(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 881 632**

(51) Int. CI.:

H04W 12/06 (2011.01)
H04W 12/04 (2011.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
G06F 21/60 (2013.01)
H04L 29/06 (2006.01)
H04W 12/10 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.07.2015 PCT/SE2015/050822**

(87) Fecha y número de publicación internacional: **01.09.2016 WO16137374**

(96) Fecha de presentación y número de la solicitud europea: **13.07.2015 E 15883516 (5)**

(97) Fecha y número de publicación de la concesión europea: **02.06.2021 EP 3262861**

(54) Título: **Disposiciones de seguridad en la comunicación entre un dispositivo de comunicación y un dispositivo de red**

(30) Prioridad:

27.02.2015 US 201562121689 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.11.2021

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

NÄSLUND, MATS;
SAHLIN, BENGT;
NORRMAN, KARL y
ARKKO, JARI

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Disposiciones de seguridad en la comunicación entre un dispositivo de comunicación y un dispositivo de red

Campo técnico

La invención se refiere a un dispositivo de comunicación para comunicarse con un dispositivo de red, un método, un programa informático y un producto de programa informático para un dispositivo de comunicación en comunicación con un dispositivo de red de una red de comunicación, un primer dispositivo de red de una primera red de comunicación, un método, programa informático y producto de programa informático para un primer nodo de red de una primera red de comunicación así como para un sistema que comprende un primer dispositivo de red en un primer sistema de comunicación y un segundo dispositivo de red en un segundo sistema de comunicación. La invención también se refiere al segundo dispositivo de red.

Antecedentes

Los datos transferidos a través de las redes de comunicación son cada vez más sensibles. Las redes de comunicación, tales como las redes de comunicación móviles, inalámbricas y fijas, se usan hoy en día cada vez con más frecuencia para, por ejemplo, diversas transacciones económicas y comerciales, control de sistemas ciberfísicos, etc. Por lo tanto, son necesarias medidas de seguridad más estrictas.

Por ejemplo, en las comunicaciones móviles, es importante que la red de comunicación y el equipo de usuario (en inglés, User Equipment, UE) se autentiquen mutuamente y puedan cifrar los datos de tráfico intercambiados, donde ambos servicios de seguridad son dependientes críticamente de la gestión de claves segura, que incluye el acuerdo de claves o el establecimiento de claves.

A este respecto, las redes móviles de la segunda generación (en inglés, second generation, 2G) en adelante, han hecho uso de un acuerdo de claves de cifrado y autenticación fuerte basado en tarjetas de módulo de identidad de abonado universal (en inglés, (Universal) Subscriber Identity Module, (U)SIM). Desde las redes de tercera generación (en inglés, third generation, 3G) en adelante, la autenticación ha sido mutua: tanto la red como el equipo de usuario se autentican entre sí. La autenticación 3G/4G basada en el módulo de identidad de abonado universal (en inglés, Universal Subscriber Identity Module, USIM) se describe en, por ejemplo, la especificación técnica TS 33.102 V12.2.0 y la especificación técnica TS 33.401 V12.13.0 de 3GPP. El protocolo se conoce como acuerdo de claves y autenticación (en inglés, Authentication and Key Agreement, AKA) de UMTS o AKA de LTE, que depende de qué tipo de red de acceso se use, donde AKA de UMTS es un acrónimo para autenticación y acuerdo de claves de un sistema de telecomunicación móvil universal (en inglés, Universal Mobile Telecommunication System Authentication and Key Agreement, UMTS AKA) y AKA de LTE es un acrónimo para autenticación y acuerdo de claves de evolución a largo plazo (en inglés, Long Term Evolution Authentication and Key Agreement, AKA LTE). Como nota, mientras los estándares de 3GPP usan el término acuerdo de claves, los protocolos usados en realidad son más bien de naturaleza establecimiento de claves. Sin embargo, la diferencia no es importante para el análisis. Se han desarrollado variantes de este protocolo AKA para subsistemas de multimedia IP (en inglés, IP Multimedia Subsystem, IMS), AKA de IMS, tecnologías de acceso que no son de 3GPP (EAP-AKA, IETF RFC 4187) y para autenticación de capa de servicio general (Arquitectura de arranque genérico (en inglés, Generic Bootstrapping Architecture, GBA), en la especificación técnica TS 33.220 V12 .3.0 de 3GPP).

La Fig. 1 muestra el funcionamiento de AKA a alto nivel para una red de 3G según la especificación técnica TS 33.102 V12.2.0, donde una estación móvil (en inglés, Mobile Station, MS), que es un tipo de dispositivo de comunicación que corresponde a un equipo de usuario, se comunica con un registro de ubicación visitante (en inglés, Visiting Location Register, VLR)/nodo de soporte de pasarela de servicio (en inglés, Servicing Gateway Support Node, SGSN) de una red de servicio (en inglés, Servicing Network, SN), que a su vez se comunica con un entorno doméstico (en inglés, Home Environment, HE)/registro de ubicación de inicio (en inglés, Home Location Register, HLR). En 4G/LTE, una entidad de gestión de la movilidad (en inglés, Mobile Management Entity, MME) que sustituye a VLR/SGSN y HE/HLR corresponde al servidor de abonado doméstico (en inglés, Home Subscriber Server, HSS).

En la Fig. 1, el VLR/SGSN se muestra enviando 10 una solicitud de datos de autenticación al HE/HLR con respecto a una estación móvil (en inglés, Mobile Station, MS) visitante. El HE/HLR genera 12 un conjunto de vectores de autenticación (AV(1..n)) y envía 14 los vectores (AV1..n) al VLR/SGSN en un mensaje de respuesta de datos de autenticación, donde el VLR/SGSN luego almacena 16 los vectores de autenticación. Estas etapas aquí juntas forman una fase 17 de distribución y vectores de autenticación del HE.

A continuación sigue una fase 31 de autenticación y establecimiento de claves (o acuerdo de claves). Cuando la autenticación va a tener lugar en esta fase 31, el VLR/SGSN selecciona 18 un vector de autenticación disponible (no usado) y, basado en el contenido de este vector, envía un mensaje 20 de solicitud de autenticación de usuario ARQ que comprende un desafío que usa un valor aleatorio RAND(i) y un testigo (en inglés, token) de autenticación AUTN(i), donde AUTN(i) comprende un código de verificación del desafío, y el índice i indica que el valor está asociado con AV_i. El AUTN(i) se verifica en la MS y, si la verificación tiene éxito, se calcula 22 un resultado RES(i) en una etapa de verificación. Para ser precisos, estas operaciones las lleva a cabo el USIM en la MS. La MS luego envía un mensaje 20 de respuesta de autenticación de usuario (ARE) que comprende el resultado RES(i). El vector de autenticación

comprende el resultado esperado XRES(i) y el VLR/SGSN luego compara 26 el resultado recibido RES(i) con el resultado esperado XRES(i), y si la comparación fue exitosa (es decir, los dos valores son iguales), el VLR/SGSN luego selecciona 30 una clave de cifrado CK(i) y una clave de protección de integridad IK(i) correspondientes. Al mismo tiempo, la MS (de nuevo, para ser precisos, el USIM) calcula 28 las mismas claves CK(i) e IK(i). En el caso de LTE, otras claves se derivan de CK(i) e IK(i), por ejemplo, una así llamada clave de entidad de gestión de la seguridad del acceso a las claves (en inglés, Key Access Security Management Entity, Kasme) (no mostrada), esta derivación se hace en la parte de la MS que está fuera del USIM. Esta parte fuera del USIM se conoce como equipo móvil (en inglés, Mobile Equipment, ME).

En una autenticación y acuerdo de claves del tipo mostrado en la fig. 1 y descrito anteriormente, una clave secreta K, con ventaja compartida previamente, se usa y almacena tanto en el equipo de usuario (específicamente, en el USIM) como en la red doméstica. La clave compartida K luego se usa para derivar CK(i) e IK(i).

Por tanto, la seguridad de AKA depende de que la clave K se mantenga en secreto. Recientemente, se informó en los medios de comunicación que se había violado la seguridad de un fabricante de tarjetas USIM y que un conjunto de claves K se había "filtrado" (o caído en manos equivocadas), poniendo, por tanto, a los abonados asociados con estas claves en riesgos, tales como la suplantación de identidad, secuestro de conexiones, y escuchas clandestinas (ya que también las claves de cifrado, derivadas de CK(i) y/o IK(i), también están, por tanto, potencialmente en riesgo). En el artículo, https://firstlook.org/theintercept/2015/02/19/great-sim-heist/, recuperado el 6 de julio de 2015, se mencionó que un problema potencial con el protocolo AKA, que conduce a las implicaciones de seguridad antes mencionadas, residía en que AKA carece del así llamado secreto perfecto hacia adelante (en inglés, Perfect Forward Secrecy, PFS).

En vista de lo que se ha descrito anteriormente, es de interés elevar el nivel de seguridad de la comunicación entre un dispositivo de comunicación y una red de comunicación cuando la seguridad se basa en módulos de identidad tal como USIM que hace uso de un secreto/clave compartida con un nodo de red de comunicación.

Por tanto, es necesario mejorar la seguridad de la comunicación entre un dispositivo de comunicaciones y una red de comunicación.

El documento US-2006/0205388-A1 describe un método de autenticación mutua entre una función de servidor de arranque (en inglés, Bootstrapping Server Function, BSF) y un terminal móvil que admite, por ejemplo, el sistema global para comunicaciones móviles (en inglés, Global System for Mobile Communication, GSM), pero no AKA de 3G. La BSF genera un exponente secreto aleatorio x y calcula una clave pública Diffie-Hellman. El terminal móvil autentica la BSF basado en un certificado de servidor de arranque recibido de antemano.

El documento S40-20050925-006 de 3GGP2 con el título "Simplification of bootstrapping procedures" describe un método para la generación de una clave AKA temporal basada en parámetros Diffie-Hellman. La clave AKA temporal luego se usa como clave básica para la generación de CK, IK y RES.

El documento US-2007/0192602-A1 describe una solución destinada a mitigar los riesgos de seguridad en caso de que se filtre la clave compartida K entre un centro de autenticación del entorno doméstico (en inglés, Home Environment Autentication Center, HE/AuC) y un USIM. Se pretende especialmente una protección de clonación mejorada para los módulos de identidad de abonado (en inglés, Subscriber Identity Module, SIM), los módulos de identidad de abonado universal (USIM), y los módulos de identidad de abonado del subsistema de multimedia IP (en inglés, IP Multimedia Subsystem SIM, ISIM). Un método descrito para proporcionar un acceso de módulo de identidad válido a una red, mientras se evita un clon de módulo de identidad no autorizado, incluye un cálculo de un valor $R=g^{xy}$, donde x es una clave privada Diffie-Hellman conocida por el módulo de identidad de acceso.

