíz_de_dispositivo* 208 o derivada de las mismas) y la devuelve a la red 108. El dispositivo 202 puede usar los datos en la *pregunta_de_dispositivo* y la *respuesta_de_dispositivo* para calcular una clave de seguridad compuesta *K_ASME_D* 216. Cabe destacar que, en el caso del dispositivo 202, la clave de seguridad compuesta *K_ASME_D* 216 puede generarse antes o después de que se envíe la *respuesta_de_dispositivo* 214. En un ejemplo, la clave de seguridad compuesta *K_ASME_D* puede ser la clave equivalente a la clave de seguridad *K_ASME* definida en la Red de Acceso Radioeléctrico Terrestre Universal Evolucionada (E-UTRAN) definida en la especificación técnica 33.401 de 3GPP, excepto que la clave *K_ASME_D* está vinculada a la *identidad_de_dispositivo* 209 así como a una clave resultante de la autenticación AKA, tal como la clave K_ASME. Si la red 108 recibe una *respuesta_de_dispositivo* válida*,* la red 108 también calcula la clave de seguridad compuesta *K_ASME_D* 218.

[0049] El cálculo de la *pregunta_de_dispositivo* 212, la *respuesta_de_dispositivo* 214 y la clave de seguridad compuesta *K_ASME_D* puede ser como sigue. La *pregunta_de_dispositivo* 212 se puede calcular como:

$$pregunta\_de\_dispositivo = \text{eKSI}, [\text{E}\_clave\_raíz\_de\_dispositivo\ (\text{clave\_temp\_de\_dispositivo})], nonce\_de\_red,$$

donde *eKSI* es un identificador de conjunto de claves evolucionado/extendido que se asociará con *K_ASME_D,* [..] denota un parámetro opcional, *E_k (datos)* significa *datos* cifrados con la clave k, y *nonce_de_red* es un número aleatorio de tamaño adecuado (por ejemplo, 128 bits) elegido por la red. El algoritmo de cifrado puede ser asimétrico (en caso de que la *clave_raíz_de_dispositivo* sea una clave pública asociada a un certificado de dispositivo) o simétrico (en caso de que la *clave_raíz_de_dispositivo* sea una clave compartida). La *clave_temp_de_dispositivo* puede ser una clave que se obtiene o genera como parte de la autenticación de dispositivo. En un ejemplo, la *clave_temp_de_dispositivo* puede ser elegida por la red 108 (por ejemplo, aleatoriamente), es enviada al dispositivo 202 en forma cifrada y tiene la longitud adecuada (por ejemplo, valor de 256 o 128 bits).

[0050] Tanto el dispositivo 202 como la red 108 pueden mantener la *clave_temp_de_dispositivo* entre accesos a red para fines de optimización. Si este no es el caso, el segundo parámetro ([E_*clave_raíz_de_dispositivo* (clave_temp_de_dispositivo)]) en la *pregunta_de_dispositivo* 212 no es opcional.

[0051] La *respuesta_de_dispositivo* 214 se puede calcular como:

$$respuesta\_de\_dispositivo = nonce\_de\_dispositivo, res\_de\_dispositivo,$$

donde *nonce_de_dispositivo* es un número aleatorio de tamaño adecuado (por ejemplo, 128 bits) elegido por el dispositivo y

$$res\_de\_dispositivo = KDF\ (clave\_temp\_de\_dispositivo, nonce\_de\_red, nonce\_de\_dispositivo)$$

donde KDF es una función criptográfica adecuada para generar la respuesta *res_de_dispositivo.*

[0052] Habiendo obtenido previamente una clave de autenticación *K_ASME* (por ejemplo, como parte del intercambio AKA 210), el cálculo de una clave de seguridad compuesta *K_ASME_D* 216 y 218 (es decir, que vincula autenticación de dispositivo y autenticación de abonado), se puede hacer de la siguiente manera:

$$K\_ASME\_D = \text{KDF}\ (clave\_temp\_de\_dispositivo, K\_ASME, nonce\_de\_red, nonce\_de\_dispositivo)$$

donde *K_ASME* puede ser una clave o un valor obtenido durante la autenticación de abonado entre el dispositivo y la red (como resultado del intercambio de autenticación AKA 210). En un ejemplo, la clave *K_ASME* puede ser una clave generada y/o usada previamente entre el dispositivo 202 y la red 108. De forma alternativa, si el proceso de

autenticación de dispositivo 212 y 214 se está realizando usando los mismos mensajes NAS que los mensajes NAS usados para el procedimiento AKA 210, la clave *K_ASME* puede haberse generado recientemente o generarse simultáneamente. De manera similar, la *clave_temp_de_dispositivo* puede ser una clave o valor obtenido durante la autenticación de dispositivo entre el dispositivo 202 y la red 108.

[0053] La clave de seguridad compuesta se puede usar después como base y/o raíz para calcular claves de seguridad adicionales 217 y 219. Las claves de seguridad adicionales pueden servir para dotar de seguridad a, por ejemplo, las comunicaciones de nivel NAS y/o AS.

[0054] La clave de seguridad compuesta *K_ASME_D*, los parámetros de seguridad asociados y todas las claves derivadas de *K_ASME_D* pueden mantenerse de forma segura en el dispositivo 202 y no se almacenan en la UICC 204. La clave de seguridad compuesta *K_ASME_D* puede usarse después para proteger los mensajes intercambiados 220 entre el dispositivo 202 y la red central 108.

[0055] La FIG. 3 (que comprende la FIG. 3A y la FIG. 3B) ilustra un ejemplo de cómo se puede modificar una jerarquía de claves basada en la autenticación de abonado para incluir también la autenticación de dispositivo. Se puede implementar una jerarquía de claves para establecer los parámetros de seguridad (por ejemplo, una clave de seguridad) para su uso en el cifrado/descifrado de comunicaciones entre un dispositivo y una red. En este ejemplo, la autenticación de abonado y de dispositivo se pueden realizar entre un dispositivo 322 y una entidad de red 324. El dispositivo 322 puede ser un terminal de acceso (AT), un equipo de usuario (UE), un teléfono móvil y/o un nodo de retransmisión, por ejemplo. La entidad de red 324 puede ser uno o más dispositivos de red, tales como una entidad de gestión de movilidad (MME) y/o un servidor de abonado propio (HSS).

[0056] Este ejemplo ilustra cómo se modifica una primera jerarquía de claves 300 basada en la autenticación de abonado para obtener una segunda jerarquía de claves 300' basada tanto en la autenticación de abonado como en la autenticación de dispositivo.

[0057] Para fines de autenticación de abonado como se ilustra en la primera jerarquía de claves 300, una tarjeta de circuito integrado universal (UICC en el dispositivo 322) y la entidad de red 324 (por ejemplo, MME 110, HSS 112 en la FIG. 1 u otra entidad de red) pueden usar una clave maestra K 302 para generar una clave de cifrado (CK) 304 y una clave de integridad (IK) 306. La clave de cifrado (CK) 304 y la clave de integridad (IK) 306 pueden ser usadas por el dispositivo 322 y la entidad de red 324 como parte de un intercambio de autenticación y de acuerdo claves (AKA) para generar una clave de entidad de gestión de seguridad de acceso K_ASME 308 (también denominada en el presente documento clave de autenticación de abonado). La activación de la seguridad del dispositivo 202 puede realizarse a través de un procedimiento de acuerdo de autenticación de claves (AKA), un procedimiento de configuración de modo de seguridad de estrato de no acceso (NAS) (SMC NAS) y un procedimiento de configuración de modo de seguridad de estrato de acceso (AS) (SMC AS).

[0058] En este ejemplo, la autenticación de abonado puede incluir el intercambio AKA 326 que da como resultado la K_ASME 308. El intercambio AKA 326 puede incluir una solicitud de autenticación de abonado 340 y una respuesta de autenticación de abonado 342. En este ejemplo, el proceso de autenticación de abonado que genera la clave K_ASME 308 también puede generar claves de nivel NAS asociadas (por ejemplo, K_NAS-enc 305 y K_NAS-int 311) y/o claves de nivel AS (por ejemplo, K_UP-enc 315, K_RRC-enc 317 y K_RRC-int 319). Cabe destacar que, en algunas implementaciones, si no se usan estas versiones de las claves de nivel NAS y las claves de nivel AS, entonces se puede evitar la generación de estas claves durante la autenticación de abonado.

[0059] La segunda jerarquía de claves 300' ilustra cómo la autenticación de dispositivo puede estar vinculada a la autenticación de abonado para generar claves de seguridad de nivel NAS y nivel AS. Simultáneamente, antes o después de la autenticación del abonado (y generando su correspondiente clave K_ASME 308), la autenticación del dispositivo 328 puede realizarse basándose, al menos parcialmente, en una clave raíz específica del dispositivo. La autenticación de dispositivo 328 puede incluir una solicitud de autenticación de dispositivo 344 y una respuesta de autenticación de dispositivo 346. En una implementación, la autenticación de dispositivo 307 puede ser independiente de la autenticación de abonado; sólo si se cumplen la autenticación de abonado y de dispositivo se genera una clave de seguridad compuesta *K_ASME_D* 309. En una implementación alternativa, la autenticación de dispositivo se puede realizar antes de la autenticación de abonado.

[0060] La clave de seguridad compuesta *K_ASME_D* 309 se puede usar como una clave base para el cálculo de, por ejemplo, las claves NAS (estrato de no acceso) 310 y 312 y las claves AS (estrato de acceso) 314, 316, 318 y 320. Es decir, el dispositivo 322 y la entidad de red 324 pueden usar la clave K_ASME_D 309 para generar una o más claves de seguridad.

[0061] Las redes de conmutación de paquetes pueden estructurarse en múltiples capas de protocolo jerárquicas, donde las capas de protocolo inferiores proporcionan servicios a las capas superiores y cada capa es responsable de diferentes tareas. Por ejemplo, la FIG. 4 ilustra una pila de protocolos ejemplar que puede implementarse en un dispositivo que funciona en una red de conmutación de paquetes. En este ejemplo, la pila de protocolos 402 incluye una capa física (PHY) 404, una capa de control de acceso al medio (MAC) 406, una capa de control de radioenlace

(RLC) 408, una capa de protocolo de convergencia de datos por paquetes (PDCP) 410, una capa de control de recursos de radio (RRC) 412, una capa de estrato de no acceso (NAS) 414 y una capa de aplicación (APP) 416.

[0062] Las capas por debajo de la capa NAS 414 a menudo se denominan capa de estrato de acceso (AS) 418. La capa RLC 408 puede incluir uno o más canales 420. La capa RRC 412 puede implementar diversos modos de supervisión para el terminal de acceso, incluyendo estado conectado y estado inactivo. La capa de estrato de no acceso (NAS) 414 puede mantener el contexto de gestión de movilidad del dispositivo de comunicación, el contexto de datos por paquetes y/o sus direcciones IP. Cabe destacar que otras capas pueden estar presentes en la pila de protocolos 402 (por ejemplo, encima, debajo y/o entre las capas ilustradas), pero se han omitido con fines ilustrativos.

[0063] Con referencia a la FIG. 4, se pueden establecer portadoras de radio/sesión 422, por ejemplo en la capa RRC 412 y/o la capa NAS 414. En consecuencia, la capa NAS 414 puede ser usada por el dispositivo 202 y la red central 108 para generar las claves de seguridad K_NAS-enc 310 y K_NAS-int 312 mostradas en la FIG. 3. De manera similar, el dispositivo 202 y el nodo de acceso 108 pueden usar la capa RRC 412 para generar las claves de seguridad de estrato de acceso (AS) K_UP-enc 316, K_RRC-enc 318 y K_RRC-int 320. Aunque las claves de seguridad K_UP-enc 316, K_RRC-enc 318 y K_RRC-int 320 pueden generarse en la capa RRC 312, la capa PDCP 410 puede usar estas claves para dotar de seguridad a la señalización y/o las comunicaciones de usuario/datos. Por ejemplo, la clave K UP-enc 316 puede ser usada por la capa PDCP 410 para dotar de seguridad a las comunicaciones en el plano de usuario/datos (UP), mientras que las claves K RRC-enc 318 y K_RRC-int 320 se pueden usar para dotar de seguridad a comunicaciones de señalización (es decir, control) en la capa PDCP 410.

[0064] En la obtención de estas claves de seguridad, usadas para los algoritmos de cifrado e integridad, tanto en el AS (plano de usuario y RRC) como en el NAS se requiere que se proporcione una identidad de algoritmo individual como una de las entradas. En el nivel AS, los algoritmos que se usarán son proporcionados por un comando de modo de seguridad de control de recursos de radio (RRC).

[0065] La FIG. 5 es un diagrama de bloques que ilustra un sistema de red en el que pueden generarse las diversas claves de autenticación y/o seguridad ilustradas en las FIGS. 3 y 4. En este caso, el dispositivo 322 puede implementar una pila de comunicación que incluye diversas capas (por ejemplo, APP, NAS, RRC, RLC, MAC y PHY). Una red de acceso 504 (por ejemplo, el nodo de acceso 106 en la FIG. 1) puede proporcionar conectividad inalámbrica al dispositivo 322 para que pueda comunicarse con la red 108. El servidor de abonado propio 506 y el dispositivo 322 pueden conocer o tener acceso a una clave raíz (K) que se puede usar para generar u obtener una clave de cifrado (CK) y/o una clave de integridad (IK). El dispositivo 322 y/o el HSS 506 pueden usar la clave de cifrado (CK) y/o la clave de integridad (IK) para generar una clave de entidad de gestión de seguridad de acceso K ASME. La autenticación de dispositivo también se puede realizar y combinar con o en base a la clave K_ASME para generar una clave de seguridad compuesta K_ASME_D, combinando así la autenticación de abonado y de dispositivo en una clave. Usando la clave K_ASME_d, el dispositivo 322 y una entidad de gestión de movilidad (MME) 510 pueden generar las claves K_NAS-enc y K_NAS-int. El dispositivo 322 y la MME 510 también pueden generar una clave específica de red de acceso K_eNB/NH. Usando esta clave específica de red de acceso K_eNB/NH, el dispositivo 322 y la red de acceso 504 pueden generar las claves K_UP-enc y K_RRC-enc y K_RRC-int.

[0066] Los detalles sobre la obtención de estas claves se proporcionan en el documento 3GPP STD-T63-33.401 "System Architecture Evolution (SAE): Security Architecture" (conocido como 3GPP TS 33.401) Versión 8. Cabe destacar que mientras que las FIGS. 3-5 describen un entorno/contexto particular en el que se pueden implementar la autenticación y vinculación de dispositivo y de abonado, esto no pretende limitar esta característica, que se puede implementar en otros diversos tipos de redes.

Dispositivo inalámbrico ejemplar

[0067] La FIG. 6 es un diagrama de bloques que ilustra componentes seleccionados de un dispositivo inalámbrico 600 que pueden adaptarse para vincular la autenticación de abonado y la autenticación de dispositivo. El dispositivo inalámbrico 600 incluye generalmente un circuito de procesamiento 602 acoplado a una o más interfaces de comunicación inalámbrica 604. Por ejemplo, el dispositivo inalámbrico 600 puede ser un nodo de retransmisión y/o un terminal de acceso.

[0068] El circuito de procesamiento 602 puede estar dispuesto para obtener, procesar y/o enviar datos, controlar el acceso y almacenamiento de datos, emitir comandos y controlar otras operaciones deseadas. El circuito de procesamiento 602 puede comprender circuitos configurados para implementar una programación deseada proporcionada por medios apropiados en al menos un modo de realización. Por ejemplo, el circuito de procesamiento 602 puede implementarse como uno o más de un procesador, un controlador, una pluralidad de procesadores y/u otra estructura configurada para ejecutar instrucciones ejecutables incluyendo, por ejemplo, instrucciones de software y/o firmware y/o circuitos de hardware. Los modos de realización del circuito de procesamiento 602 pueden incluir un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), una matriz de puertas programables *in situ* (FPGA) u otro componente de lógica programable, lógica de transistor o de puertas discretas, componentes de hardware discretos o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede

ser un microprocesador pero, como alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados convencional. Un procesador también puede implementarse como una combinación de componentes informáticos, tal como una combinación de un DSP y un microprocesador, varios microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo. Estos ejemplos del circuito de procesamiento 602 tienen fines ilustrativos y también se contemplan otras configuraciones adecuadas dentro del alcance de la presente divulgación.

[0069] La interfaz de comunicaciones inalámbricas 604 se puede configurar para facilitar las comunicaciones inalámbricas del dispositivo inalámbrico 600. Por ejemplo, la interfaz de comunicaciones 604 puede configurarse para comunicar información bidireccionalmente con respecto a otros dispositivos inalámbricos, tales como terminales de acceso, nodos de acceso, otros nodos de retransmisión, etc. La interfaz de comunicaciones 604 puede acoplarse a una antena (no mostrada) y puede incluir circuitos de transceptor inalámbrico, incluyendo, al menos, un transmisor y/o, al menos, un receptor (por ejemplo, una o más cadenas de transmisores/receptores) para comunicaciones inalámbricas.

[0070] El circuito de procesamiento 602 puede incluir un módulo de vinculación de autenticación de abonado y de dispositivo 610. El módulo de autenticación de abonado y de dispositivo 610 puede comprender circuitos y/o programación adaptados para realizar procedimientos de autenticación de abonado usando credenciales de seguridad de abonado (por ejemplo, una clave específica de abonado 607 y/o una identidad de abonado 609 almacenada en una tarjeta de circuito integrado universal 608), adaptados para realizar (dentro de un entorno de confianza 606) procedimientos de autenticación de dispositivos usando credenciales específicas de dispositivo (por ejemplo, una clave específica de dispositivo 605 y/o una identidad de dispositivo 611), y vincular las autenticaciones de abonado y de dispositivo entre sí. Dicha "vinculación" puede implicar la combinación de algunos resultados de la autenticación de abonado y la autenticación de dispositivo. Por ejemplo, una primera clave de seguridad obtenida de la autenticación de abonado puede combinarse con una segunda clave de seguridad obtenida de la autenticación de dispositivo para obtener una tercera clave de seguridad (compuesta).

[0071] En algunos modos de realización, el dispositivo inalámbrico 600 puede incluir un entorno de confianza (TrE) 606. El entorno de confianza 606 puede adaptarse para cumplir las especificaciones para un entorno de confianza en el detalle de las especificaciones 3GPP en TS 33.320. El entorno de confianza 606 puede dotarse previamente de (o integrarse de forma segura con) al menos algunas credenciales de seguridad (por ejemplo, la clave específica de dispositivo 605 y/o la identidad de dispositivo 611). Por ejemplo, el entorno de confianza 606 puede tener credenciales de seguridad relacionadas con la autenticación de dispositivo.

[0072] En algunos modos de realización, el dispositivo inalámbrico 600 puede incluir un procesamiento seguro dentro de la tarjeta de circuito integrado universal (UICC) 608. La UICC 608 puede estar acoplada de forma extraíble al dispositivo inalámbrico 600. La UICC 608 puede dotarse previamente de credenciales de seguridad de abonado (por ejemplo, clave específica de abonado 607 y/o identidad de abonado 609), tales como las credenciales iniciales de acuerdo de autenticación de claves (AKA). De forma alternativa, el procesamiento seguro puede realizarse dentro de un módulo de identidad de abonado universal (USIM).

[0073] De acuerdo con una o más características del dispositivo inalámbrico 600, el circuito de procesamiento 602 puede adaptarse para realizar cualquiera o cada uno de los procesos, funciones, etapas y/o rutinas relacionados, ilustrados en las FIG. 2-5, 7, 10, 11 y 12. Como se usa en el presente documento, el término "adaptado" en relación con el circuito de procesamiento 602 puede referirse al circuito de procesamiento 602 que está configurado, empleado, implementado y/o programado para realizar un proceso, función, etapa y/o rutina particular de acuerdo con diversas características descritas en el presente documento.

[0074] La FIG. 7 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en un dispositivo inalámbrico para generar una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo. El dispositivo inalámbrico puede dotarse previamente de una clave específica de dispositivo 702. Por ejemplo, dicha clave específica de dispositivo puede integrarse en un chip o configurarse durante la fabricación del dispositivo inalámbrico. El dispositivo inalámbrico también puede incluir un identificador de dispositivo asociado a la clave específica de dispositivo. Además, el dispositivo inalámbrico puede dotarse previamente de una clave específica de abonado 704. Por ejemplo, dicha clave específica de abonado puede ser una clave raíz asignada a un abonado y puede almacenarse dentro de un módulo fijo o extraíble (por ejemplo, UICC o USIM) acoplado al dispositivo inalámbrico. El dispositivo inalámbrico también puede incluir una identidad de suscripción asociada a la clave específica de abonado. El dispositivo inalámbrico puede realizar la autenticación de abonado con una entidad de red (por ejemplo, usando la clave específica de abonado) 706. Esto puede incluir, por ejemplo, un intercambio de acuerdo de autenticación de claves con la entidad de red. El dispositivo inalámbrico también puede realizar la autenticación de dispositivo con la entidad de red (por ejemplo, usando la clave específica de dispositivo) 708. La autenticación de abonado y la autenticación de dispositivo se pueden realizar al mismo tiempo o en diferentes momentos y con la misma entidad de red o con diferentes entidades de red. A continuación, el dispositivo inalámbrico puede generar una clave de seguridad (por ejemplo, K_ASME_D, etc.), donde dicha clave de seguridad vincula la autenticación de abonado y la autenticación de dispositivo 710. Por ejemplo, en un ejemplo, los datos (por ejemplo, una o más claves, certificados, identificadores, etc., resultantes) de la autenticación de dispositivo y los datos (por ejemplo, una o más

claves, certificados, identificadores, etc., resultantes) de la autenticación de abonado pueden combinarse para generar la clave de seguridad. Por ejemplo, en la FIG. 1, la clave K_ASME de la autenticación de abonado 210 y la clave_temp_de_dispositivo de la autenticación de dispositivo en la FIG. 1 se pueden combinar para generar la clave de seguridad K_ASME_D. La clave de seguridad se puede usar entonces para dotar de seguridad a las comunicaciones inalámbricas entre el dispositivo inalámbrico y la entidad de red 712. Por ejemplo, la clave de seguridad se puede usar para generar otras claves y/o certificados (por ejemplo, claves de seguridad de nivel NAS y/o nivel AS) que pueden servir para cifrar/descifrar comunicaciones (por ejemplo, datos y señalización) entre el dispositivo inalámbrico y la red.

Entidad de red ejemplar

[0075] La FIG. 8 es un diagrama de bloques que ilustra componentes seleccionados de una entidad de red 800 que pueden adaptarse para vincular la autenticación de abonado y la autenticación de dispositivo. La entidad de red 800 puede incluir un circuito de procesamiento 802 acoplado a una interfaz de comunicaciones 804. El circuito de procesamiento 802 está dispuesto para obtener, procesar y/o enviar datos, controlar el acceso y almacenamiento de datos, emitir comandos y controlar otras operaciones deseadas. El circuito de procesamiento 802 puede comprender circuitos configurados para implementar una programación deseada proporcionada por medios apropiados en al menos un modo de realización. Por ejemplo, el circuito de procesamiento 802 puede implementarse como uno o más de un procesador, un controlador, una pluralidad de procesadores y/u otra estructura configurada para ejecutar instrucciones ejecutables incluyendo, por ejemplo, instrucciones de software y/o firmware, y/o circuitos de hardware. Los modos de realización del circuito de procesamiento 802 pueden incluir un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la de aplicación (ASIC), una matriz de puertas programables *in situ* (FPGA) u otro componente de lógica programable, lógica de transistor o de puertas discretas, componentes de hardware discretos o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador pero, como alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados convencional. Un procesador también puede implementarse como una combinación de componentes informáticos, tal como una combinación de un DSP y un microprocesador, varios microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo. Estos ejemplos del circuito de procesamiento 802 son para ilustración y también se contemplan otras configuraciones adecuadas dentro del alcance de la presente divulgación.

[0076] El circuito de procesamiento 802 incluye un módulo de vinculación de autenticación de abonado y de dispositivo 806. El módulo de vinculación de autenticación de abonado y de dispositivo 806 puede comprender circuitos y/o programación adaptados para realizar procedimientos de autenticación de abonado para autenticar una suscripción en base a credenciales de seguridad de abonado (por ejemplo, clave específica de abonado y/o identificador de abonado), realizar procedimientos de autenticación de dispositivo para autenticar el dispositivo en base a credenciales específicas de dispositivo (por ejemplo, clave específica de dispositivo y/o identificador de dispositivo), y vincular datos (por ejemplo, claves, valores, certificados, etc.) de la autenticación de dispositivo y la autenticación de abonado para generar una clave de seguridad.

[0077] La interfaz de comunicaciones 804 está configurada para facilitar las comunicaciones de la entidad de red 800 para comunicarse, directa o indirectamente (por ejemplo, a través de una o más entidades de red distintas), con otros dispositivos, tales como nodos de retransmisión y terminales de acceso.

[0078] De acuerdo con una o más características de la entidad de red 800, el circuito de procesamiento 802 puede adaptarse para realizar cualquier o cada uno de los procesos, funciones, etapas y/o rutinas relacionados con las diversas entidades de red, tales como una entidad de gestión de movilidad (MME) 110 y un servidor de abonado propio (HSS) 112. Además, la entidad de red 800 puede comprender una única entidad, o una combinación de dos o más entidades de la red. A modo de ejemplo y sin limitación, la entidad de red 800 puede comprender una entidad de gestión de movilidad (MME), un servidor de abonado propio (HSS), un servidor de autenticación de dispositivo, entre otros. Como se usa en el presente documento, el término "adaptado" en relación con el circuito de procesamiento 802 puede referirse al circuito de procesamiento 802 que está uno o más de entre configurado, empleado, implementado o programado para realizar un proceso, función, etapa y/o rutina particular de acuerdo con diversas características descritas en el presente documento.