Compendio

Un objeto de la invención es mejorar la seguridad de la comunicación de un dispositivo de comunicación en relación con el uso de claves compartidas a largo plazo.

Este objeto según un primer aspecto se logra por un dispositivo de comunicación para comunicarse con un dispositivo de red de una red de comunicación. El dispositivo de comunicación está operativo para:

recibir un desafío, un primer parámetro de secreto perfecto hacia adelante, PFS, y un primer código de verificación para el primer parámetro de PFS del dispositivo de red, en donde el primer código de verificación comprende un código de autenticación de mensajes basado en al menos el primer parámetro de PFS;

reenviar el desafío o un derivado del mismo a un módulo de identidad;

recibir al menos un parámetro de resultado como respuesta del módulo de identidad;

determinar, basado en dicho parámetro de resultado, si dicho primer parámetro de PFS es auténtico; y

generar y enviar un segundo parámetro de PFS al dispositivo de red si dicha determinación es que el primer parámetro de PFS es auténtico.

El objeto se logra según un segundo aspecto a través de un método realizado por un dispositivo de comunicación, cuyo dispositivo de comunicación está en comunicación con un dispositivo de red de una red de comunicación.

El método comprende:

recibir un desafío, un primer parámetro de PFS y un primer código de verificación para el primer parámetro de PFS del dispositivo de red, en donde el primer código de verificación comprende un código de autenticación de mensajes basado en al menos el primer parámetro de PFS;

reenviar el desafío o un derivado del mismo a un módulo de identidad, recibir al menos un parámetro de resultado como respuesta del módulo de identidad,

determinar, basado en dicho parámetro de resultado, si dicho primer parámetro de PFS es auténtico, y

generar y enviar un segundo parámetro de PFS al dispositivo de red si dicha determinación es que el primer parámetro de PFS es auténtico.

La invención según el primer y segundo aspecto tiene una serie de ventajas. La seguridad mejorada establece barreras contra los atacantes que pueden comprometer la clave compartida a largo plazo, lo que les obliga a lanzar los así llamados ataques de intermediario (en inglés, man-in-the-middle) para explotar la clave comprometida.

Un derivado puede ser idéntico al desafío. Un derivado también puede ser un hash del desafío.

En una primera variación del primer aspecto, el dispositivo de comunicación está configurado para generar una clave de sesión para la comunicación entre el dispositivo de comunicación y el dispositivo de red, donde la clave de sesión se basa al menos en los valores usados para generar el primer y segundo parámetro de PFS. Esta variación tiene la ventaja de proporcionar una sesión que ha mejorado la seguridad de la comunicación contra potenciales compromisos futuros de la clave compartida.

En una realización más específica del primer aspecto, la clave de sesión se basa en el primer parámetro de PFS y un exponente del segundo parámetro de PFS.

Los parámetros primero y segundo de PFS pueden ser más particularmente parámetros Diffie-Hellman.

En una tercera variación del primer aspecto, el dispositivo de comunicación está operativo para recibir el desafío, el primer parámetro de PFS y el primer código de verificación en un mensaje de solicitud de autenticación del dispositivo de red y en este caso el mensaje de solicitud de autenticación también comprende un código de verificación del desafío. Además, cuando el dispositivo de comunicación recibe el al menos un parámetro de resultado, está operativo para recibir un parámetro de respuesta como una respuesta al desafío. Finalmente, cuando el dispositivo de comunicación está operativo para generar y enviar el segundo parámetro de PFS, está operativo para generar el segundo parámetro de PFS junto con un segundo código de verificación y enviarlos en un mensaje de respuesta de autenticación que también comprende el parámetro de respuesta. Esta variación tiene la ventaja de permitir que el primer y segundo parámetro de PFS y el primer y segundo código de verificación sean transferidos en mensajes ya existentes. De este modo se evitan mensajes adicionales. Esto puede ahorrar energía en el dispositivo de comunicación, lo que puede ser un recurso limitado.

Además, es posible que el dispositivo de comunicación comprenda el módulo de identidad, donde el módulo de identidad a su vez comprende una clave y un medio de procesamiento criptográfico.

Otro objeto es proporcionar seguridad de la comunicación mejorada de un primer dispositivo de red en una red de comunicación en relación con el uso de claves compartidas a largo plazo.

Este objeto se logra según un tercer aspecto a través de un primer dispositivo de red de una primera red de comunicación. El primer dispositivo de red está operativo para:

obtener un desafío;

obtener un primer parámetro de PFS;

obtener un primer código de verificación para el primer parámetro de PFS, en donde el primer código de verificación comprende un código de autenticación de mensajes basado en al menos el primer parámetro de PFS;

enviar el desafío, el primer parámetro de PFS y el primer código de verificación a un dispositivo de comunicación;

recibir un segundo parámetro de PFS, un segundo código de verificación y un parámetro de respuesta del dispositivo de comunicación;

determinar la autenticidad del parámetro de respuesta; y

verificar el segundo parámetro de PFS basado en el segundo código de verificación.

El objeto se logra según un cuarto aspecto a través de un método para un primer dispositivo de red de una primera red de comunicación. El método lo realiza el primer dispositivo de red y comprende:

obtener un desafío;

obtener un primer parámetro de PFS;

obtener un primer código de verificación para el primer parámetro de PFS, en donde el primer código de verificación comprende un código de autenticación de mensajes basado en al menos el primer parámetro de PFS;

enviar el desafío, el primer parámetro de PFS y el primer código de verificación a un dispositivo de comunicación;

recibir un segundo parámetro de PFS, un segundo código de verificación y un parámetro de respuesta del dispositivo de comunicación;

determinar la autenticidad del parámetro de respuesta; y

verificar el segundo parámetro de PFS basado en el segundo código de verificación.

La invención según los aspectos tercero y cuarto mejora la seguridad de la comunicación entre un primer dispositivo de red y un dispositivo de comunicación. La seguridad mejorada establece barreras contra los llamados ataques de intermediario (en inglés, man-in-the-middle).

En una primera variación del tercer aspecto, el primer dispositivo de red también está operativo para calcular una clave de sesión para la comunicación entre el dispositivo de comunicación y el primer dispositivo de red. La clave de sesión se basa al menos en los valores usados para generar el primer y segundo parámetro de PFS.

En una realización más específica del tercer aspecto, la clave de sesión se basa en el segundo parámetro de PFS y un exponente del primer parámetro de PFS.

En una variación del tercer aspecto, el primer dispositivo de red cuando está operativo para obtener el desafío también está operativo para obtener un código de verificación del desafío, cuando está operativo para enviar el desafío, el primer parámetro de PFS y el primer código de verificación está operativo para enviarlos en un mensaje de solicitud de autenticación junto con el código de verificación del desafío y cuando está operativo para recibir el segundo parámetro de PFS, el segundo código de verificación y el parámetro de respuesta está operativo para recibirlos en un mensaje de respuesta de autenticación.

Se debe enfatizar que el término "comprende/que comprende" cuando se usa en esta especificación se toma para especificar la presencia de características, números enteros, etapas o componentes declarados, pero no excluye la presencia o adición de una o más características, números enteros, etapas, componentes o grupos de los mismos. La palabra 'parámetro' debe interpretarse como que abarca los valores del parámetro, por ejemplo, que el cálculo de un parámetro comprende el cálculo de un valor para ese parámetro, y que un cálculo o derivación de un resultado o respuesta basado en uno o más parámetros comprende un cálculo del resultado o la respuesta basado en uno o más valores del uno o más parámetros. De la misma manera, recibir un parámetro y enviar/reenviar un parámetro comprende la recepción y envío de un valor de ese parámetro.

Breve descripción de los dibujos

La invención se describirá ahora con más detalle en relación con los dibujos adjuntos, en los que:

La Fig. 1 muestra esquemáticamente un diagrama de un esquema de autenticación conocido realizado entre un dispositivo de comunicación y una red de comunicación,

La Fig. 2 muestra esquemáticamente una primera y una segunda red de comunicación, así como un dispositivo de comunicación que se comunica con la primera red de comunicación,

La Fig. 3 muestra esquemáticamente el uso de un protocolo Diffie-Hellman entre el dispositivo de comunicación y la primera red de comunicación,

La Fig. 4 muestra un esquema de bloques del equipo de usuario que comprende un módulo de identidad y un equipo móvil,

La Fig. 5 muestra un esquema de bloques del equipo móvil,

La Fig. 6 muestra un esquema de bloques que describe un dispositivo de red, que es aplicable a un dispositivo que actúa como un nodo tanto en la primera como en la segunda red de comunicación,

La Fig. 7 muestra un diagrama de flujo de una serie de etapas del método en un método para mejorar la seguridad de la comunicación de un dispositivo de comunicación según una primera realización y que se realiza en el dispositivo de comunicación,

La Fig. 8 muestra un diagrama de flujo de una serie de etapas del método en un método para un primer dispositivo de red en la primera red de comunicación según la primera realización y que se realiza en el primer dispositivo de red,

La Fig. 9 muestra un diagrama de señalización con señales intercambiadas entre el dispositivo de comunicación, el primer dispositivo de red y un segundo dispositivo de red en la segunda red de comunicación según una segunda realización,

La Fig. 10 muestra un código de verificación del desafío con más detalle,

La Fig. 11 muestra un diagrama de señalización con señales intercambiadas, entre el dispositivo de comunicación, el primer dispositivo de red y el segundo dispositivo de red según una tercera realización,

La Fig. 12 muestra un producto de programa informático que comprende un medio de almacenamiento de datos con un código de programa informático para implementar la funcionalidad del dispositivo de comunicación,

La Fig. 13 muestra un producto de programa informático que comprende un medio de almacenamiento de datos con un código de programa informático para implementar la funcionalidad de un dispositivo de red,

La Fig. 14 muestra otra forma de realizar el dispositivo de comunicación,

La Fig. 15 muestra otra forma de realizar el primer dispositivo de red, y

La Fig. 16 muestra otra forma de realizar el segundo dispositivo de red.

Descripción detallada

En la siguiente descripción, con fines explicativos y no limitativos, se establecen detalles específicos tales como arquitecturas particulares, interfaces, técnicas, etc. para proporcionar una comprensión completa de la invención. Sin embargo, será evidente para los expertos en la técnica que la invención se puede poner en práctica en otras realizaciones que se aparten de estos detalles específicos. En otros casos, se omiten descripciones detalladas de dispositivos, circuitos y métodos bien conocidos para no oscurecer la descripción de la invención con detalles innecesarios.

La invención se refiere a una seguridad de la comunicación mejorada en una red de comunicación que usa claves previamente compartidas como base para la seguridad de la comunicación. Una red de comunicación puede ser aquí una red de comunicación móvil, tal como una red de comunicación móvil de segunda generación (2G) como el sistema global para comunicaciones móviles (GSM), una red de tercera generación (3G) como el sistema universal de telecomunicaciones móviles (en inglés, Universal Mobile Telecommunications System, UMTS) o una cuarta red de generación (4G) tal como evolución a largo plazo (en inglés, Long-Term Evolution, LTE) o cualquier sistema evolucionado futuro como la 5ª Generación (5G) de 3GPP actualmente en desarrollo. Estos son solo unos pocos ejemplos de redes donde se puede implementar la invención. Otros tipos de redes que pueden usarse son, por ejemplo, las redes de área local inalámbricas (en inglés, Wireless Local Area Network, WLAN). Un dispositivo de comunicación, tal como un equipo de usuario (UE), una estación móvil (MS), a veces denominada teléfono celular, puede comunicarse usando estas redes de comunicación. Además, un dispositivo de comunicación aquí está conectado a un módulo de identidad, donde el módulo de identidad puede ser una tarjeta inteligente tal como una tarjeta de circuito integrado universal (en inglés, Universal Integrated Circuit Card, UICC) que contiene un módulo de identidad de abonado (SIM) y/o un módulo de identidad de abonado universal (USIM) o un SIM del subsistema multimedia IP (ISIM), un módulo SIM integrado (en inglés, embedded SIM, eSIM), un módulo de software, un módulo de ejecución confiable de plataforma global (en inglés, Global Platform Trusted Execution) o similares. Por tanto, el módulo de identidad también se puede implementar en software que se ejecuta en un entorno de ejecución confiable, o software que se ejecuta en un procesador de propósito general, aunque este último no es el preferido. En lo sucesivo, el término USIM se usará como un ejemplo en las descripciones, pero el experto en la técnica apreciará que cualquier tipo de módulo de identidad servirá para el mismo fin. Debe tenerse en cuenta que el módulo de identidad puede ser una parte del dispositivo de comunicación. También puede ser una entidad separada que esté conectada al dispositivo de comunicación, cuando se va a usar el dispositivo de comunicación.

Como base para la seguridad de la comunicación se usa una clave, por ejemplo, para autenticación y acuerdo de claves. De forma ventajosa, la clave puede compartirse previamente y almacenarse en un módulo de identidad como se acaba de describir.

A continuación, solo se analizará el ejemplo del dispositivo de comunicación en la forma de un UE. Sin embargo, debe tenerse en cuenta que el dispositivo de comunicación no se limita a ser un UE. Puede ser cualquier tipo de terminal inalámbrico, estación móvil, teléfono móvil, teléfono de bucle local inalámbrico, teléfono inteligente, equipo de usuario, ordenador de escritorio, PDA, teléfono celular, tableta, ordenador portátil, teléfono de VoIP o teléfono, que pueda enviar y recibir de forma inalámbrica datos y/o señales hacia y desde un nodo de red. También puede ser un módem de comunicación que proporcione, por ejemplo, conectividad de 3G o 4G para algún tipo de dispositivo electrónico (por ejemplo, un sensor o cámara digital), un vehículo, una pasarela doméstica, un punto de acceso WiFi/4G

doméstico, un dispositivo electrodoméstico como un frigorífico, termostato, alarma antirrobo, aspiradora, robot cortacésped o similares. También puede ser un terminal fijo conectado a una red de comunicación fija.

Como se mencionó anteriormente y como se muestra en la Fig. 1, la autenticación y el acuerdo de claves (AKA) es un sistema de acuerdo de claves conocido usado en algunas redes de comunicación.

Como puede verse en la Fig. 1, el registro de ubicación de visitante/nodo de soporte de pasarela de servicio (VLR/SGSN) se muestra enviando 10 una solicitud de datos de autenticación al entorno doméstico/registro de ubicación de inicio (HE/HLR) en relación con un equipo de usuario visitante (UE). El HE/HLR genera 12 un conjunto de vectores de autenticación (AV (1..n)) y envía 14 los vectores (AV (1..n)) al VLR/SGSN en un mensaje de respuesta de datos de autenticación, donde el VLR/SGSN luego almacena 16 los vectores de autenticación.

El VLR/SGSN selecciona 18 un vector de autenticación y basado en el contenido de este vector envía un mensaje 20 de solicitud de autenticación de usuario ARQ que comprende un desafío que usa un parámetro RAND asignado a un valor aleatorio RAND(i) y un testigo de autenticación AUTN(i), donde AUTN(i) también comprende un código de verificación del desafío como se explicará con más detalle a continuación, e i denota que el valor está asociado con AVi. En el UE, luego se verifica AUTN(i) y se calcula un resultado RES(i) en una etapa de verificación 22. El UE luego envía un mensaje 20 de respuesta de autenticación de usuario (ARE) que comprende el resultado RES(i). El vector de autenticación comprende un resultado esperado XRES(i) y el VLR/SGSN luego compara 26 el resultado recibido RES(i) con el resultado esperado XRES(i), y si la comparación fue exitosa, es decir, si se encontró que eran iguales, el VLR/SGSN luego selecciona 30 la clave de cifrado CK(i) y la clave de protección de integridad IK(i). El UE también calcula 28 las mismas claves CK(i) e IK(i). Éstas luego se usan para obtener las claves de sesiones. En algunos sistemas (por ejemplo, LTE) las claves CK(i) e IK(i) se usan para obtener una clave de sesión Kasme.

En una autenticación del tipo mostrada en la Fig. 1 y descrita anteriormente, una clave secreta K, con ventaja compartida previamente, se usa tanto en el equipo de usuario como en la red.

Se prevé que el AKA de UMTS/LTE se utilizará también como base en las redes móviles de la generación futura (por ejemplo, 5G) debido a su historial probado de seguridad y robustez. En lo sucesivo, a menos que se indique lo contrario, "AKA" se usará para indicar AKA de UMTS, AKA de LTE, o un protocolo basado en estos, por ejemplo, una futura extensión para redes "5G".

Como también se mencionó anteriormente, el protocolo AKA mostrado en la Fig. 1 es compatible con la especificación técnica TS 33.102 de 3GPP donde la comunicación tiene lugar entre un UE, un registro de ubicación de visitantes/nodo de soporte de pasarela de servicio (VLR/SGSN) y un entorno doméstico/registro de ubicación de inicio (HE/HLR). En 4G/LTE, la entidad de gestión de la movilidad (MME) que sustituye a VLR/SGSN y HE/HLR corresponde al servidor de abonado doméstico (HSS). Tenga en cuenta que el terminal/UE/dispositivo de comunicación se denomina MS en esta figura. Para los fines de esta descripción, la MS y el UE son la misma entidad.

El AUTN(i) (Testigo de Autenticación, (en inglés, Authentication Token)) es un parámetro compuesto por diferentes campos: campo de gestión de autenticación (en inglés, Authentication Management Field, AMF), códigos de autenticación de mensajes (en inglés, Message Authentication Code, MAC) y una indicación de número de secuencia (SQN, posiblemente cifrado/modificado por una clave de anonimato AK). El MAC (i) es un código de autenticación de mensajes que protege el desafío RAND(i) (número aleatorio (RANDom)), así como SQN y AMF de ser falsificados por un tercero a través de las funciones criptográficas implementadas por el USIM. Las claves CK(i) e IK(i) se usan directamente para la protección de cifrado/integridad en 3G y se usan indirectamente para estos fines en 4G/LTE derivando claves de cifrado/integridad de CK(i) e IK(i) (específicamente: desde una clave Kasme, formada por CK(i) e IK(i)).

En estas funciones criptográficas, que se proporcionan tanto en el UE como en el HE, se usa, por tanto, una clave compartida K.

K es una clave (generalmente de 128 bits) que, por tanto, es compartida por el USIM y el HSS/AuC, donde AuC es la abreviatura de centro de autenticación (en inglés, Authentication Center). La clave compartida debe mantenerse en secreto para otras partes.

Como una convención de notación simplificadora usada en el resto de la descripción de los cálculos criptográficos y otras formas de cálculo, se pueden introducir parámetros, distintos a los mencionados explícitamente, a las funciones tales como las funciones de derivación de clave (en inglés, Key Derivation Function, KDF), los códigos de autenticación de mensajes (en inglés, Message Authentication Codes, MAC) y todas las demás funciones en todos los casos descritos en la presente memoria. Los parámetros se pueden poner en un orden diferente al mencionado explícitamente. Los parámetros se pueden transformar antes de introducirse a la función. Por ejemplo, un conjunto de parámetros P1, P2, ..., Pn, para algún entero no negativo n, podrían ser transformados pasando primero por una segunda función f y el resultado de la misma, es decir, f(P1, P2, ..., Pn), se introduce a la función.

Un ejemplo de una derivación de clave cuando un parámetro P1 se transforma primero antes de introducirse a una KDF para calcular una clave llamada "clave_de_salida" podría ser una derivación de la forma clave_de_salida=KDF(f(P1), algún otro parámetro), donde f es alguna función arbitraria o cadena de funciones. La

entrada "algún otro parámetro" podría ser 0,1 o más de otros parámetros, por ejemplo, usados para vincular la clave a un contexto determinado. A veces, la notación "..." puede usarse como un sinónimo de "algún otro parámetro". Los parámetros se pueden introducir como parámetros separados o pueden concatenarse juntos y luego introducirse en una sola entrada a la KDF. Por tanto, un experto en la técnica comprenderá que pueden usarse parámetros adicionales, que los parámetros se pueden transformar o reorganizar, etc. e incluso en presencia de variaciones como estas, el núcleo de la idea sigue siendo el mismo.

Como se mencionó anteriormente, la seguridad de AKA depende de que la clave K se mantenga en secreto. Recientemente, se informó en los medios de comunicación que se había violado la seguridad de un fabricante de tarjetas USIM y que un conjunto de claves K se había "filtrado" (o caído en manos equivocadas), poniendo, por tanto, a los abonados asociados con estas claves en riesgos tales como la suplantación de identidad, secuestro de conexiones, y escuchas clandestinas (ya que también las claves de cifrado, derivadas de CK(i) y/o IK(i), también, por tanto, están potencialmente en riesgo). En el artículo, https://firstlook.org/theintercept/2015/02/19/great-sim-heist/ se mencionó que un problema potencial con el protocolo AKA, que conduce a las implicaciones de seguridad antes mencionadas, residía en que AKA carece del así llamado secreto perfecto hacia adelante (PFS). El PFS significa que incluso si la clave a largo plazo usada para establecer las claves de sesión está expuesta, todavía no implica que las claves de sesión pasadas también estén expuestas. Es decir, la clave de sesión está segura en un futuro donde la clave a largo plazo se ha visto comprometida. El AKA, de hecho, tiene una propiedad ventajosa pero más débil, a menudo denominada separación de claves: incluso si las claves de sesión (CK(i), IK(i), etc.) están expuestas, CK (j), IK (j) pasadas/futuras (y otras claves derivadas) no están expuestas. Sin embargo, cuando la clave K a largo plazo está expuesta, todas estas propiedades de seguridad proporcionan poco valor.