[0079] La FIG. 9 es un diagrama de flujo que ilustra un ejemplo de un procedimiento operativo en una entidad de red para generar una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo. La entidad de red puede obtener una clave específica de dispositivo para un dispositivo inalámbrico 902. Por ejemplo, dicha clave específica de dispositivo puede integrarse en un chip o configurarse durante la fabricación del dispositivo inalámbrico y esta información puede almacenarse en una base de datos a la que puede acceder la entidad de red. Un identificador de dispositivo puede estar asociado a la clave específica de dispositivo y se puede usar para identificar el dispositivo y su clave. Además, la entidad de red puede obtener una clave específica de abonado asociada a una suscripción para el dispositivo inalámbrico 904. Por ejemplo, dicha clave específica de abonado puede ser una clave raíz asignada a un abonado y puede almacenarse dentro de un módulo fijo o extraíble (por ejemplo, UICC o USIM) acoplado al dispositivo inalámbrico. La entidad de red puede realizar la autenticación de abonado con el dispositivo

inalámbrico (por ejemplo, usando la clave específica de abonado) 906. Esto puede incluir, por ejemplo, un intercambio de acuerdo de autenticación de claves con la entidad de red. La entidad de red también puede realizar la autenticación de dispositivo con el dispositivo inalámbrico (por ejemplo, usando la clave específica de dispositivo) 908. La autenticación de abonado y la autenticación de dispositivo se pueden realizar al mismo tiempo o en momentos diferentes. A continuación, la entidad de red puede generar una clave de seguridad (compuesta) (por ejemplo, K_ASME_D, etc.), donde dicha clave de seguridad vincula la autenticación de abonado y la autenticación de dispositivo 910. Por ejemplo, en un ejemplo, los datos (por ejemplo, una o más claves, certificados, identificadores, etc., resultantes) de la autenticación de dispositivo y los datos (por ejemplo, K_ASME, etc.) de la autenticación de abonado pueden combinarse para generar la clave de seguridad. La clave de seguridad se puede usar para dotar de seguridad a las comunicaciones inalámbricas entre la entidad de red y el dispositivo inalámbrico 912. Por ejemplo, la clave de seguridad se puede usar para generar otras claves y/o certificados que pueden servir para cifrar/descifrar comunicaciones entre el dispositivo inalámbrico y la red.

Primer procedimiento ejemplar de autenticación de abonado-dispositivo

[0080] La FIG. 10 ilustra un primer procedimiento ejemplar para generar una clave de seguridad mediante la vinculación de la autenticación de abonado y de dispositivo. En este ejemplo, el dispositivo 1002 puede ser un nodo de retransmisión o un terminal de acceso, por ejemplo. Durante una etapa de conexión, donde el dispositivo 1102 puede intentar conectarse a una red inalámbrica (por ejemplo, que incluye la MME 1002 y el HSS 1006), el revelar la identidad de un dispositivo u otra información de dispositivo relacionada de forma inalámbrica puede ser un problema de seguridad (por ejemplo, para el dispositivo 1002). En consecuencia, en este procedimiento, el dispositivo 1002 no presenta sus credenciales de dispositivo (por ejemplo, un identificador específico de dispositivo, tal como una identidad de equipo móvil internacional (IMEI), etc.) de forma inalámbrica hasta que la red lo solicite de forma segura para evitar ataques pasivos a la identidad del dispositivo.

[0081] El dispositivo puede comenzar enviando a la red una solicitud de conexión 1010 que incluye una indicación de que es capaz de autenticar el dispositivo. Al recibir la solicitud de conexión 1010, una entidad de gestión de movilidad (MME) 1004 puede solicitar y recibir información de suscripción y autenticación 1012 (por ejemplo, asociada a una cuenta basada en suscripción o usuario del dispositivo 1002) desde un servidor de abonado propio (HSS) 1006. La MME 1004 envía después una solicitud de autenticación 1014 que incluye una pregunta AKA para realizar la autenticación AKA. Al recibir la solicitud de autenticación AKA 1014, el dispositivo 1002 envía una respuesta de autenticación 1016 que incluye una respuesta AKA. La solicitud de autenticación AKA 1014 y la respuesta 1016 sirven para realizar la autenticación de suscripción. Dichos procedimientos de autenticación AKA pueden dar como resultado que el dispositivo 1002 y la MME generen una clave de autenticación de abonado (por ejemplo, K_ASME).

[0082] La autenticación de dispositivo se puede realizar en diversas fases durante este proceso de activación de seguridad. En este ejemplo, la autenticación de dispositivo puede ir intercalada en los mensajes de seguridad de nivel NAS. Por ejemplo, la MME 1004 puede enviar un comando de modo de seguridad NAS 1018 que incluye una solicitud referente a la identidad de dispositivo (por ejemplo, una solicitud referente a la versión del software IMEI (IMEISV) y/o una solicitud referente a las *credenciales_de_dispositivo*). En respuesta, el dispositivo 1002 puede proporcionar una identidad o credencial de dispositivo, dentro de un mensaje de modo de seguridad completo 1020, de que se debe realizar la autenticación de dispositivo. Cabe destacar que, para evitar exponer la identidad o credencial de dispositivo de forma inalámbrica durante la transmisión, la identidad o credencial de dispositivo en el modo de seguridad completo 1020 puede asegurarse mediante la clave de autenticación de abonado calculada previamente (por ejemplo, K_ASME). Al recibir la identidad o credencial de dispositivo, la MME 1004 puede enviar un mensaje de solicitud de identidad 1022, con un identificador de conjunto de claves evolucionado/extendido (eKSI) y una pregunta_de_dispositivo. El eKSI puede estar asociado a una *K_ASME_D* que se generará. Por lo tanto, el eKSI usado en la solicitud de identidad 1022 puede ser diferente o distinto de cualquier otro eKSI que pueda haberse usado, por ejemplo, para AKA (es decir, autenticación de abonado). Al recibir el mensaje de solicitud de identidad 1022, el dispositivo 1002 puede generar una respuesta_de_dispositivo en base a la pregunta_de_dispositivo y la envía como parte de un mensaje de respuesta_de_identidad 1024. La respuesta_de_dispositivo puede basarse en la pregunta de dispositivo y la identidad o credencial de dispositivo. El dispositivo 1002 puede calcular después una clave de seguridad (compuesta) (K_ASME_D) 1025 en base a la clave de autenticación (por ejemplo, K ASME) y los datos de autenticación de dispositivo (por ejemplo, respuesta de dispositivo, etc.). La MME 1004 verifica la respuesta_de_dispositivo, por ejemplo, mediante el uso de la identidad de dispositivo o el certificado del dispositivo 1002 y usando la pregunta_de_dispositivo. Si el dispositivo 1002 es autenticado con éxito por la MME 1004, la MME 1004 también genera la clave de seguridad (K_ASME_D) 1027. En este punto, el dispositivo 1002 y la MME 1004 comparten la clave de seguridad (K_ASME_D) y su identificador asociado eKSI.

[0083] La MME 1004 puede enviar después un comando de modo de seguridad 1026 con el identificador de conjunto de claves evolucionado/extendido eKSI asociado a la clave de seguridad (K_ASME_D). Esto permite que el dispositivo 1002 calcule una o más claves de seguridad en base a la clave de seguridad (K_ASME_D). El dispositivo 1002 puede enviar un mensaje de modo de seguridad completo 1028 a la MME 1004, permitiendo así que la MME 1004 envíe un mensaje de conexión completa 1030.

Segundo procedimiento ejemplar de autenticación de abonado-dispositivo

[0084] La FIG. 11 ilustra un segundo procedimiento ejemplar para generar una clave de seguridad mediante la vinculación de la autenticación de abonado y de dispositivo. En este ejemplo, revelar la identidad o el certificado de dispositivo (u otra información de credenciales relacionada) en una transmisión inalámbrica no es un problema de seguridad. A diferencia del procedimiento de la FIG. 10, en este caso, se supone que presentar la identidad de dispositivo por adelantado no generará problemas o riesgos de privacidad.

[0085] El dispositivo ya tiene un identificador o credenciales de dispositivo (por ejemplo, IMEI) que la MME aceptará, pero no tiene un contexto de seguridad E-UTRAN que la MME esté dispuesta a usar.

[0086] El dispositivo 1102 envía una solicitud de conexión 1108 que incluye su *identificador* o *credenciales de dispositivo* a la MME 1104. La MME 1104 puede obtener una información de suscripción y autenticación 1110 del HSS 1106 y envía una solicitud de autenticación 1112 que incluye, por ejemplo, una pregunta AKA (para autenticación de suscripción) y/o una pregunta de dispositivo (para autenticación de dispositivo). Cabe destacar que el dispositivo 1102 puede responder enviando una respuesta de autenticación 1114 que puede incluir una respuesta AKA y/o una respuesta de dispositivo. La respuesta AKA puede basarse, al menos parcialmente, en el identificador de abonado. La respuesta de dispositivo puede basarse en el *identificador* y/o *credenciales* de dispositivo y la pregunta de dispositivo. El dispositivo 1104 puede generar después una clave de seguridad (compuesta) K_ASME_D combinando información de autenticación de abonado e información de autenticación de dispositivo. De manera similar, tras una verificación exitosa de la respuesta AKA y la respuesta de dispositivo, la MME 1104 también puede generar la clave de seguridad K_ASME_D combinando la información de autenticación de abonado y la información de autenticación de dispositivo.

[0087] La MME envía un mensaje de comando de modo de seguridad 1116 para comenzar a usar el contexto de seguridad en base a la clave de seguridad K_ASME_D. El dispositivo 1102 responde con un mensaje de modo de seguridad completo 1118. Es decir, el dispositivo 1102 y la MME 1104 pueden generar una o más claves de seguridad adicionales (o comunicaciones seguras de otro modo entre el dispositivo 1102 y la MME 1104) usando la clave de seguridad K_ASME_D. A continuación, la MME 1104 puede enviar un mensaje de conexión completa 1120 al dispositivo 1102.

[0088] Una observación en este caso es que si el identificador y/o las credenciales de dispositivo (o claves de dispositivo obtenidas/generadas previamente) se almacenaron en el HSS 1106 u otro servidor en la red con un identificador de suscripción, entonces el dispositivo 1102 podría usar este flujo para realizar la conexión. Para hacer esto allí, el dispositivo 1102 puede indicar (por ejemplo, en la solicitud de conexión 1108) que su identificador de dispositivo y/o credenciales pueden obtenerse del HSS 1106 u otro servidor de red. De forma alternativa, la MME 1104 puede indicar al dispositivo 1102 que la *pregunta_de_dispositivo* está asociada a un identificador de dispositivo particular (por ejemplo, al incluir el identificador de dispositivo, tal como el IMEI, junto con la *pregunta_de_dispositivo* de alguna forma). De esta manera, el dispositivo 1102 puede saber que la pregunta de dispositivo (en la solicitud de autenticación 1112) está asociada a su identificador de dispositivo.

Tercer procedimiento ejemplar de autenticación de abonado-dispositivo

[0089] La FIG. 12 ilustra un tercer procedimiento ejemplar para generar una clave de seguridad mediante la vinculación de la autenticación de abonado y de dispositivo. En este ejemplo, la autenticación de abonado se ha realizado previamente, por lo que ya existe un contexto de seguridad de abonado 1206 (por ejemplo, clave K_ASME). La red puede iniciar la autenticación combinada de abonado y dispositivo para reemplazar el contexto de seguridad existente. Este modo de realización puede ser beneficioso para dispositivos que podrían necesitar establecer un contexto de seguridad inicial basado en AKA para obtener credenciales completas u operativas del operador.

[0090] Este enfoque supone que la MME ya conoce el identificador de dispositivo (por ejemplo, *IMEI*) y/o las credenciales_de_dispositivo.

[0091] La MME 1204 envía una solicitud de autenticación 1208 al dispositivo 1202 que incluye una *pregunta_de_dispositivo.* En respuesta, el dispositivo 1202 envía una respuesta de autenticación 1210 a la MME 1204 que incluye una *respuesta_de_dispositivo.* La *respuesta_de_dispositivo* puede basarse en la *pregunta_de_dispositivo* y en el identificador y/o certificado de dispositivo. En este punto, tanto el dispositivo 1202 como la MME 1204 pueden tener información suficiente para calcular una clave de seguridad (compuesta) K_ASME_D (por ejemplo, basándose en el contexto de seguridad basado en AKA y la información de autenticación de dispositivo).

[0092] La MME 1204 puede enviar un comando de modo de seguridad NAS 1212 al dispositivo 1202 para reemplazar el contexto de seguridad existente 1206 por uno basado en la nueva clave de seguridad K_ASME_D (por ejemplo, que incorpora tanto la autenticación de abonado como la autenticación de dispositivo). En respuesta, el dispositivo 1202 puede generar un nuevo contexto de seguridad basado en la clave de seguridad K_ASME_D y puede enviar un mensaje de modo de seguridad completo NAS 1214 en respuesta.

[0093] Cabe destacar que, aunque diversos ejemplos en el presente documento ilustran que tanto la autenticación de abonado como la autenticación de dispositivo se pueden realizar por medio de la MME, otras entidades de red pueden realizar algunas de estas funciones en combinación con la MME o en su lugar.

[0094] Uno o más de los componentes, etapas, características y/o funciones ilustrados en las FIGS. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 y/o 12 se pueden reorganizar y/o combinarse en un único componente, etapa, característica o función o incluirse en varios componentes, etapas o funciones. También pueden añadirse elementos, componentes, etapas y/o funciones adicionales sin apartarse de la presente divulgación. Los aparatos, dispositivos y/o componentes ilustrados en las FIGS. 1, 5, 6 y/u 8 pueden configurarse para realizar uno o más de los procedimientos, características o etapas descritos en las FIGS. 2, 3, 4, 7 y/o 9-12. Los algoritmos novedosos descritos en el presente documento también se pueden implementar eficazmente en software y/o integrarse en hardware.