Los aspectos de la invención se refieren a la mejora de la función de autenticación descrita anteriormente a través de la adición de un secreto perfecto hacia adelante. Por tanto, se refiere a la seguridad de la comunicación tanto para el equipo de usuario como para la red.

Sin embargo, antes de que se haga una descripción detallada sobre cómo se hace esto, se darán ahora algunos detalles más del entorno.

La Fig. 2 muestra esquemáticamente un entorno de comunicación ejemplar de un dispositivo 40 de comunicación, cuyo dispositivo 40 de comunicación en la Fig. 2 está en la forma de un equipo de usuario (UE) para el que se mejora la seguridad de la comunicación. En este ejemplo hay una primera y una segunda red de comunicación, que en este caso son ambas redes de comunicación móviles, tales como las redes LTE. En este caso, un equipo de usuario UE está en contacto inalámbrico a través de una interfaz aérea con una estación base BS 42 de una primera red 36 de comunicación, cuya red de comunicación es una primera red inalámbrica WN1. La estación base 42 está a su vez conectada a un primer dispositivo 44 de red de la primera red inalámbrica WNi, cuyo primer dispositivo 44 de red también puede ser considerado un nodo de red. En este ejemplo, es una MME. La MME 44 está a su vez conectada a un segundo dispositivo 46 de red en una segunda red 38 de comunicación, cuya segunda red 46 de comunicación es una segunda red inalámbrica WN2. En este caso el segundo dispositivo 46 de red es un HSS y puede ser considerado un nodo de red. La primera red inalámbrica WN1 puede ser una red visitada, es decir, una red que visita el UE, mientras que la segunda red inalámbrica WN2 puede ser una red doméstica del UE, es decir, una red que aloja una suscripción asociada con el UE. La estación base 42, que en muchas redes puede denominarse nodo B (en inglés, node B, nodeB) o nodo B evolucionado (en inglés, evolved NodeB, eNodoB), se proporciona en una parte de la primera red inalámbrica WN1 llamada red de acceso AN, mientras que la MME 44 se proporciona en una parte llamada red central CN.

Por tanto, en este ejemplo la primera red 36 de comunicación es una red que es visitada por el UE, mientras que la segunda red 38 de comunicación es una red doméstica del UE.

En diferentes realizaciones, cada red inalámbrica puede comprender cualquier número de redes cableadas o inalámbricas, nodos de red, estaciones base, controladores, dispositivos inalámbricos, estaciones de retransmisión, y/o cualquier otro componente que pueda facilitar o participar en la comunicación de datos y/o señales ya sea a través de conexiones por cable o inalámbricas.

Cada red inalámbrica puede comprender una o más redes IP, redes telefónicas públicas conmutadas (en inglés, Public Switched Telephone Network, PSTN), redes de datos de paquetes, redes ópticas, redes de área amplia (en inglés, Wide Area Network, WAN), redes de área local (en inglés, Local Area Newtork, LAN), redes de área local inalámbricas (WLAN), redes cableadas, redes inalámbricas, redes de área metropolitana, y otras redes para permitir la comunicación entre dispositivos.

Como puede verse en la Fig. 1, la comunicación tiene lugar entre el UE y el primer dispositivo de red. Sin embargo, como también puede verse, la información de autenticación (AVs) fue proporcionada en esencia por el segundo dispositivo de red en la red doméstica del UE.

Como se mencionó anteriormente, la invención está dirigida a introducir un secreto perfecto hacia adelante en un sistema tal como el de la Fig. 2.

Un esquema adecuado para usar como base es el esquema definido en el protocolo Diffie-Hellman. Este esquema implementado entre el UE y la primera red inalámbrica WN1 se indica esquemáticamente en la Fig. 3.

Como puede verse en la Fig. 3, la primera red inalámbrica WN1 (y luego, típicamente, el primer dispositivo de red) envía un parámetro que se genera como un valor base g elevado a un número aleatorio x y el UE responde con un parámetro que se genera como el mismo valor base g elevado a otro número aleatorio y (el término "aleatorio" debe entenderse que incluye tanto estadísticamente aleatorio así como pseudoaleatorio). Los parámetros también deben autenticarse usando, por ejemplo, una clave compartida (no mostrada). Una vez autenticados, el UE y el primer dispositivo de red pueden usar una clave de sesión común, que por tanto también se comparte. Se puede obtener una base para la clave de sesión como K' = g^(xy) o K' = g^(yx) (que producirá el mismo valor K'). La clave se puede obtener más particularmente como g elevado a x elevado a y, o, g elevado a y elevado a x, es decir,

(g^x)^y o (g^y)^x.

Como puede verse, la clave de sesión K', que es una clave de sesión segura, puede generarse basada en los valores x e y. El experto en la técnica reconocerá que las curvas elípticas, y otros grupos cíclicos donde el problema del logaritmo discreto es difícil, también pueden usarse; sin embargo, para simplificar, usamos la notación multiplicativa g^x aunque la notación aditiva x*g sería más apropiada en el caso de la curva elíptica. Para más detalles, véase Menezes et al, "Handbook of Applied Cryptography", quinta impresión (agosto de 2001), CRC Press.

La Fig. 4 muestra una realización ejemplar del UE. El UE puede comprender un módulo 48 de identidad de abonado universal (USIM), por ejemplo, en la forma de una tarjeta inteligente que se conecta a un módulo 52 de acuerdo de claves y autenticación de seguridad perfecta hacia adelante (PFS-AKA), que a su vez está conectado a una módulo 50 de comunicación, que puede ser un módulo de comunicación inalámbrica. Aquí el módulo 50 de comunicación y el módulo 52 de PFS-AKA juntos forman un equipo móvil 46, mientras que el USIM es un módulo 48 de identidad. Así, juntos, el USIM, el módulo de PFS-AKA, y el módulo de comunicación forman el equipo de usuario.

Una forma de realizar el ME 46 se muestra esquemáticamente en la Fig. 5. El ME 46 comprende el procesador 54, el almacenamiento 56, la interfaz 50B y la antena 50A. Estos componentes pueden trabajar juntos para proporcionar la funcionalidad del ME, tal como proporcionar conexiones inalámbricas en una red inalámbrica. Los componentes del ME 46 se representan como cajas individuales ubicadas dentro de una caja individual más grande, sin embargo, en la práctica, un ME puede comprender múltiples componentes físicos diferentes que conforman un componente ilustrado individual (por ejemplo, el almacenamiento 56 puede comprender múltiples microchips discretos, cada microchip representa un parte de la capacidad de almacenamiento total).

El procesador 54 puede ser una combinación de uno o más de un microprocesador, controlador, microcontrolador, unidad central de procesamiento, procesador de señal digital, circuito integrado específico de aplicación, matriz de puerta programable en campo, o cualquier otro dispositivo informático, recurso, o combinación de hardware, software y/o lógica codificada operable para proporcionar, ya sea solo o en combinación con otros componentes del ME, tal como almacenamiento 56, la funcionalidad del ME. Tal funcionalidad puede incluir proporcionar diversas características inalámbricas analizadas en la presente memoria, que incluye cualquiera de las características o beneficios descritos en la presente memoria.

El almacenamiento 56 puede ser cualquier forma de memoria volátil o no volátil que incluye, sin limitación, almacenamiento persistente, memoria de estado sólido, memoria montada de forma remota, medios magnéticos, medios ópticos, memoria de acceso aleatorio (en inglés, Random Access Memory, RAM), memoria de solo lectura (en inglés, Read-Only Memory, ROM), medios extraíbles, o cualquier otro componente de memoria local o remota adecuado. El almacenamiento 56 puede almacenar cualquier dato, instrucciones, o información adecuada, que incluyen software y lógica codificada, usados por el ME 46. El almacenamiento 56 puede usarse para almacenar cualquier cálculo realizado por el procesador 54 y/o cualquier dato recibido a través de la interfaz 50B.

La interfaz 50B puede usarse en la comunicación inalámbrica de señalización y/o datos entre el UE y un dispositivo de red, tal como la estación base 42. Por ejemplo, la interfaz 50B puede realizar cualquier formateo, codificación, o traducción que pueda ser necesaria para permitir que el UE envíe y reciba datos desde la estación base 42 a través de una conexión inalámbrica. La interfaz 50B también puede incluir un transmisor y/o receptor de radio que se puede acoplar a la antena 50a o ser parte de ella. La radio puede recibir datos digitales que se van a enviar a la estación base 42 a través de una conexión inalámbrica. La radio puede convertir los datos digitales en una señal de radio que tenga el canal y los parámetros de ancho de banda apropiados. Luego, la señal de radio puede transmitirse a través de la antena 50a a la estación base 42.

La antena 50a puede ser cualquier tipo de antena capaz de transmitir y recibir datos y/o señales de forma inalámbrica.

El almacenamiento 56 también puede comprender instrucciones para manejar el secreto perfecto hacia adelante en relación con la comunicación del ME a la primera red inalámbrica.

El almacenamiento 56 puede comprender más particularmente instrucciones informáticas que hacen que el procesador 54 implemente el módulo 52 de PFS-AKA. El módulo 50 de comunicación se puede, a su vez, implementar en esencia a través de la combinación de la interfaz 50B y la antena 50A.

La Fig. 6 muestra un dispositivo 57 de red general, cuya estructura es aplicable tanto al primer como al segundo dispositivo 44 y 46 de red. El dispositivo 47 de red comprende el procesador 60, el almacenamiento 62 y la interfaz 58. Estos componentes se representan como cajas individuales ubicadas dentro de una caja individual más grande. Sin embargo, en la práctica, un dispositivo de red puede comprender múltiples componentes físicos diferentes que conforman un componente ilustrado individual (por ejemplo, la interfaz 58 puede comprender los terminales para acoplar cables para una conexión cableada). De manera similar, el dispositivo 57 de red puede estar compuesto por múltiples componentes físicamente separados, cada uno de los cuales puede tener su propio procesador, almacenamiento, e interfaz respectivos. En ciertos escenarios en los que el dispositivo 57 de red comprende múltiples componentes separados, uno o más de los componentes separados pueden compartirse entre varios dispositivos de red.