[0095] Además, debe observarse que al menos algunas implementaciones se han descrito como un proceso que se representa como un organigrama, un diagrama de flujo, un diagrama estructural o un diagrama de bloques. Aunque un organigrama puede describir las operaciones como un proceso secuencial, muchas de las operaciones se pueden realizar en paralelo o simultáneamente. Además, el orden de las operaciones se puede reorganizar. Un procedimiento termina cuando se acaban sus operaciones. Un procedimiento puede corresponder a un método, una función, un procedimiento, una subrutina, un subprograma, etc. Cuando un procedimiento corresponde a una función, su finalización corresponde a un retorno de la función a la función de llamada o a la función principal.

[0096] Además, los modos de realización pueden implementarse en hardware, software, firmware, middleware, microcódigo o cualquier combinación de los mismos. Al implementarse en software, firmware, middleware o microcódigo, el código de programa o segmentos de código para realizar las tareas necesarias pueden almacenarse en un medio legible por máquina, tal como un medio de almacenamiento u otro(s) almacenamiento(s). Un procesador puede realizar las tareas necesarias. Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase o cualquier combinación de instrucciones, estructuras de datos o sentencias de programa. Un segmento de código se puede acoplar a otro segmento de código o a un circuito de hardware pasando y/o recibiendo información, datos, argumentos, parámetros o contenidos de memoria. Se puede pasar, enviar o transmitir información, argumentos, parámetros, datos, etc. por medio de cualquier medio adecuado, incluido la compartición de memoria, el paso de mensajes, el paso de testigos, la transmisión por red, etc.

[0097] Las expresiones "medio legible por máquina", "medio legible por ordenador" y/o "medio legible por procesador" pueden incluir, pero no se limitan a, dispositivos de almacenamiento portátiles o fijos, dispositivos de almacenamiento ópticos y otros diversos medios no transitorios capaces de almacenar, contener o portar instrucciones y/o datos. Por lo tanto, los diversos procedimientos descritos en el presente documento pueden implementarse parcial o completamente mediante instrucciones y/o datos que pueden almacenarse en un "medio legible por máquina", "medio legible por ordenador" y/o un "medio legible por procesador" y ejecutarse por uno o más procesadores, máquinas y/o dispositivos.

[0098] Los procedimientos o algoritmos descritos en relación con los ejemplos divulgados en el presente documento pueden realizarse directamente en hardware, en un módulo de software ejecutable por un procesador, o en una combinación de ambas maneras, en forma de unidad de procesamiento, instrucciones de programación u otras instrucciones, y pueden almacenarse en un único dispositivo o distribuirse en múltiples dispositivos. Un módulo de software puede residir en una memoria RAM, una memoria flash, una memoria ROM, una memoria EPROM, una memoria EEPROM, registros, un disco duro, un disco extraíble, un CD-ROM o en cualquier otra forma de medio de almacenamiento no transitorio conocida en la técnica. Un medio de almacenamiento puede estar acoplado al procesador de manera que el procesador pueda leer información de, y escribir información en, el medio de almacenamiento. De forma alternativa, el medio de almacenamiento puede estar integrado en el procesador.

[0099] Los expertos en la técnica apreciarán además que los diversos bloques lógicos, módulos, circuitos y etapas de algoritmo ilustrativos descritos en relación con los modos de realización divulgados en el presente documento pueden implementarse como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, anteriormente se han descrito diversos componentes, bloques, módulos, circuitos y etapas ilustrativos, en general, en lo que respecta a su funcionalidad. Que dicha funcionalidad se implemente como hardware o software depende de la aplicación particular y de las restricciones de diseño impuestas en el sistema general.

[0100] Las diversas características de la invención descritas en el presente documento pueden implementarse en diferentes sistemas sin apartarse de la invención. Cabe destacar que los modos de realización anteriores son simplemente ejemplos y no han de interpretarse como limitantes de la invención. La descripción de los modos de realización pretende ser ilustrativa y no limitar el alcance de la divulgación. Como tales, las presentes enseñanzas pueden aplicarse fácilmente a otros tipos de aparatos, y muchas alternativas, modificaciones y variaciones serán evidentes para los expertos en la técnica.

REIVINDICACIONES

1. Un procedimiento operativo en un dispositivo (202), que comprende:

realizar (706) una autenticación de abonado con una entidad de red (324) en base a un intercambio de acuerdo de autenticación de claves, AKA, entre el dispositivo y la entidad de red, llevada a cabo en mensajes de estrato de no acceso, NAS;

realizar (708) una autenticación de dispositivo del dispositivo (202) con la entidad de red (324), llevada a cabo en los mismos mensajes de NAS usados para la autenticación de abonado basada en AKA, donde el dispositivo (202) está dotado previamente (702) de una clave específica de dispositivo (202) que se usa para la autenticación de dispositivo;

generar (710) una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo; y

usar (712) la clave de seguridad para asegurar las comunicaciones entre el dispositivo (202) y una red de servicio (108).

2. El procedimiento según la reivindicación 1, en el que la autenticación de dispositivo se basa en un intercambio de pregunta-respuesta entre el dispositivo (202) y la entidad de red (324).

3. El procedimiento según la reivindicación 1, en el que la autenticación de abonado es realizada por un primer servidor de autenticación que es parte de la entidad de red (324), y la autenticación de dispositivo es realizada por un segundo servidor de autenticación que es parte de la entidad de red (324).

4. El procedimiento según la reivindicación 1, que comprende además:

enviar una solicitud de conexión desde el dispositivo (202) a la entidad de red (324), incluyendo la solicitud de conexión una indicación de las capacidades de autenticación de dispositivo del dispositivo (202) y/o en el que se dota de seguridad a la autenticación de dispositivo mediante al menos una clave generada durante la autenticación de abonado y/o en el que la autenticación de abonado y la autenticación de dispositivo se realizan simultáneamente en intercambios de mensajes combinados.

5. El procedimiento según la reivindicación 1, en el que la clave de seguridad se genera en función de al menos una primera clave obtenida de la autenticación de abonado y una segunda clave obtenida de la autenticación de dispositivo, y en el que la clave de seguridad depende además de un nonce de red y de un nonce de dispositivo.

6. El procedimiento según la reivindicación 1, en el que el dispositivo (202) es un nodo de retransmisión que parece un terminal de acceso para la entidad de red (324) y parece un dispositivo de red para uno o más terminales de acceso y/o en el que la clave de seguridad es generada por separado por el dispositivo (202) y la entidad de red (324).

7. El procedimiento según la reivindicación 1, que comprende además:

proporcionar una clave específica de abonado como parte de un acuerdo de servicio, donde la clave específica de abonado se usa para la autenticación de abonado.

8. Un dispositivo (202), que comprende:

medios para realizar una autenticación de abonado con una entidad de red (324) en base a un intercambio de acuerdo de autenticación de claves, AKA, entre el dispositivo y la entidad de red, llevada a cabo en mensajes de estrato no de acceso, NAS;

medios para realizar una autenticación de dispositivo (202) con la entidad de red (324), llevada a cabo en los mismos mensajes NAS usados para la autenticación de abonado basada en AKA, donde el dispositivo está dotado previamente de una clave específica de dispositivo que se usa para la autenticación de dispositivo;

medios para generar una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo; y

medios para usar la clave de seguridad para dotar de seguridad a las comunicaciones entre el dispositivo (202) y una red de servicio (108).

9. El dispositivo (202) según la reivindicación 8, que comprende además:

medios para almacenar una clave específica de abonado usada para la autenticación de abonado; y

medios para almacenar la clave específica de dispositivo usada para la autenticación de dispositivo.

10. Un procedimiento operativo en una entidad de red (324), que comprende:

realizar (906) una autenticación de abonado con un dispositivo (202) en base a un intercambio de acuerdo de autenticación de claves, AKA, entre el dispositivo y la entidad de red, llevada a cabo en mensajes de estrato de no acceso, NAS;

realizar (908) una autenticación de dispositivo del dispositivo (202), llevada a cabo en los mismos mensajes NAS usados para la autenticación de abonado basada en AKA, donde el dispositivo (202) está dotado previamente de una clave específica de dispositivo que se usa para la autenticación de dispositivo;

generar (910) una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo; y

usar (912) la clave de seguridad para dotar de seguridad a las comunicaciones entre la entidad de red (324) y el dispositivo (202).

11. El procedimiento según la reivindicación 10, en el que la autenticación de dispositivo incluye:

recibir un certificado desde el dispositivo (202);

verificar que el certificado asociado al dispositivo (202) no ha sido revocado.

12. El procedimiento según la reivindicación 10, que comprende además:

recibir una solicitud de conexión desde el dispositivo (202), incluyendo la solicitud de conexión una indicación de las capacidades de autenticación de dispositivo del dispositivo (202).

13. El procedimiento según la reivindicación 10, en el que se dota de seguridad a la autenticación de dispositivo mediante al menos una clave generada durante la autenticación de abonado.

14. Una entidad de red (324), que comprende

medios para realizar una autenticación de abonado con un dispositivo (202) en base a un intercambio de acuerdo de autenticación de claves, AKA, entre el dispositivo y la entidad de red, llevada a cabo en mensajes de estrato de no acceso, NAS;

medios para realizar una autenticación de dispositivo del dispositivo (202), llevada a cabo en los mismos mensajes NAS usados para la autenticación de abonado basada en AKA, donde el dispositivo (202) está dotado previamente de una clave específica de dispositivo que se usa para la autenticación de dispositivo;

medios para generar una clave de seguridad que vincula la autenticación de abonado y la autenticación de dispositivo; y

medios para usar la clave de seguridad para dotar de seguridad a las comunicaciones entre la entidad de red (324) y el dispositivo (202).

15. Un medio legible por procesador que comprende instrucciones que, cuando se ejecutan por un procesador, hacen que el procesador lleve a cabo las etapas de procedimiento de cualquiera de las reivindicaciones 1 a 7 y 10 a 13.

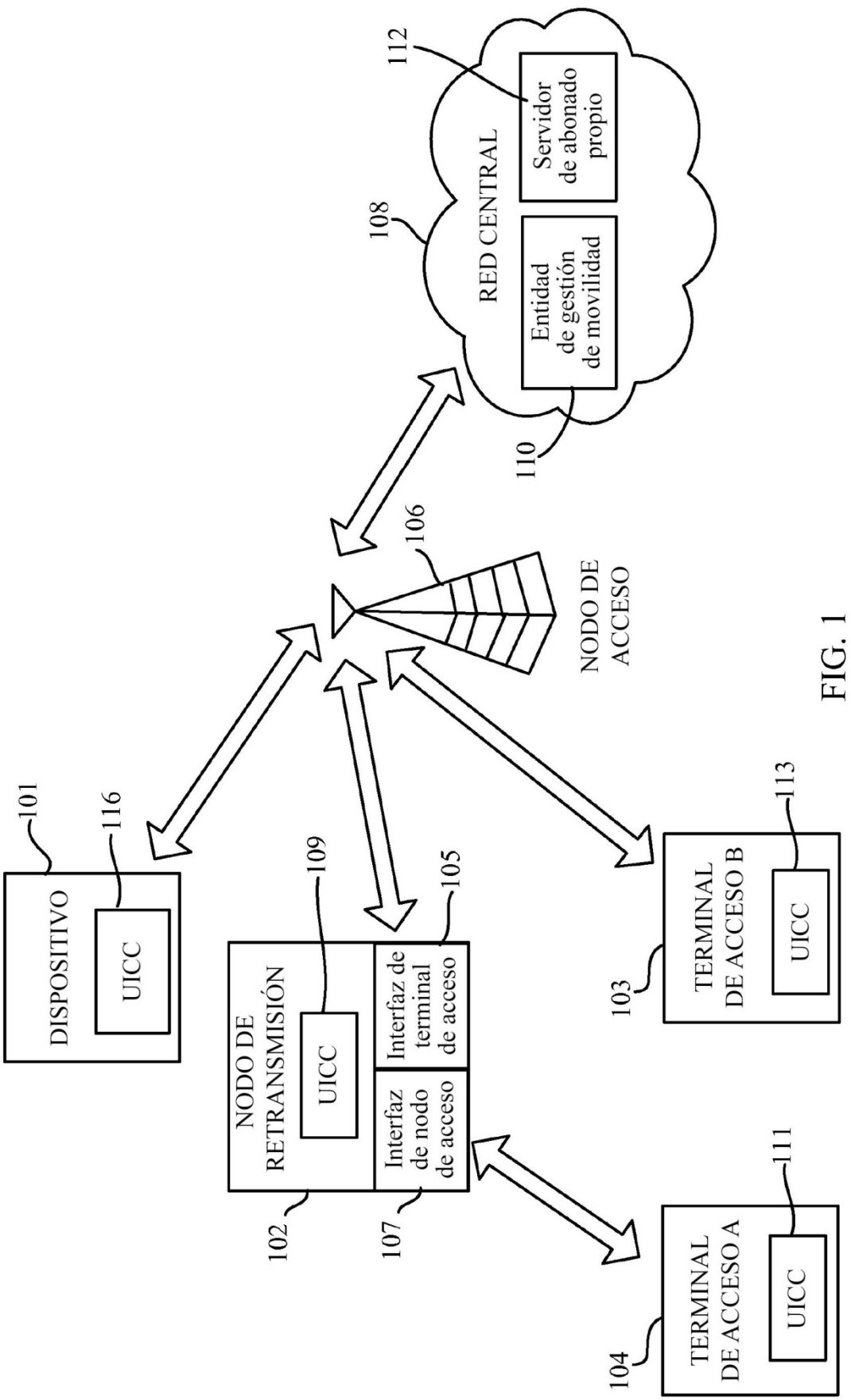
RED CENTRAL
Servidor de abonado propio
Entidad de gestión de movilidad
112
108
110
106
NODO DE ACCESO
101
DISPOSITIVO
116
UICC
109
NODO DE RETRANSMISIÓN
UICC
102
105
Interfaz de terminal de acceso
107
Interfaz de nodo de acceso
103
TERMINAL DE ACCESO B
UICC
113
104
TERMINAL DE ACCESO A
UICC
111

FIG. 1

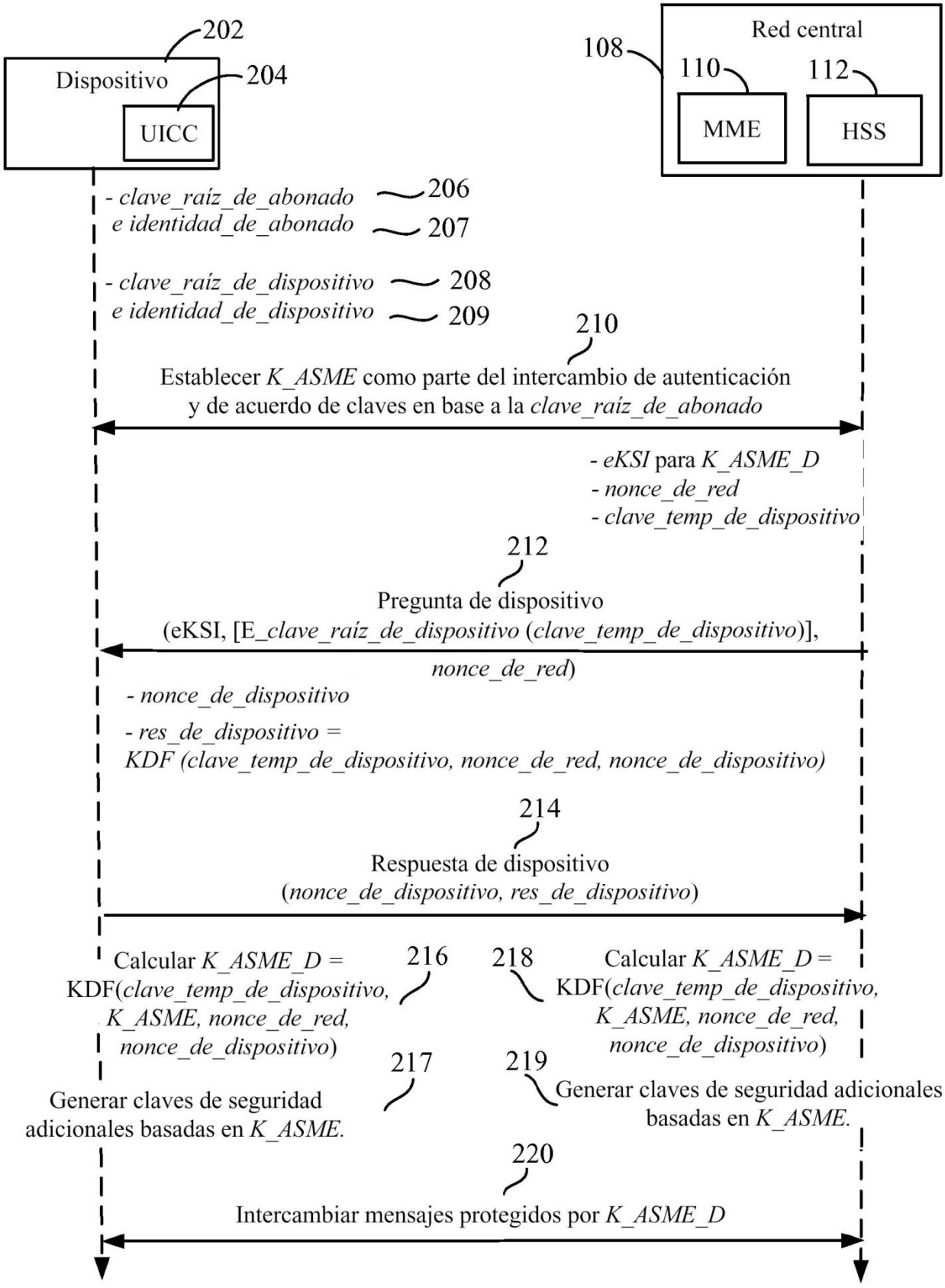
202
Dispositivo
204
UICC
Red central
108
110
112
MME
HSS
- clave_raíz_de_abonado
206
e identidad_de_abonado
207
- clave_raíz_de_dispositivo
208
e identidad_de_dispositivo
209
210
Establecer K_ASME como parte del intercambio de autenticación y de acuerdo de claves en base a la clave_raíz_de_abonado
- eKSI para K_ASME_D
- nonce_de_red
- clave_temp_de_dispositivo
212
Pregunta de dispositivo
(eKSI, [E_clave_raíz_de_dispositivo (clave_temp_de_dispositivo)], nonce_de_red)
- nonce_de_dispositivo
- res_de_dispositivo = KDF (clave_temp_de_dispositivo, nonce_de_red, nonce_de_dispositivo)
214
Respuesta de dispositivo
(nonce_de_dispositivo, res_de_dispositivo)
Calcular K_ASME_D = KDF(clave_temp_de_dispositivo, K_ASME, nonce_de_red, nonce_de_dispositivo)
216
218
Calcular K_ASME_D = KDF(clave_temp_de_dispositivo, K_ASME, nonce_de_red, nonce_de_dispositivo)
217
Generar claves de seguridad adicionales basadas en K_ASME.
219
Generar claves de seguridad adicionales basadas en K_ASME.
220
Intercambiar mensajes protegidos por K_ASME_D

FIG. 2

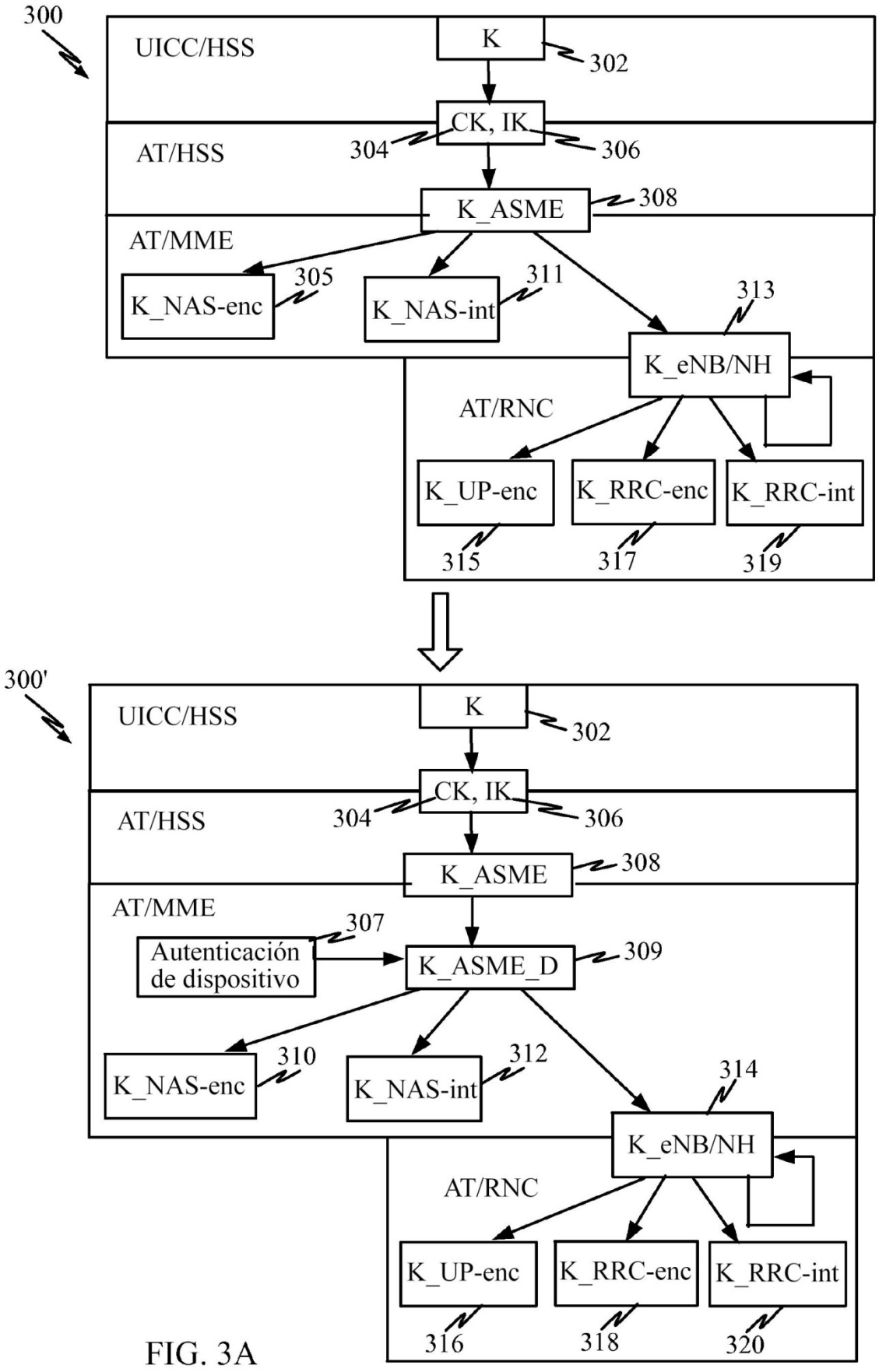
300
UICC/HSS
K
302
CK, IK
304
306
AT/HSS
K_ASME
308
AT/MME
K_NAS-enc
305
K_NAS-int
311
313
K_eNB/NH
AT/RNC
K_UP-enc
K_RRC-enc
K_RRC-int
315
317
319
300'
UICC/HSS
K
302
CK, IK
304
306
AT/HSS
K_ASME
308
AT/MME
307
Autenticación de dispositivo
K_ASME_D
309
K_NAS-enc
310
K_NAS-int
312
314
K_eNB/NH
AT/RNC
K_UP-enc
K_RRC-enc
K_RRC-int
316
318
320

FIG. 3A

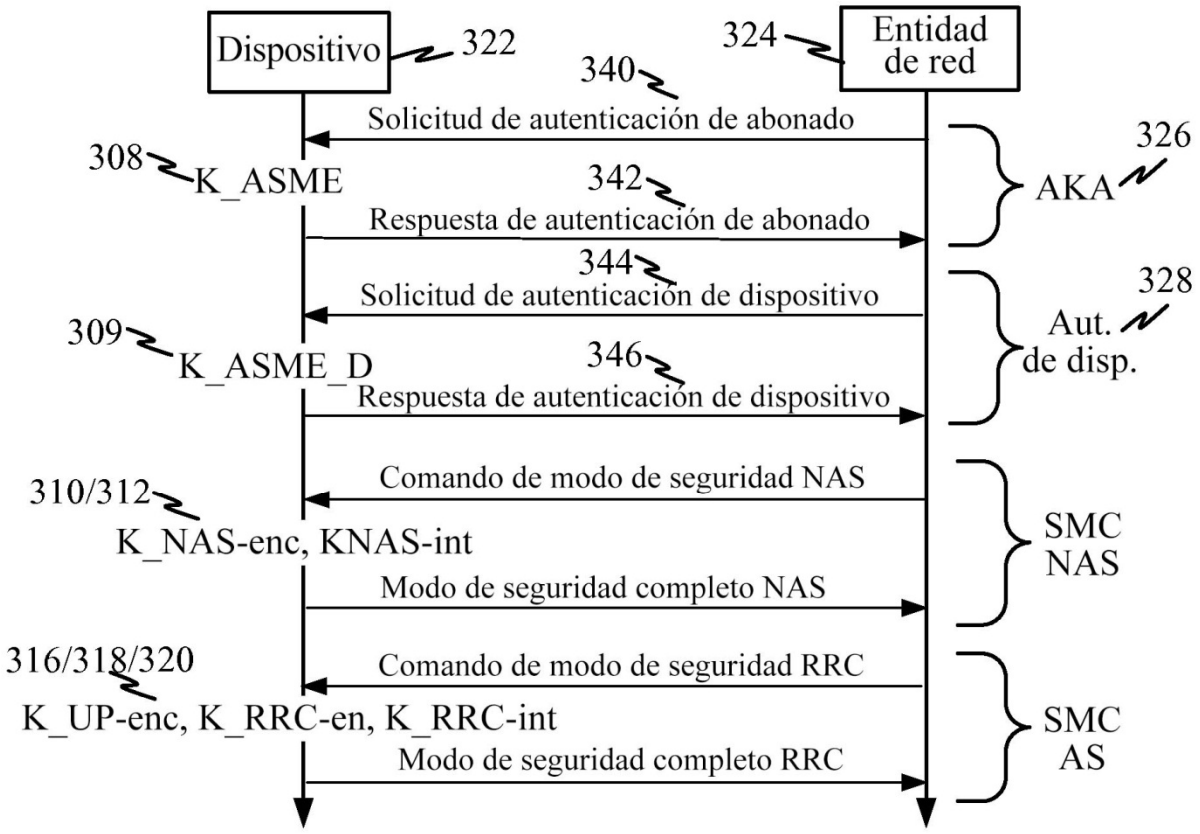
Dispositivo
322
324
Entidad de red
340
Solicitud de autenticación de abonado
326
308
K_ASME
342
AKA
Respuesta de autenticación de abonado
344
328
Solicitud de autenticación de dispositivo
Aut. de disp.
309
K_ASME_D
346
Respuesta de autenticación de dispositivo
Comando de modo de seguridad NAS
310/312
K_NAS-enc, KNAS-int
SMC NAS
Modo de seguridad completo NAS
316/318/320
Comando de modo de seguridad RRC
K_UP-enc, K_RRC-en, K_RRC-int
SMC AS
Modo de seguridad completo RRC