El procesador 60 puede ser una combinación de uno o más de un microprocesador, controlador, microcontrolador, unidad central de procesamiento, procesador de señal digital, circuito integrado específico de aplicación, matriz de puerta programable en campo, o cualquier otro dispositivo informático, recurso, o combinación de hardware, software y/o lógica codificada adecuados operables para proporcionar, ya sea solo o junto con otros componentes del dispositivo de red, tales como almacenamiento 62, la funcionalidad del dispositivo de red. Por ejemplo, el procesador 60 puede ejecutar las instrucciones almacenadas en el almacenamiento 62.

El almacenamiento 62 puede comprender cualquier forma de memoria legible por ordenador volátil o no volátil que incluye, sin limitación, almacenamiento persistente, memoria de estado sólido, memoria montada de forma remota, medios magnéticos, medios ópticos, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), medios extraíbles, o cualquier otro componente de memoria local o remota adecuado. El almacenamiento 62 puede almacenar cualquier instrucción, dato o información adecuada, que incluye software y lógica codificada, usados por el dispositivo 57 de red. El almacenamiento 62 puede usarse para almacenar cualquier cálculo hecho por el procesador 60 y/o cualquier dato recibido a través de la interfaz 58.

El dispositivo 57 de red también comprende la interfaz 58 que puede usarse en la comunicación por cable de señalización y/o datos entre el dispositivo 57 de red, la red WN1 o WN2, y/o el UE. Por ejemplo, la interfaz 58 puede realizar cualquier formateo, codificación, o traducción que pueda ser necesaria para permitir que el dispositivo 57 de red envíe y reciba datos de la red WN1 o WN2 a través de una conexión por cable.

Los aspectos de la invención se refieren a la adición de PFS a AKA.

Las siguientes realizaciones se describirán en el contexto 4G/LTE por simplicidad, pero también es aplicable a AKA del subsistema multimedia IP (en inglés, IP Multimedia Subsystem AKA, IMS AKA) y protocolo de autentificación extensible de AKA (en inglés, Extensible Authentication Protocol AKA, EAP-AKA) y las realizaciones también se ven actualmente como aplicables a los sistemas de 5G actualmente analizados o cualquier otro sistema futuro basado en AKA, u otros entornos en los que se usen módulos de identidad con claves previamente compartidas.

Como se mencionó anteriormente, los aspectos de la invención se refieren a proporcionar un secreto perfecto hacia adelante en la comunicación entre el dispositivo de comunicación y el primer dispositivo de red, con la ventaja basada en el protocolo Diffie-Hellman (DH).

Sin embargo, este protocolo requiere un esfuerzo de cálculo y un ancho de banda adicional para transportar los parámetros necesarios: los parámetros de DH intercambiados son mucho más grandes que los parámetros del protocolo AKA actualmente estandarizados (RAND, RES, etc.). Incluso si fuera posible aumentar el número de bits señalizados a través de la interfaz aérea, sería deseable mantener la interfaz entre el USIM y el ME (USIM-ME, por sus siglas en inglés) estandarizada en el UE, lo que implica un cuello de botella para el tamaño de los parámetros del protocolo que cae por debajo del nivel donde DH ofrece una gran seguridad. (RAND es actualmente de 128 bits y para lograr una seguridad que coincida con la fuerza de 128 bits de AKA, se necesitan parámetros de DH de al menos 256 bits para variantes de curva elíptica de DH, y alrededor de 3000 bits para logaritmo discreto estándar DH módulo a primo, p.) Además, DH es sensible a un ataque de intermediario (en inglés, Man-In-The-Middle, MITM) que implica la necesidad de añadir algún mecanismo para autenticar los parámetros de DH. El enfoque natural para hacer esto sería añadir otro campo de datos a AKA y conducir a una sobrecarga de señalización incluso mayor.

Por lo tanto, un objeto es elevar el nivel de seguridad de la comunicación entre un dispositivo de comunicación y una red de comunicación en relación con el uso de claves compartidas a largo plazo. También puede ser de interés evitar el envío de mensajes adicionales. Por tanto, es deseable que se use la estructura de mensajes existente sin añadir nuevos mensajes. Esto puede ser importante desde una perspectiva de ahorro de energía tanto en lo que respecta al dispositivo de comunicación así como al nivel de entorno general, ya que el envío de mensajes adicionales usa energía, que puede ser un recurso limitado especialmente en el dispositivo de comunicación. Además, la comunicación de red también está típicamente estandarizada y, a menudo, es mucho más difícil ponerse de acuerdo sobre la introducción de nuevos mensajes, que en la adición de nuevos elementos en los mensajes ya existentes que serían necesarios para proporcionar autenticación y protección MITM si se usa un enfoque sencillo para añadir un secreto perfecto hacia adelante.

Antes de continuar, es beneficioso hacer algunas observaciones sobre la autenticación en protocolos que proporcionan PFS, ejemplificados por el protocolo de DH. En el contexto específico de AKA, un experto en la técnica puede tener la tentación de usar uno o más de los parámetros de resultado de AKA producidos por los cálculos en el USIM, es decir, RES, CK y/o IK para este fin. En general, esto es peligroso para la seguridad. El cálculo, por ejemplo, de los parámetros DH g^x y/o g^y a través de x = F'(CK, IK) y/o y = F'(CK, IK) para alguna función F' no conducirá a un secreto perfecto hacia adelante ya que estos parámetros se pueden calcular a partir del conocimiento de la clave K a largo plazo. Por lo tanto, mientras la reutilización de los parámetros de AKA y los campos de datos de los protocolos es beneficiosa, tiene que realizarse con precaución. Por lo tanto, x e y deben ser independientes de los parámetros AKA.

Por otro lado, para la protección contra MITM, podemos usar uno o más de los parámetros de AKA y añadir un MAC estándar. Por ejemplo, una respuesta de AKA del UE podría comprender:

RES, g^y, MAC(CK || IK || ..., g^y || ...).

(Por tanto, esta es posiblemente otra función de MAC que no debe confundirse con el parámetro MAC antes mencionado del protocolo AKA. También tenga en cuenta que, ya que estamos considerando un conjunto fijo de parámetros AKA, suprimimos el índice i y escribimos, por ejemplo, CK en lugar de CK(i) como anteriormente.) Tenga en cuenta que generalmente habrá varias opciones para qué clave usar en el MAC, es decir, como el primer parámetro en la entrada al MAC (..., ...). Por lo tanto, para no oscurecer la descripción con demasiados detalles, a menudo suprimimos la clave (y otros parámetros menos importantes), por ejemplo, escribiendo MAC(g^y) en lugar de MAC(CK || IK || ..., g^y || ...) como arriba. Donde ... indica posiblemente otras variables/parámetros y || denota una forma de combinar las entradas a la función de MAC, por ejemplo, concatenación. Sin embargo, una forma incluso más económica sería incorporar el MAC anterior en el elemento de información existente que transporta el RES cuando se transmite desde el UE a la MME, por ejemplo, calculando RES '= MAC(RES, g^y, ...), usando RES (y opcionalmente CK, IK) como clave y por tanto, el UE responde solo con RES', g^y. La función de MAC puede basarse en código de autenticación de mensajes con clave-hash (HMAC), una de las funciones f nativas de AKA (como se define en la especificación técnica TS 33.102 de 3GPP) u otra función adecuada, por ejemplo, basada en el estándar de cifrado avanzado (en inglés, Advanced Encryption Standard, AES). Como RES' se calcula como un MAC que se basa en g^y y un valor clave (CK/IK o RES), está claro que, de hecho, es un código de verificación para la autenticidad de g^y. Además, cuando el MAC también se basa en RES como la clave, al mismo tiempo puede usarse para verificar el RES. Aquí también debe tenerse en cuenta que un MAC es solo una función posible que puede usarse para calcular RES'. Otro ejemplo es una función de derivación de clave o una función pseudoaleatoria en general.

Se aplican consideraciones similares para el valor de DH g^x transmitido desde la red al ME para ahorrar sobrecarga de comunicación y, sin embargo, proporcionar el PFS.

Específicamente, el AuC/HSS puede, en algunas realizaciones, generar los vectores de autenticación enviados a la red de servicio en consecuencia, es decir, calcular los parámetros tales como RAND = g^x, aplicar un hash a RAND antes de introducirlo a las funciones f, etc. Por tanto, g^x se transporta efectivamente en el campo de protocolo AKA de RAND sin añadir un nuevo elemento de información. En algunas realizaciones, el HSS no necesita enviar CK, IK (o claves derivadas del mismo tal como Kasme) a la MME como parte de los vectores de autenticación (AV) ya que la clave compartida resultante se basará en g^(xy) que de todos modos, no es conocida por el HSS en el momento de la generación de AV. En otras realizaciones, el AuC/HSS puede incluir estos CK, IK para incluirse en la generación de claves. Por ejemplo, en LTE las claves están "vinculadas" a la red de acceso a través de la inclusión de un identificador de PLMN (red móvil terrestre pública) en la derivación de la clave Kasme de CK, IK. Ya que el HSS, como se indica, no conoce g^(xy) en el punto en el que se generan los AV, se podría lograr un enlace al identificador de PLMN (en inglés, Identifier PLMN, PLMN ID) que incluye el PLMN ID en la derivación de alguna clave adicional de CK, IK e incluir esa clave derivada en el AV. También se puede adoptar la MME, es decir, dado XRES en el vector de autenticación (en inglés, Authentication Vector, AV) del HSS, en la realización anterior calcularía XRES' = MAC(XRES, g^y) antes de verificar la autenticidad del abonado, y puede derivar Kasme como F(g^(xy) || ...) para alguna función adecuada F, etc. El ME puede calcular Kasme de manera similar.

Ahora se describirá una primera realización también con referencia a la Fig. 7 y 8, donde la Fig. 7 muestra un diagrama de flujo de un método para mejorar la seguridad de la comunicación del equipo de usuario en comunicación con un dispositivo de red de una red de comunicación y la Fig. 8 muestra un diagrama de flujo de las etapas del método en un método para mejorar la seguridad de la comunicación del primer dispositivo de red de la red de comunicación.

En los ejemplos dados aquí, la red 36 de comunicación es la primera red inalámbrica WN1 y el primer dispositivo 44 de red es la MME de la primera red inalámbrica.

El funcionamiento puede comenzar con el UE conectándose a la primera red 36 de comunicación. Como parte de esto, un identificador, por ejemplo, la identidad de abonado móvil internacional IMSI se puede proporcionar desde el UE o más bien desde el USIM 48 del UE al primer dispositivo 44 de red, que a su vez envía una solicitud de un vector de autenticación AV al segundo dispositivo 46 de red en la segunda red 38 de comunicación. El segundo dispositivo 46 de red genera el vector de autenticación, que puede comprender el testigo de autenticación AUTN, el valor aleatorio RAND, el resultado esperado del cálculo de verificación XRES así como una clave de sesión inicial Kasme. También puede comprender otras claves tales como las claves CK/IK. Por tanto, hasta ahora, el segundo nodo 46 de red puede

funcionar según las especificaciones de AKA existentes (3GPP). De esta forma, el primer dispositivo 44 de red obtiene el vector de autenticación, etapa 74, que puede comprender al menos un valor aleatorio RAND y un resultado de verificación esperado XRES. Aquí se puede mencionar que RAND se proporciona para su uso como un desafío para el UE y AUTN comprende un código de verificación del desafío para este desafío.