FIG. 3B

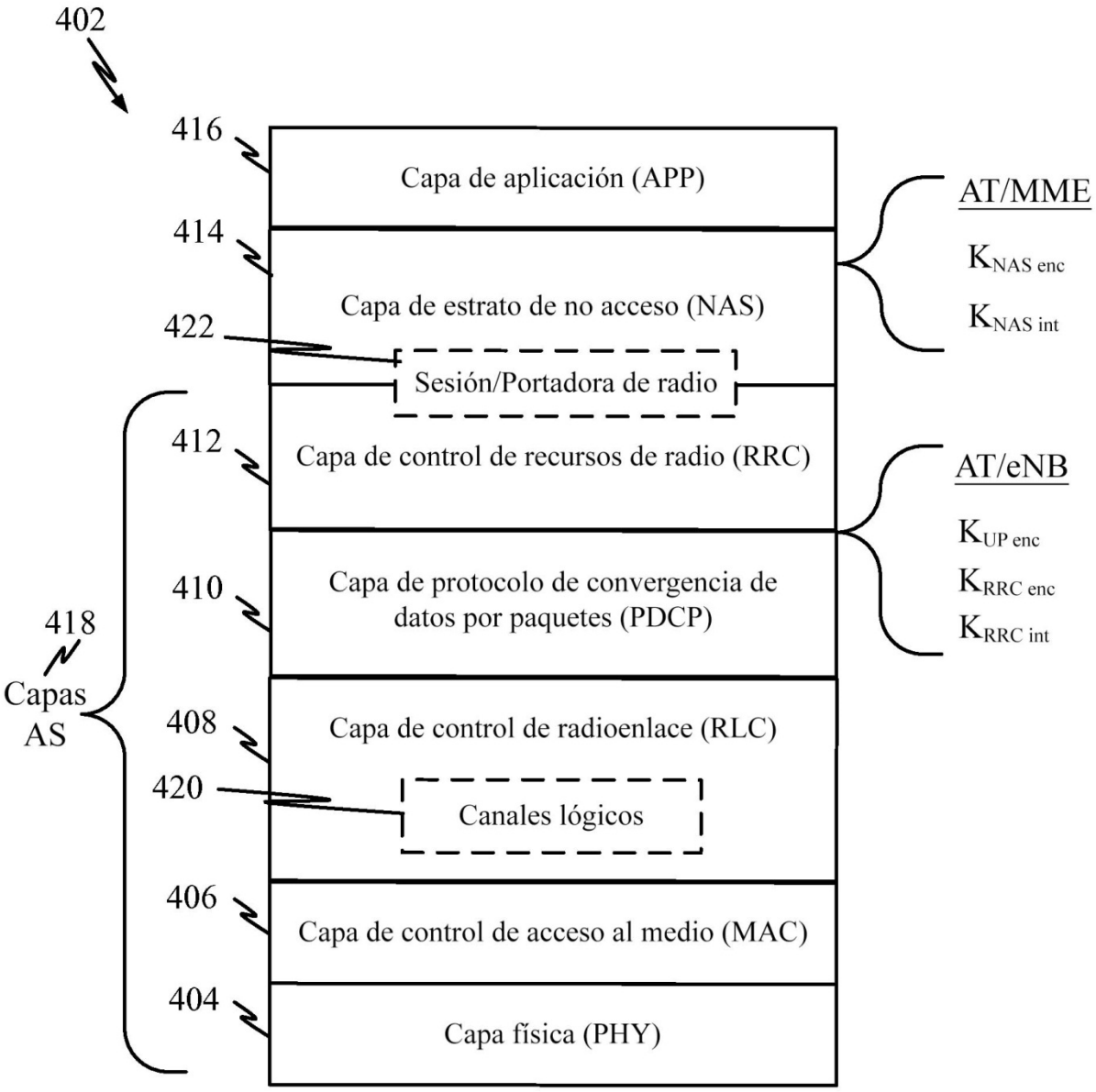
402
416
Capa de aplicación (APP)
414
Capa de estrato de no acceso (NAS)
422
Sesión/Portadora de radio
412
Capa de control de recursos de radio (RRC)
410
Capa de protocolo de convergencia de datos por paquetes (PDCP)
408
Capa de control de radioenlace (RLC)
420
Canales lógicos
406
Capa de control de acceso al medio (MAC)
404
Capa física (PHY)
418
Capas AS
AT/MME
K NAS enc
K NAS int
AT/eNB
K UP enc
K RRC enc
K RRC int

FIG. 4

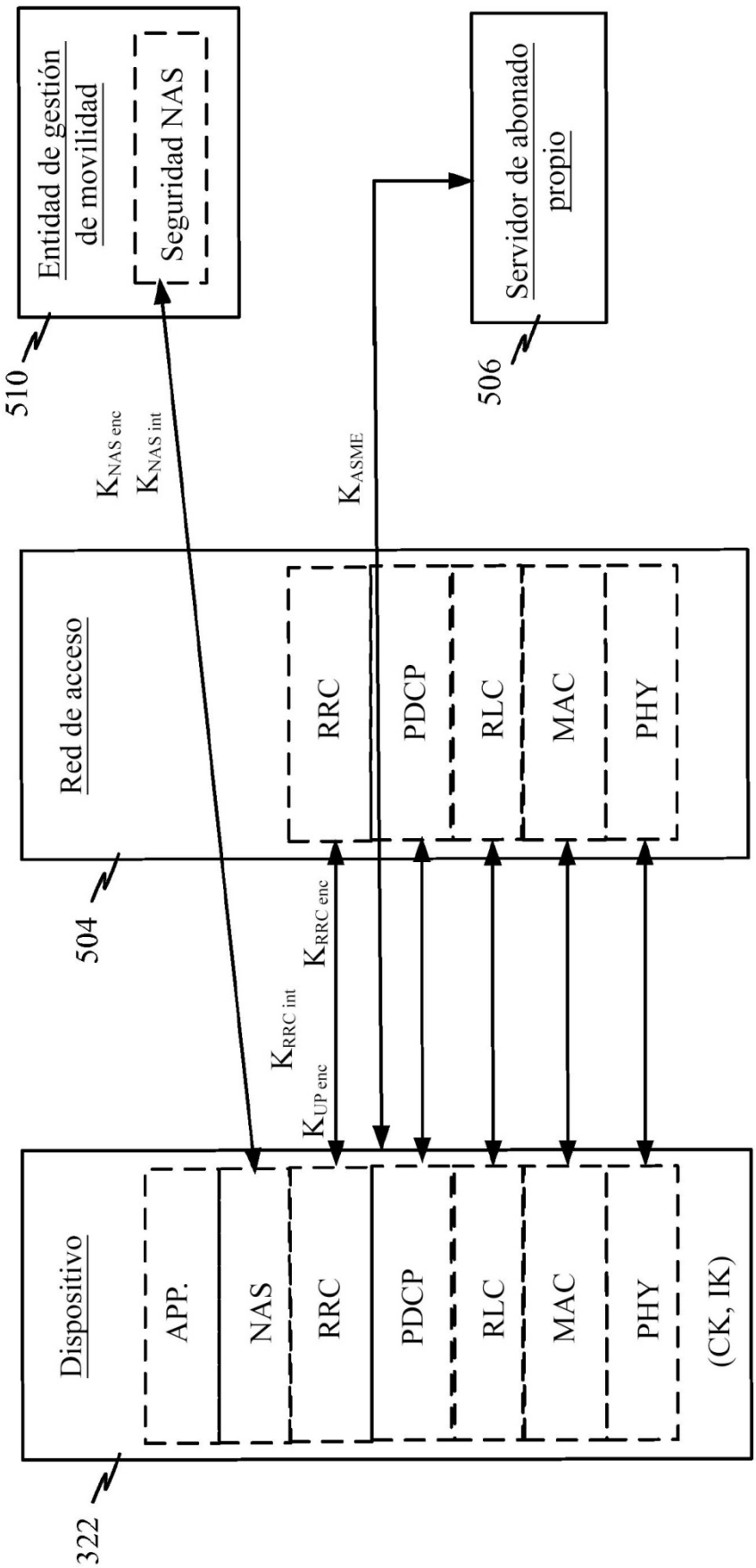
Entidad de gestión de movilidad
Seguridad NAS
510
Servidor de abonado propio
506
$K_{NAS\ enc}$
$K_{NAS\ int}$
K_{ASME}
Red de acceso
RRC
PDCP
RLC
MAC
PHY
504
$K_{RRC\ int}$
$K_{RRC\ enc}$
$K_{UP\ enc}$
Dispositivo
APP.
NAS
RRC
PDCP
RLC
MAC
PHY
(CK, IK)
322

FIG. 5

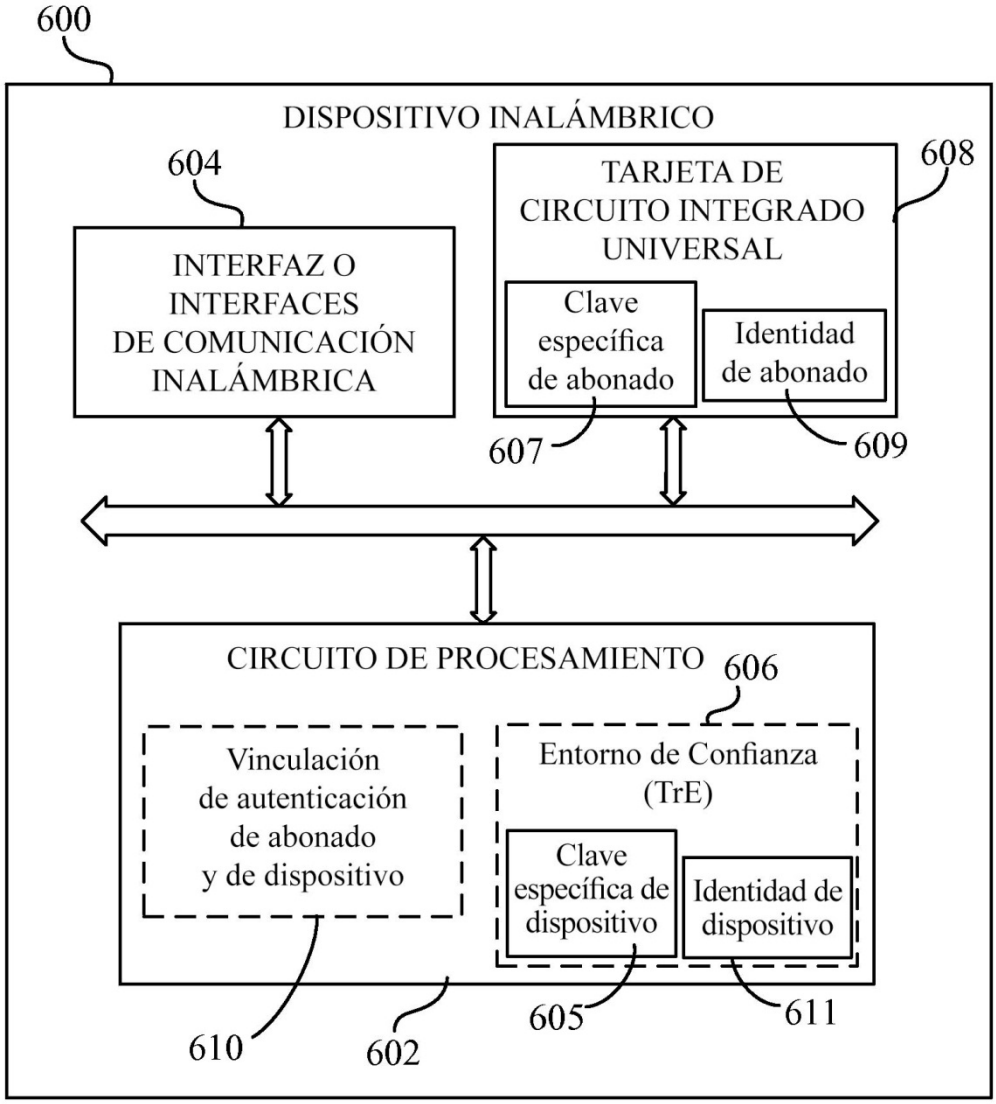
600
DISPOSITIVO INALÁMBRICO
604
INTERFAZ O INTERFACES DE COMUNICACIÓN INALÁMBRICA
608
TARJETA DE CIRCUITO INTEGRADO UNIVERSAL
Clave específica de abonado
Identidad de abonado
607
609
CIRCUITO DE PROCESAMIENTO
606
Vinculación de autenticación de abonado y de dispositivo
Entorno de Confianza (TrE)
Clave específica de dispositivo
Identidad de dispositivo
610
602
605
611

FIG. 6

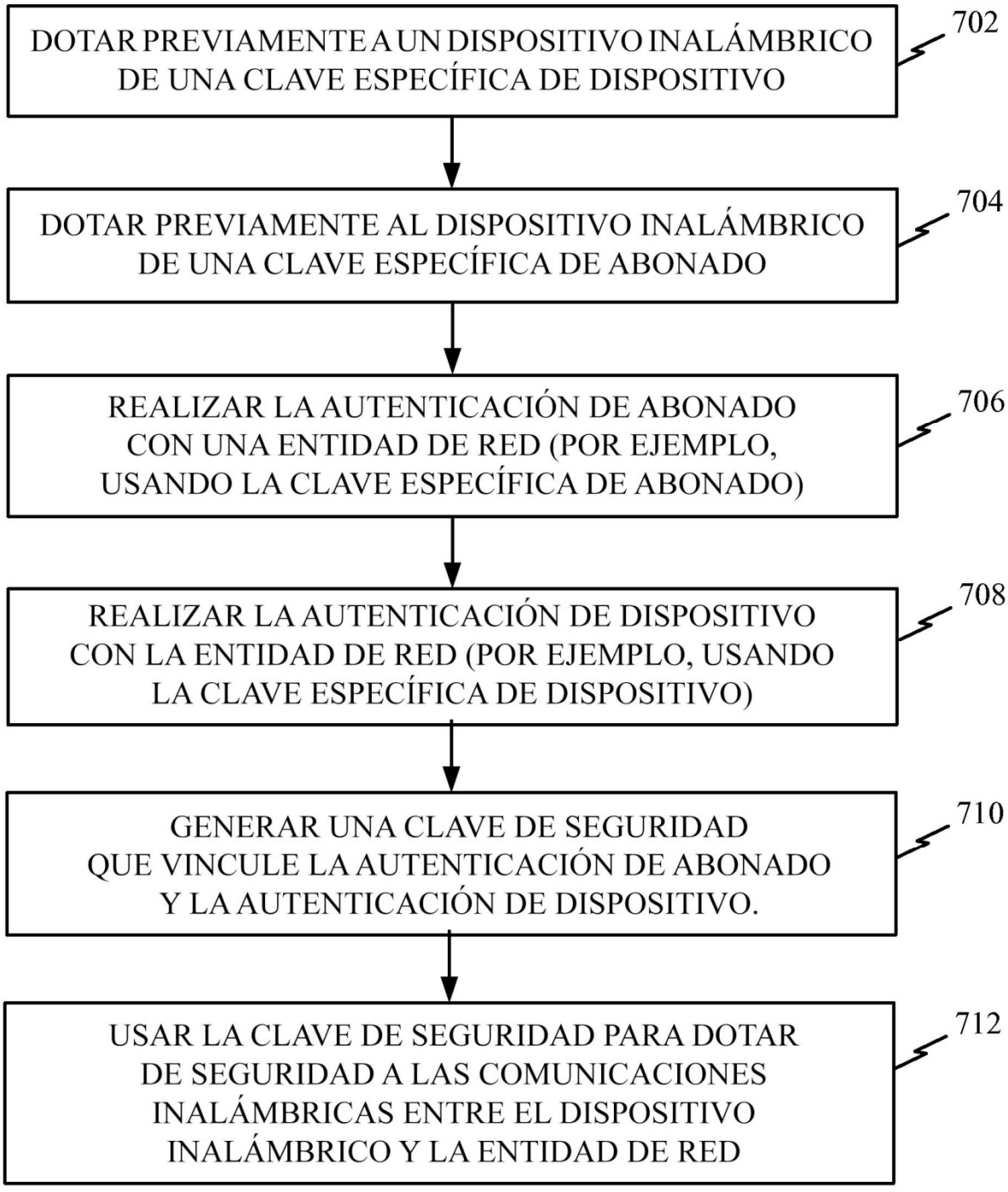
DOTAR PREVIAMENTE A UN DISPOSITIVO INALÁMBRICO DE UNA CLAVE ESPECÍFICA DE DISPOSITIVO
702
DOTAR PREVIAMENTE AL DISPOSITIVO INALÁMBRICO DE UNA CLAVE ESPECÍFICA DE ABONADO
704
REALIZAR LA AUTENTICACIÓN DE ABONADO CON UNA ENTIDAD DE RED (POR EJEMPLO, USANDO LA CLAVE ESPECÍFICA DE ABONADO)
706
REALIZAR LA AUTENTICACIÓN DE DISPOSITIVO CON LA ENTIDAD DE RED (POR EJEMPLO, USANDO LA CLAVE ESPECÍFICA DE DISPOSITIVO)
708
GENERAR UNA CLAVE DE SEGURIDAD QUE VINCULE LA AUTENTICACIÓN DE ABONADO Y LA AUTENTICACIÓN DE DISPOSITIVO.
710
USAR LA CLAVE DE SEGURIDAD PARA DOTAR DE SEGURIDAD A LAS COMUNICACIONES INALÁMBRICAS ENTRE EL DISPOSITIVO INALÁMBRICO Y LA ENTIDAD DE RED
712

FIG. 7

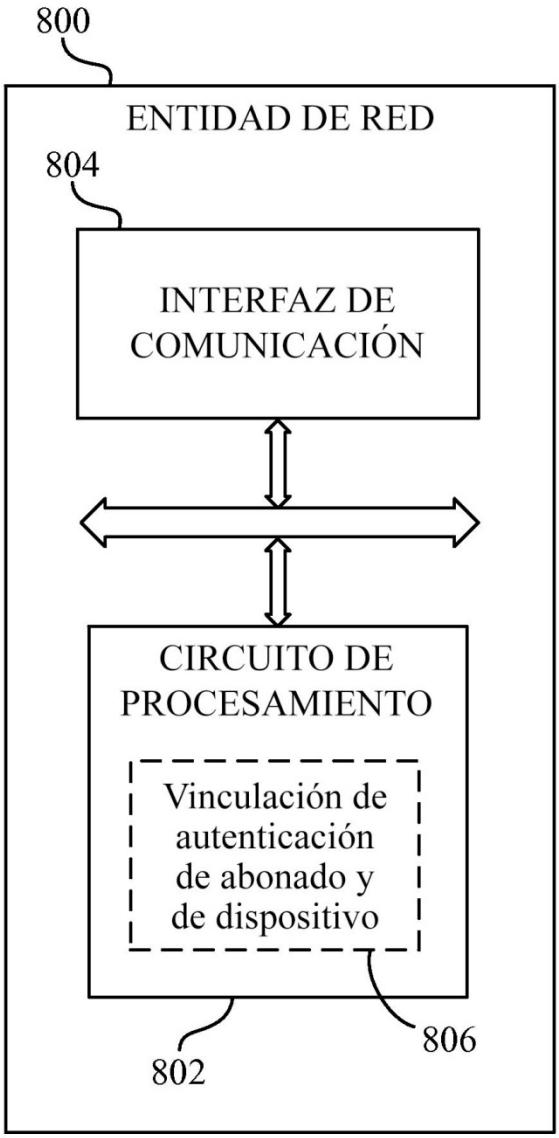
800
ENTIDAD DE RED
804
INTERFAZ DE COMUNICACIÓN
CIRCUITO DE PROCESAMIENTO
Vinculación de autenticación de abonado y de dispositivo
802
806

FIG. 8

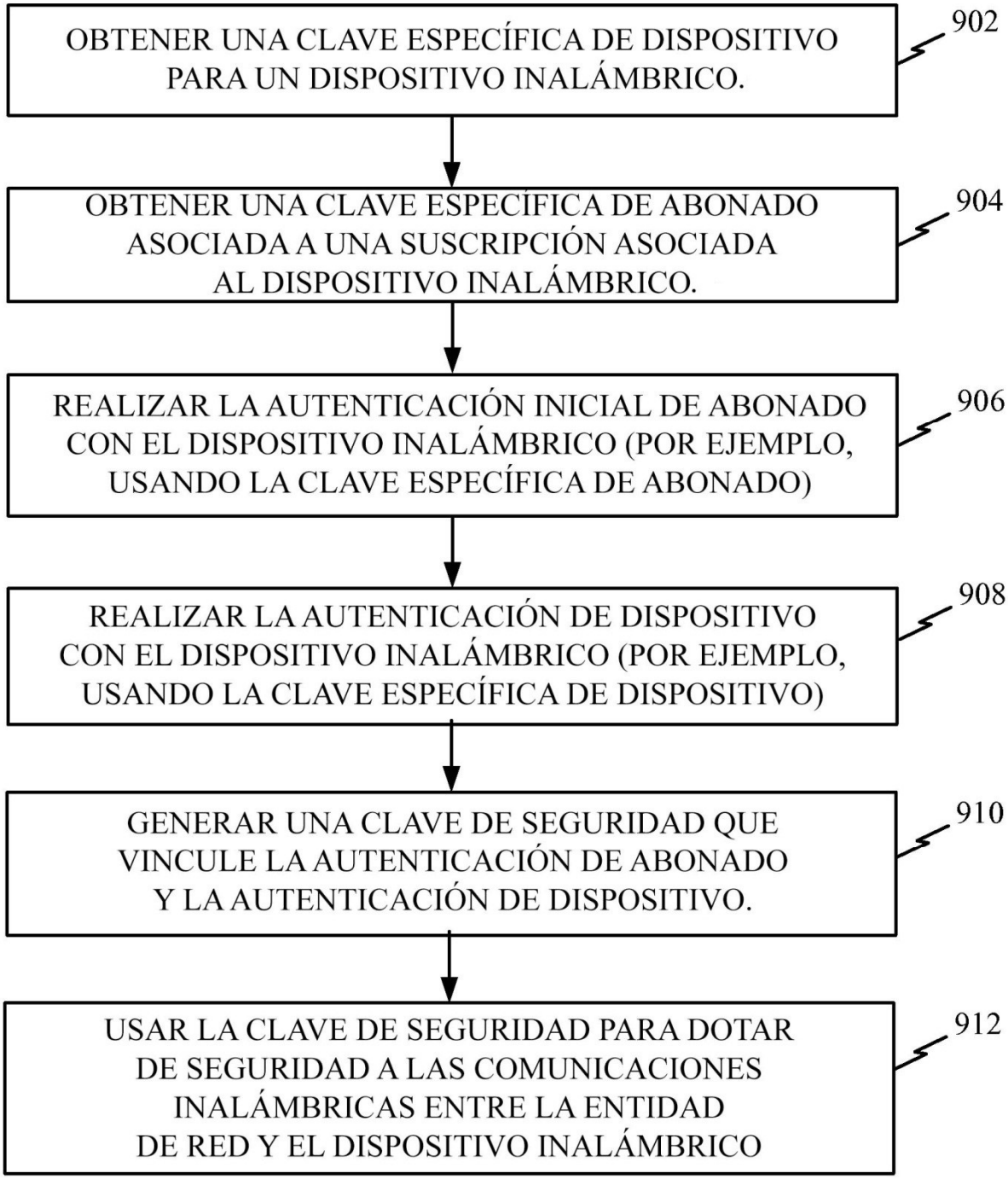
OBTENER UNA CLAVE ESPECÍFICA DE DISPOSITIVO PARA UN DISPOSITIVO INALÁMBRICO.
902
OBTENER UNA CLAVE ESPECIFICA DE ABONADO ASOCIADA A UNA SUSCRIPCIÓN ASOCIADA AL DISPOSITIVO INALÁMBRICO.
904
REALIZAR LA AUTENTICACIÓN INICIAL DE ABONADO CON EL DISPOSITIVO INALÁMBRICO (POR EJEMPLO, USANDO LA CLAVE ESPECÍFICA DE ABONADO)
906
REALIZAR LA AUTENTICACIÓN DE DISPOSITIVO CON EL DISPOSITIVO INALÁMBRICO (POR EJEMPLO, USANDO LA CLAVE ESPECÍFICA DE DISPOSITIVO)
908
GENERAR UNA CLAVE DE SEGURIDAD QUE VINCULE LA AUTENTICACIÓN DE ABONADO Y LA AUTENTICACIÓN DE DISPOSITIVO.
910
USAR LA CLAVE DE SEGURIDAD PARA DOTAR DE SEGURIDAD A LAS COMUNICACIONES INALÁMBRICAS ENTRE LA ENTIDAD DE RED Y EL DISPOSITIVO INALÁMBRICO
912