Después de haber obtenido el vector de autenticación, el primer dispositivo de red luego obtiene un primer parámetro PFS1 de PFS, etapa 76, cuyo primer parámetro PFS1 de PFS se puede obtener a través de la generación como un valor base g elevado con un valor aleatorio x, es decir, como g^x, donde el valor aleatorio x puede generarse por el primer dispositivo 44 de red. Alternativamente, el valor aleatorio x y/o el primer parámetro PFS1 de PFS se obtienen del segundo dispositivo 46 de red, en cuyo caso el segundo nodo 46 realiza operaciones adicionales además de las actualmente especificadas por AKA. A continuación, el primer dispositivo 44 de red obtiene un primer código de verificación, VC1, para el primer parámetro PFS1 de PFS, etapa 78. En una variación, obtiene el VC1 generando el código de verificación en sí mismo y en otra variación, el segundo dispositivo de red genera el primer código de verificación. Por tanto, en la segunda variación, también se da el caso de que el segundo nodo 46 realiza operaciones adicionales además de las especificadas actualmente por AKA. El primer código de verificación VC1 puede generarse como un código de autenticación de mensajes (MAC) sobre el primer parámetro PFS1 de PFS usando como clave, una clave conocida del vector de autenticación, tal como XRES o la clave de sesión inicial Kasme. Cuando el segundo dispositivo 46 de red genera el primer código de verificación, el valor RAND se basa en el primer parámetro PFS1 de PFS. En este caso, el valor RAND puede generarse por el segundo dispositivo 46 de red como el primer parámetro PFS1 de PFS o como un hash del primer parámetro PFS1 de PFS, tal como un hash criptográfico. De este modo es posible, por ejemplo, por el UE, usar el código de verificación del desafío AUTN también como el primer código de verificación VC1 para el primer parámetro PFS1 de PFS. Aquí también se puede mencionar que RAND en ambos de estos ejemplos es de hecho un desafío para el USIM 48 del UE.

El primer dispositivo 44 de red luego envía el desafío RAND, el primer parámetro PFS1 de PFS, posiblemente ambos codificados por el elemento de información RAND, y el primer código de verificación VC1 al UE, que puede ser enviado con ventaja en un mensaje de solicitud de autenticación ARQ, etapa 80. En caso de que el primer código de verificación VC1 sea un código separado (es decir, diferente de AUTN), por ejemplo, un MAC dedicado generado por el primer dispositivo 44 de red, luego también el testigo de autenticación AUTN se puede proporcionar por separado en el mensaje.

El desafío RAND, el primer parámetro PFS1 de PFS (codificado en RAND o en un parámetro adicional) y el primer código de verificación VC1 (codificado en AUTN o un código separado) luego se reciben en el UE, etapa 64. Pueden recibirse más particularmente a través del mensaje de solicitud de autenticación ARQ que es recibido por el módulo 50 de comunicación del ME 46 y reenviado desde el mismo al módulo 52 de PFS-AKA.

En el módulo 52 de PFS-AKA, el desafío o un derivado del mismo se reenvía al USIM 48, etapa 65. Esto se hace para reenviar un desafío puro al USIM 48. El desafío puro se puede obtener de una de dos formas, dependiendo de las alternativas descritas anteriormente. Si el elemento de información RAND codifica el primer parámetro PFS1 de PFS se puede obtener como un derivado a través del módulo de PFS-AKA calculando un hash del elemento de información RAND, es decir, un hash de g^x. Esto significa que si RAND no es ya un hash del primer parámetro de PFS g^x, luego se puede calcular uno en esta etapa. Si el elemento de información RAND no codifica el primer parámetro PFS1 de PFS, luego el valor del elemento de información RAND puede introducirse directamente en el USIM. Además, si el desafío recibido por el módulo de PFS-AKA es un hash del primer parámetro de PFS, tal como un hash criptográfico, se puede reenviar directamente al USIM. El reenvío se realiza a través de la interfaz USIM-ME estandarizada en el UE.

Como se indicó anteriormente, el USIM 48 comprende una clave K, con la ventaja de una clave K que se comparte previamente con el segundo dispositivo 46 de red. También comprende medios de procesamiento criptográfico. Este módulo 48 luego puede proporcionar al menos un parámetro de resultado (CK/IK) como respuesta al desafío (RAND y AUTN). Un parámetro de resultado puede ser una o más claves criptográficas, tal como una clave de cifrado CK y una clave de protección de integridad IK, que pueden usarse por el módulo 52 de PFS-AKA para obtener la clave de sesión inicial Kasme. Otro parámetro de resultado puede ser un parámetro de respuesta RES al desafío, cuyo parámetro de respuesta tiene un valor de respuesta. Por tanto, un parámetro de respuesta de este tipo tiene un valor criptográfico calculado basado en la clave previamente compartida y dichos medios de procesamiento criptográfico.

El equipo móvil 46 y más particularmente el módulo 52 de PFS-AKA obtiene por tanto, o más bien recibe el uno o más parámetros de resultado, etapa 66, y continúa y determina la autenticidad del primer parámetro PFS1 de PFS, es decir, la autenticidad de g^x, etapa 68. Determina por tanto, basado en VC1 y el uno o más parámetros de resultado si el parámetro PFS1 de PFS es auténtico. Esto se puede hacer a través de la clave para que el primer código de verificación se base en uno o más de los parámetros de resultado y que use dicha clave para verificar un MAC transportado en VC1. Si el primer código de verificación es parte del desafío o más bien se transporta en el código de verificación del desafío AUTN, es decir, el subcampo MAC de AUTN, luego es suficiente que se obtenga un parámetro de resultado para determinar la autenticidad. Es decir, el USIM 49 ni siquiera proporcionaría ninguno de los parámetros de resultado si la verificación de AUTN hubiera fallado internamente al USIM, en su lugar devolverá un código de estado de error. Por tanto, el primer código de verificación se puede proporcionar como al menos una parte del código

de verificación del desafío. Por tanto, la autenticidad se determina basado en el USIM 48 que proporciona el al menos un parámetro de resultado.

El al menos un parámetro de resultado puede comprender una indicación de error, que indica el fallo del módulo de identidad para verificar dicho desafío o, derivado del desafío usando la clave K previamente compartida y los medios de procesamiento criptográfico. Este puede ser el caso cuando RAND = g^x y la verificación de AUTN falla internamente en el USIM. Si el módulo 52 de PFS-AKA recibe una señal de error de este tipo, puede determinar directamente que el primer parámetro de PFS no es auténtico.

A continuación, el ME 46 o más bien el módulo 52 de PFS-AKA del ME 46 genera un segundo parámetro PFS2 de PFS, y un segundo código de verificación, VC2, etapa 70, cuyo segundo parámetro PFS2 de PFS, puede generarse como el valor base g elevado con otro valor aleatorio y, es decir, como g^y. El código de verificación VC2 puede generarse a su vez como un código de autenticación de mensajes (MAC) del segundo parámetro PFS2 de PFS y una clave, por ejemplo, uno de los parámetros de resultado, o una derivada, Kd, de un parámetro de resultado, por ejemplo, Kasme. Por tanto, el segundo código de verificación se puede calcular usando el segundo parámetro de PFS y un parámetro de resultado o una derivada de un parámetro de resultado. Si este segundo código de verificación VC2 se genera basado en el parámetro de respuesta RES, VC2 puede codificarse en el elemento de información que normalmente transporta RES. Luego, puede generarse en función de RES y g^y, tal como un MAC de RES y g^y, donde RES actúa como una clave. Por tanto, el módulo de PFS calcula VC2 ya sea, como MAC(Kd, g^y, ...), o como MAC(Kasme, g^y, ...), o como MAC (RES, g^y, ...). El segundo parámetro PFS2 de PFS, y el segundo código de verificación VC2 se envían luego al primer dispositivo de red, ya sea junto con el parámetro de respuesta separado RES (si se usó Kd como clave), o (si se usó RES como clave) por la codificación de VC2 en lo que normalmente sería el elemento de información RES, etapa 72, y puede enviarse más particularmente en un mensaje de respuesta de solicitud de autenticación ARE.

El módulo 52 de PFS-AKA también puede verificar si los códigos de verificación primero y segundo satisfacen una relación específica. Este puede ser el caso cuando el primer parámetro de PFS, es decir, g^x, no se codifica en el desafío RAND y donde el primer código de verificación VC1 es un código separado, por ejemplo, un MAC explícito, que se verifica fuera del USIM. En este caso, la relación específica es la igualdad.

El segundo parámetro PFS2 de PFS y el segundo código de verificación VC2 y posiblemente también el parámetro de respuesta separado son recibidos, por tanto, por el primer dispositivo 44 de red, por ejemplo en el mensaje de respuesta de solicitud de autenticación ARE, etapa 82. El primer dispositivo 44 de red luego determina la autenticidad del parámetro de respuesta RES, etapa 84, que se puede hacer a través de la comparación del resultado de desafío o el valor del parámetro de respuesta RES con el resultado de desafío esperado XRES. Finalmente, el segundo parámetro PFS2 de PFS, se verifica basado en el segundo código de verificación VC2, etapa 86. Si el segundo código de verificación VC2 se proporciona por separado de la respuesta RES, la verificación en la etapa 86 puede basarse en un MAC del segundo parámetro de PFS, que usa la clave de sesión inicial Kasme o un derivado de la misma, Kd, como clave, para verificar el segundo código de verificación VC2. En caso de que el segundo código de verificación VC2 se proporcionó como una función basada en el valor del parámetro de respuesta como una clave, y VC2 se codificó en el parámetro RES, luego el primer dispositivo de red puede realizar las etapas 84 y 86 simultáneamente, ya que un valor correcto para el segundo código de verificación implica que el UE usó el RES correcto, es decir, los mismos valores indicados por XRES.

De este modo se ha implementado un esquema que mejora la seguridad de la comunicación. Más particularmente, mejora la seguridad si el secreto, la clave secreta previamente compartida se ha visto comprometida, ya que proporciona un secreto perfecto hacia adelante.

En las siguientes sesiones, por ejemplo, el intercambio de datos o señalización entre el UE y la red y más particularmente entre el UE y el primer dispositivo 44 de red luego es posible que se use una clave de sesión para proteger la comunicación y que esta clave de sesión se base en el primer y segundo parámetro de PFS. La clave de sesión puede basarse más particularmente en la base g elevada con el valor x elevada con el valor y según g^(xy).