FIG. 9

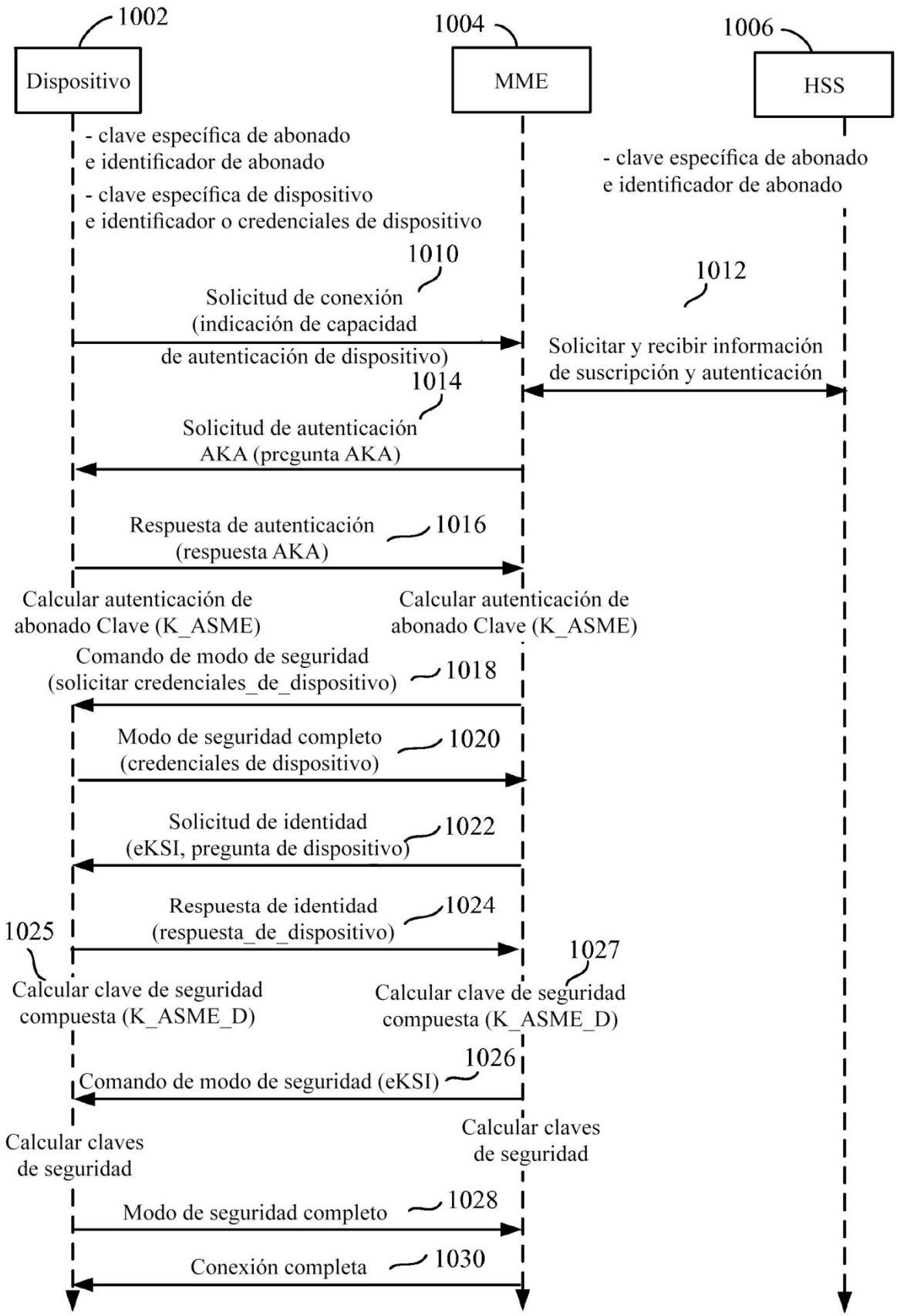
1002
Dispositivo
1004
MME
1006
HSS
- clave específica de abonado
e identificador de abonado
- clave específica de dispositivo
e identificador o credenciales de dispositivo
- clave específica de abonado
e identificador de abonado
1010
Solicitud de conexión
(indicación de capacidad
de autenticación de dispositivo)
1012
Solicitar y recibir información
de suscripción y autenticación
1014
Solicitud de autenticación
AKA (pregunta AKA)
Respuesta de autenticación
(respuesta AKA)
1016
Calcular autenticación de
abonado Clave (K_ASME)
Calcular autenticación de
abonado Clave (K_ASME)
Comando de modo de seguridad
(solicitar credenciales_de_dispositivo)
1018
Modo de seguridad completo
(credenciales de dispositivo)
1020
Solicitud de identidad
(eKSI, pregunta de dispositivo)
1022
Respuesta de identidad
(respuesta_de_dispositivo)
1024
1025
Calcular clave de seguridad
compuesta (K_ASME_D)
1027
Calcular clave de seguridad
compuesta (K_ASME_D)
1026
Comando de modo de seguridad (eKSI)
Calcular claves
de seguridad
Calcular claves
de seguridad
Modo de seguridad completo
1028
Conexión completa
1030

FIG. 10

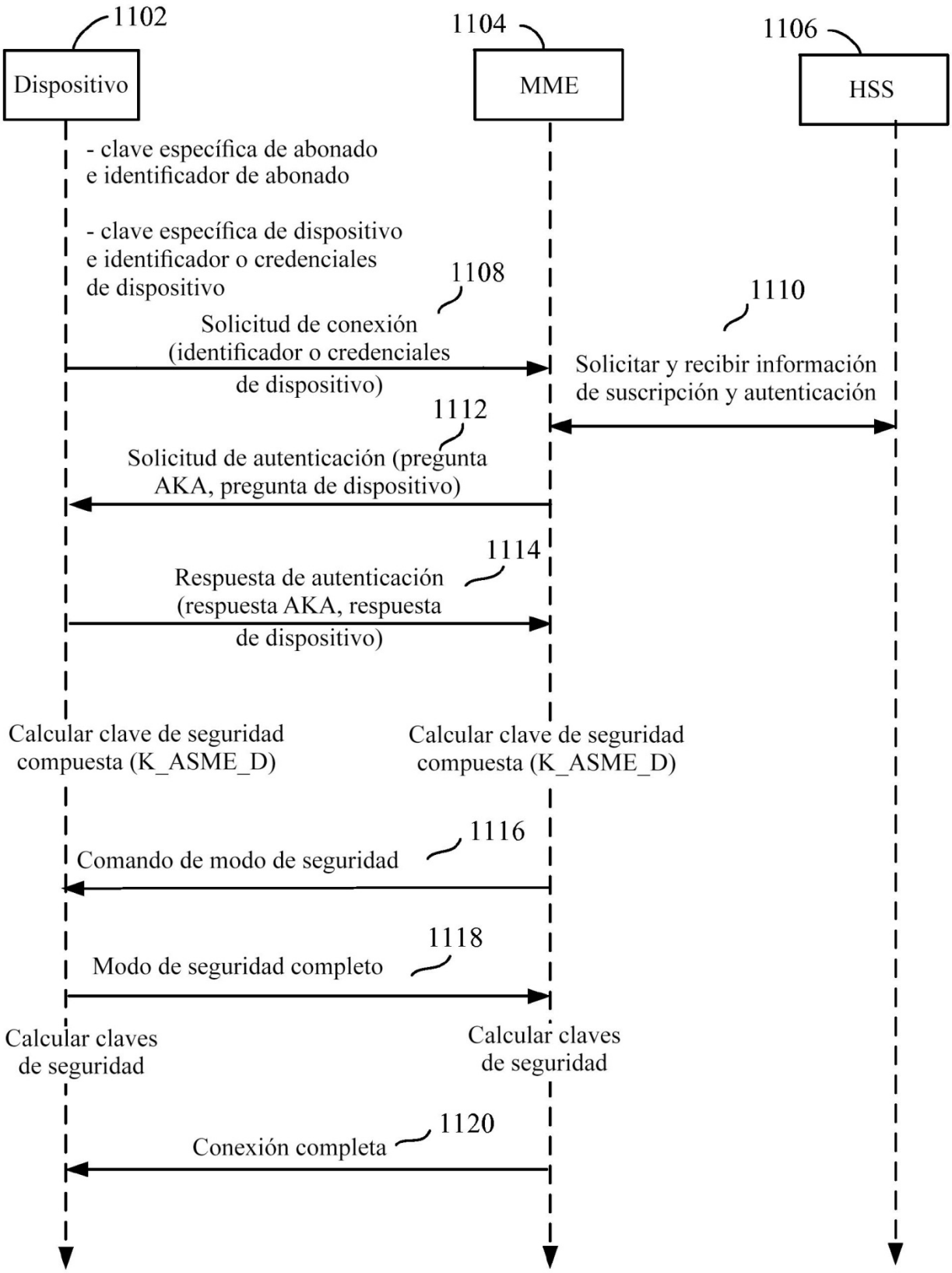
1102
Dispositivo
1104
MME
1106
HSS
- clave específica de abonado e identificador de abonado
- clave específica de dispositivo e identificador o credenciales de dispositivo
1108
Solicitud de conexión (identificador o credenciales de dispositivo)
1110
Solicitar y recibir información de suscripción y autenticación
1112
Solicitud de autenticación (pregunta AKA, pregunta de dispositivo)
1114
Respuesta de autenticación (respuesta AKA, respuesta de dispositivo)
Calcular clave de seguridad compuesta (K_ASME_D)
Calcular clave de seguridad compuesta (K_ASME_D)
1116
Comando de modo de seguridad
1118
Modo de seguridad completo
Calcular claves de seguridad
Calcular claves de seguridad
1120
Conexión completa

FIG. 11

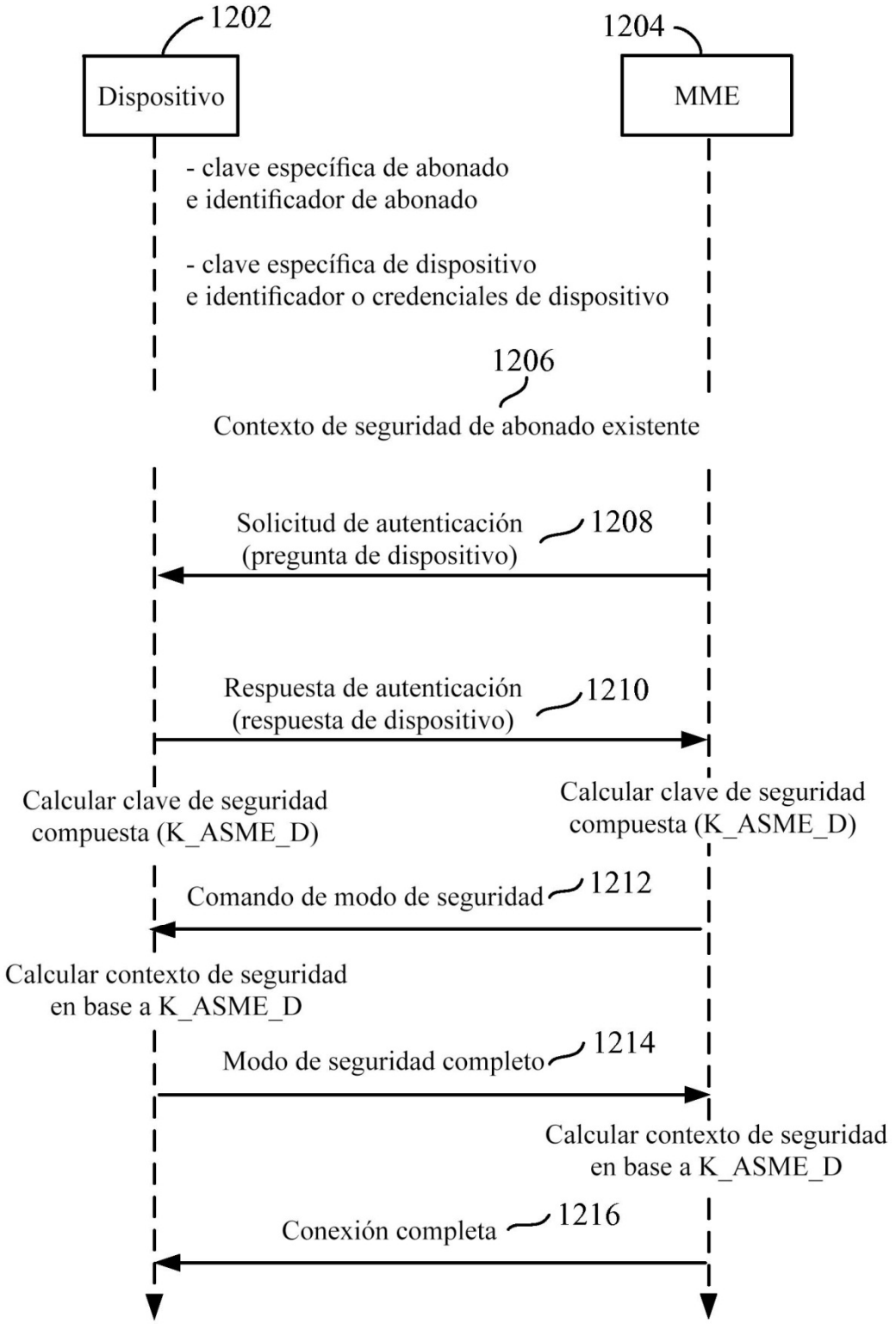
1202
Dispositivo
1204
MME
- clave específica de abonado
e identificador de abonado
- clave específica de dispositivo
e identificador o credenciales de dispositivo
1206
Contexto de seguridad de abonado existente
Solicitud de autenticación
(pregunta de dispositivo)
1208
Respuesta de autenticación
(respuesta de dispositivo)
1210
Calcular clave de seguridad
compuesta (K_ASME_D)
Calcular clave de seguridad
compuesta (K_ASME_D)
Comando de modo de seguridad
1212
Calcular contexto de seguridad
en base a K_ASME_D
Modo de seguridad completo
1214
Calcular contexto de seguridad
en base a K_ASME_D
Conexión completa
1216

FIG. 12