Alternativamente, puede usarse un derivado de una combinación de Kasme y g^(xy). De este modo puede verse que se obtiene una clave de sesión segura que se basa al menos en los valores x e y usados para generar el primer y segundo parámetro de PFS. Por tanto, se genera basado en uno de los parámetros de PFS y el exponente del otro parámetro de PFS. Esto puede significar más particularmente que el módulo 52 de PFS-AKA puede generar la clave de sesión basada en el primer parámetro PFS1 de PFS, y el exponente y del segundo parámetro PFS2 de PFS, mientras que el primer dispositivo 44 de red puede generar la clave de sesión basada en el segundo parámetro PFS2 de PFS y el exponente x del primer parámetro PFS1 de PFS.

Ahora se describirá una segunda realización con la referencia que se hace a la Fig. 9, que muestra un diagrama de señalización que incluye el segundo dispositivo de red en la forma del HSS, el primer dispositivo de red en la forma de la MME y el equipo de usuario que se separa en el ME y el USIM. En esta realización, el segundo nodo (HSS) realiza las etapas que no son parte de las especificaciones actuales de AKA y a la Fig. 10, que muestra el código de verificación del desafío con más detalle.

Como puede verse en la Fig. 10 y como se describió anteriormente, el código de verificación del desafío proporcionado por el parámetro AUTN comprende los campos: AMF (campo de gestión de autenticación), MAC (código de autenticación de mensajes) y la indicación de número de secuencia SQN, que en este caso está cifrada por una clave anónima AK. También puede verse que el campo MAC se usa como primer código de verificación VC1A. Aquí se puede mencionar que también es posible usar el campo SQN para el primer código de verificación.

La segunda realización se basa en usar el parámetro RAND para transportar un valor DH como un parámetro de PFS cuando se envió desde la red/un dispositivo de red al UE/dispositivo de comunicación: RAND = g^x o una derivada de g^x.

Tenga en cuenta que un parámetro de PFS calculado según algunas variaciones de DH puede ser sustancialmente mayor de 128 bits, que es el tamaño estandarizado actual de RAND. Por lo tanto, podría plantear problemas con la interfaz USIM-ME. Para solucionar esto, antes de introducir RAND a los algoritmos f en el USIM (y en el servidor de abonado doméstico, HSS), el valor RAND proporcionado puede comprimirse, por ejemplo, por hash criptográfico: RAND' = H(RAND) = H(g^x), donde H es una función adecuada que produce el número apropiado de bits, por ejemplo, H puede basarse en SHA2 (donde SHA significa algoritmo de hash seguro), AES (estándar de cifrado avanzado), HMAC (código de autenticación de mensajes con clave-hash), etc. En principio, H también podría ser una función que seleccione un conjunto de 128 bits del RAND, por ejemplo, los 128 bits menos significativos. En el lado del UE, H puede aplicarse de manera similar en el ME (por ejemplo, en un módulo de PFS), antes de introducir RAND' en el USIM. Como el RAND es un desafío dirigido hacia el USIM, puede verse que el ME puede generar, por tanto, un derivado del desafío y reenviarlo al USIM. Como consecuencia, el campo MAC de AKA (que está comprendido dentro de AUTN) se calculará en dependencia de RAND', pero a través del uso de H, en efecto, se seguirá calculando en dependencia de RAND, es decir, g^x. Por lo tanto, se obtiene la autenticación desde el AuC (centro de autenticación)/HSS al USIM de este valor DH, evitando ataques MITM, en particular entre la red de servicio y el UE, ya que cualquier suplantación o modificación de g^x mientras está en tránsito sería detectada por la verificación de AUTN en el USIM en el UE.

Con referencia a las Figs. 4 y 7, esto significa que las modificaciones o fabricaciones del primer parámetro PFS1 de PFS implicarán que, con alta probabilidad, el AUTN (más precisamente el subcampo MAC) será incorrecto. La verificación de AUTN luego fallará internamente en el USIM 48 y el USIM ni siquiera proporcionará ninguno de los parámetros de resultados.

La autenticidad del primer parámetro de PFS se determina, por tanto, basado en el USIM 48 que proporciona al menos un parámetro de resultado.

El AuC/HSS puede calcular un valor de RAND más grande y enviarlo en una forma modificada del vector de autenticación (AV) a la MME (entidad de gestión de la movilidad). Otra posibilidad es que la MME reciba un RAND de tamaño regular en el AV y amplíe el RAND añadiendo o anteponiendo un conjunto de bits al RAND antes de transmitirlo al UE. En este último caso, la elección de la función H debe coincidir con cómo la MME extendió el RAND recibido; de lo contrario, el USIM rechazaría el par RAND/AUTN.

El resto de esta segunda realización es idéntica a la primera realización en el caso especial de que AUTN se va a usar para proporcionar el primer código de verificación VC1 (correspondiente a VC1A a continuación), o, de manera equivalente, que el primer parámetro PFS1 de PFS esté codificado en el elemento de información RAND. El funcionamiento de la segunda realización puede ser más particularmente el siguiente y como se muestra en la Fig. 9.

- Como parte de, por ejemplo, la conexión 88 de red, un identificador, por ejemplo, la IMSI (identidad de abonado móvil internacional) se proporciona desde el UE (USIM). Esto se reenvía 10 al HSS.

- El HSS genera 89 el(los) vector(s) de autenticación (AV). Se resaltan algunos componentes nuevos añadidos por esta realización (otras partes generalmente no se ven afectadas). En particular, RAND se genera como g^x como se analizó, y una versión comprimida, RAND', se usa en los cálculos de AKA normales de f1, f2, ... etc. En la respuesta de AV 90, el HSS incluye/añade x (para permitir que la MME posteriormente calcule la clave compartida). Por lo tanto, el HSS puede omitir enviar RAND ya que la MME puede calcular RAND a partir de x. De manera similar, ya que la clave de sesión, K', ahora puede deducirse de los valores DH (g^x y g^y), puede que no siempre sea necesario enviar CK e IK (o claves derivadas de las mismas, por ejemplo, Kasme de LTE). Si CK e IK necesitan transferirse depende de los detalles de la realización como se analizó en otra parte de esta descripción.

- La MME reenvía 20 RAND y AUTN al UE/USIM. Aquí RAND es el desafío, así como el primer parámetro PFS1 de PFS y el campo MAC de AUTN es el primer código de verificación VC1A para el primer parámetro PFS1 de PFS ya que se ha calculado en dependencia de RAND, que también es, en efecto, g^x.

- El UE (por ejemplo, la parte ME) calcula RAND' = H (RAND) y lo envía 92 al USIM para la derivación del parámetro AKA (RES, CK, IK). Como se indica, cuando el USIM verifica internamente la parte MAC de AUTN, esto también sirve para verificar la autenticidad de g^x.

- El USIM puede responder 94 por RES, CK, IK. A través del ME que recibe esta respuesta, también es capaz de determinar que el primer parámetro PFS1 de PFS es auténtico, ya que de lo contrario no se proporcionaría una respuesta que comprenda estos parámetros.

- El UE genera 96 un valor de DH g^y e información de autenticación asociada. Genera, por tanto, un segundo parámetro PFS2 de PFS y un segundo código de verificación VC2A. El segundo código de verificación VC2A podría realizarse como un valor RES' de forma MAC (Kd || ..., g^y || ...). El formato exacto (qué clave Kd usar, etc.) de la información de autenticación puede variar:

    - En una variación, solo RES se usa como base para la clave Kd.

    - En otra variación, RES y al menos una de CK, IK se usan como base para Kd (esto supone que el HSS los incluyó cuando genera los vectores de autenticación). También es posible usar Kasme como base para Kd. Por tanto, el segundo código de verificación VC2A puede generarse como RES' a través de RES que se usa como base para la clave Kd. Tenga en cuenta que si RES no se incluye en la derivación de la autenticación/respuesta RES', es posible que el ME necesite enviar también RES. En general, RES' puede reemplazar a RES de los protocolos AKA actuales, o, puede enviarse como un parámetro adicional, junto con RES:

    - El ME luego envía 24 g^y y RES' a la MME.

- La MME puede realizar los cálculos correspondientes 98 para verificar RES' y calcular la clave compartida K'. Además de la dependencia de g^(xy), K' también se podría calcular en dependencia de CK, IK (o una clave Kasme), si la suministra el HSS, por ejemplo, K' = G(g^(xy), CK, IK, ...) para una función de derivación de clave G. Otras claves (por ejemplo, para protección de datos tal como cifrado) pueden derivarse de K' por UE y MME (no mostrada).

En una variación de la segunda realización, el desafío usado es un hash de g^x. Esto significa que el RAND que es generado por el HSS y enviado por la MME al UE es un hash de g^x. Esto tendría que ir acompañado también de g^x. De este modo RAND puede enviarse directamente desde el ME al USIM sin que el ME calcule un hash del mismo.

En una tercera realización, el segundo nodo puede que no necesite realizar ninguna etapa que no sea parte de las especificaciones actuales de AKA. Mientras existen algunas opciones a continuación en las que el segundo nodo realiza etapas adicionales a las especificaciones de AKA actuales, estas etapas son opcionales y se pueden evitar si así se desea.

En esta realización, el parámetro RAND no se usa para transferir o transportar información sobre g^x desde la red (red de servicio o doméstica) al UE. En consecuencia, AUTN tampoco puede usarse para transportar el primer código de verificación. En su lugar, la red transmite el RAND por separado al UE e incluye g^x en un nuevo elemento de información en el mismo mensaje que el RAND. Como se indica, la transmisión puede originarse en el HSS, o, puede originarse en la MME (por ejemplo, la MME genera localmente una x aleatoria). En este caso, el g^x necesita autenticarse y la red (de servicio o doméstica) también incluye un MAC adicional calculado sobre el g^x en el mensaje. La clave para este MAC puede ser, por ejemplo, RES, o una de CK/IK o ambas. También pueden ser derivadas de los mismas tal como Kasme. La función H sería la función de identidad en esta realización. De este modo la derivada se vuelve idéntica al desafío. Un beneficio de esta realización es que la red de servicio (por ejemplo, la MME) puede elegir el valor x y no es necesario señalizar esto entre la red de servicio y el AuC/HSS. De hecho, se puede reutilizar la misma señalización entre estos nodos que se usa hoy en día. Un inconveniente es que el RAND de 128 bits necesita enviarse desde la red de servicio al UE, así como el valor g^x mayor. Por lo tanto, se requiere algo más de ancho de banda a través de la interfaz aérea.

La tercera realización se describirá ahora con más detalle con la referencia que se hace a la Fig. 10, que muestra un gráfico de señalización que incluye a USIM, ME, MME y HSS.

- El funcionamiento puede comenzar con la MME enviando 10 una solicitud para vectores de autenticación al HSS, que responde 100 con una respuesta de vector de autenticación que comprende RAND, AUTN, XRES y la clave de sesión Kasme. Luego, la MME genera el primer parámetro PFS1 de PFS así como genera el primer código de verificación VC1B, donde el primer parámetro PFS1 de PFS puede generarse como g^x y el primer código de verificación VC1B puede generarse como MAC(g^x) usando, por ejemplo, XRES o Kasme como clave común. Cuando se ha hecho esto, la MME envía el mensaje 20 de solicitud de autenticación al ME del UE. La solicitud de autenticación en este caso comprende RAND, AUTN, g^x y MAC(g^x). Luego, el ME reenvía 102 el desafío RAND y el código de verificación del desafío como parte de AUTN al USIM, que responde 104 con las claves CK/IK y el parámetro de respuesta RES. De este modo el USIM ha respondido correctamente al desafío. El ME luego autentica el primer parámetro PFS1 de PFS usando el primer código de verificación VC1B, que en este caso se puede hacer a través del primer código de verificación VC1B que se genera a través de una clave común, que en este caso fue XRES (que es idéntica al valor del parámetro de respuesta RES en el ME). El ME luego genera un segundo parámetro PFS2 de PFS y un segundo código de verificación VC2B, donde el segundo parámetro PFS2 de PFS, puede generarse como g^y y el segundo código de verificación VC1B puede generarse

como MAC(g^y) usando cualquiera de CK/IK, Kasme o RES, lo que sea conocido por la MME, y los envía junto con el resultado RES en el mensaje de respuesta de autenticación 24. La MME luego verifica el resultado a través de la comparación de RES con XRES y también verifica g^y usando MAC(g^y) y la clave apropiada, por ejemplo, CK/IK o XRES, etc. A continuación, el ME calcula 106 una clave de sesión K' como una función de g^(xy), cuya función es típicamente un hash de g^(xy). También la MME calcula 108 una clave de sesión K' como la misma función de g^(xy).

De este modo el UE puede comunicarse con la primera red inalámbrica con seguridad mejorada.

Debe tenerse en cuenta que también en esta tercera realización, es posible usar RES' como segundo código de verificación, por ejemplo, si la clave usada para calcular el segundo código de verificación VC2B es dependiente de RES como en las realizaciones anteriores.

Tenga en cuenta que todas las realizaciones pueden combinarse con la invención descrita en la patente US 7,194,765. En este caso, el HSS no proporcionará XRES a la MME, sino más bien XRES' = H(XRES). El UE puede luego señalizar explícitamente RES a la MME para que MME pueda calcular y verificar XRES'. En este caso, al menos uno de CK e IK (o alguna clave derivada de ellas) debe incluirse en el cálculo de RES'.

Tenga en cuenta de nuevo que ya que GBA y EAP-AKA hacen uso de AKA, un experto en la técnica se dará cuenta después de esta descripción de que las realizaciones descritas también pueden aplicarse en esos contextos con modificaciones sencillas. Una ventaja de al menos una de las realizaciones de la descripción añade PFS a la autenticación de red, por ejemplo, autenticación de red móvil, a un costo bajo o incluso mínimo, que permite y/o garantiza la compatibilidad con versiones anteriores de la interfaz entre la SIM y el ME (SIM-ME, por sus siglas en inglés) para el protocolo AKA. Otra ventaja de al menos una de las realizaciones de la descripción es que limita los efectos de compromisos de clave a largo plazo, tal como los HSS pirateados y los sitios de proveedores de tarjetas inteligentes pirateados. Otras ventajas incluyen evitar el uso de transmisiones adicionales, lo que a su vez ahorra energía.

El código de programa informático de un equipo móvil puede estar en la forma de un producto de programa informático, por ejemplo, en la forma de un medio de almacenamiento de datos, tal como un disco CD ROM o un lápiz de memoria. En este caso, el medio de almacenamiento de datos transporta un programa informático con el código del programa informático, que implementará la funcionalidad del equipo móvil descrito anteriormente. Uno de tales medios 110 de almacenamiento de datos con código 112 de programa informático se muestra esquemáticamente en la Fig. 12.

El código del programa informático del primer dispositivo de red puede estar en la forma de un producto de programa informático, por ejemplo, en la forma de un medio de almacenamiento de datos, tal como un disco CD ROM o un lápiz de memoria. En este caso, el medio de almacenamiento de datos transporta un programa informático con el código del programa informático, que implementará la funcionalidad del primer dispositivo de red descrito anteriormente. Uno de tales medios 114 de almacenamiento de datos con código 116 de programa informático se muestra esquemáticamente en la Fig. 13.

Como se muestra esquemáticamente en la Fig. 14, el dispositivo 40 de comunicación puede comprender en algunas realizaciones:

una unidad 118 de recepción para recibir un desafío, un primer parámetro de PFS y un primer código de verificación de un dispositivo de red,

una unidad 120 de reenvío para reenviar el desafío o un derivado del mismo a un módulo de identidad,

una unidad 122 de recepción para recibir al menos un parámetro de resultado como respuesta del módulo de identidad,

una unidad 124 de determinación para determinar, basado en el parámetro de resultado, si el primer parámetro de PFS es auténtico, y

una unidad 126 de generación para generar y enviar un segundo parámetro de PFS al dispositivo de red si la determinación es que el primer parámetro de PFS es auténtico. En una realización, las unidades corresponden a instrucciones de software. En otra realización, las unidades se implementan como unidades de hardware en uno o más circuitos de hardware, como circuitos integrados específicos de aplicación (en inglés, Application Specific Integrated Circuits, ASIC) o matrices de puertas programables en campo (en inglés, Field Programmable Gate Arrays, FPGA).

El dispositivo de comunicación puede comprender además una unidad de generación para generar una clave de sesión para la comunicación entre el dispositivo de comunicación y el dispositivo de red, donde la clave de sesión se basa al menos en valores usados para generar el primer y segundo parámetro de PFS.

La unidad 118 de recepción para recibir un desafío, un primer parámetro de PFS y un primer código de verificación puede ser además una unidad de recepción para recibir el desafío, el primer parámetro de PFS y el primer código de verificación del dispositivo de red en un mensaje de solicitud de autenticación, donde el mensaje de solicitud de

autenticación también comprende un código de verificación del desafío. La unidad 122 de recepción para recibir al menos un parámetro de resultado puede ser a su vez una unidad de recepción para recibir un parámetro de respuesta como respuesta al desafío y la unidad 126 de generación puede ser una unidad de generación para generar el segundo parámetro de PFS junto con un segundo código de verificación y enviarlos en un mensaje de respuesta de autenticación que también comprende el parámetro de respuesta.

La unidad 124 de determinación puede ser además una unidad de determinación para determinar la autenticidad del primer parámetro de PFS usando un primer código de verificación comprendido en un elemento de información separado correspondiente del mensaje de solicitud de autenticación.

Si el primer código de verificación se proporciona como al menos parte del código de verificación del desafío, la unidad 124 de determinación puede ser además una unidad de determinación para determinar la autenticidad del primer parámetro de PFS basado en el módulo de identidad que proporciona el al menos un parámetro de resultado.

La unidad 126 de generación también puede ser una unidad de generación para generar el segundo código de verificación basado en el parámetro de respuesta y enviar el segundo código de verificación en un elemento de información del mensaje de respuesta de autenticación asignado al parámetro de respuesta.

Como se muestra en la Fig. 15, el primer dispositivo 44 de red puede comprender en algunas realizaciones

una unidad 128 de obtención para obtener un desafío,

una unidad 130 de obtención para obtener un primer parámetro de PFS,

una unidad 132 de obtención para obtener un primer código de verificación para el primer parámetro de PFS,

una unidad 134 de envío para enviar el desafío, el primer parámetro de PFS y el primer código de verificación al dispositivo de comunicación,

una unidad 136 de recepción para recibir un segundo parámetro de PFS, un segundo código de verificación y un parámetro de respuesta del dispositivo de comunicación,

una unidad 138 de determinación para determinar la autenticidad del parámetro de respuesta, y

una unidad 140 de verificación para verificar el segundo parámetro de PFS basado en el segundo código de verificación.

En una realización, las unidades corresponden a instrucciones de software. En otra realización, las unidades se implementan como unidades de hardware en uno o más circuitos de hardware, como ASIC o FPGA.

El primer dispositivo 44 de red puede comprender además una unidad de cálculo para calcular una clave de sesión para la comunicación entre el dispositivo de comunicación y el primer dispositivo de red, donde la clave de sesión se basa al menos en los valores usados para generar el primer y segundo parámetro de PFS.

La unidad 128 de obtención para obtener el desafío también puede ser una unidad de obtención para obtener un código de verificación del desafío, la unidad 134 de envío puede ser una unidad de envío para enviar el desafío, el primer parámetro de PFS y el primer código de verificación en un mensaje de solicitud de autenticación junto con el código de verificación del desafío y la unidad 136 de recepción puede ser una unidad de recepción para recibir el segundo parámetro de PFS, el segundo código de verificación y el parámetro de respuesta en un mensaje de respuesta de autenticación.

La unidad 132 de obtención para obtener la primera verificación puede comprender una unidad de generación para generar el primer código de verificación usando el primer parámetro de PFS y la unidad 134 de envío puede ser una unidad de envío para enviar el primer código de verificación en un elemento de información separado correspondiente del mensaje de solicitud de autenticación.

El primer dispositivo de red también puede comprender una unidad de recepción para recibir un valor x que se va a usar en la generación del primer parámetro de PFS. El valor x, que es un valor exponente, también puede denominarse valor semilla. En este caso, la unidad 132 de obtención para obtener el primer código de verificación puede ser una unidad de obtención para obtener el primer código de verificación como al menos parte del código de verificación del desafío y la unidad 134 de envío puede ser una unidad de envío para enviar el primer código de verificación como al menos parte del código de verificación del desafío en el mensaje de solicitud de autenticación.

La unidad 128 de obtención para obtener el desafío también puede ser una unidad de obtención para obtener un resultado de desafío esperado y la unidad 138 de determinación puede ser una unidad de determinación para determinar la autenticidad del parámetro de respuesta a través de una comparación con el resultado de desafío esperado.

El parámetro de respuesta puede incluirse en el mensaje de respuesta de autenticación a través del segundo código de verificación que se basa en el parámetro de respuesta. En este caso, la unidad 136 de recepción puede ser una unidad de recepción para recibir el segundo código de verificación en un elemento de información del mensaje de respuesta de autenticación asignado al parámetro de respuesta y la unidad 138 de determinación y la unidad 140 de verificación pueden ser una unidad combinada de determinación y verificación para determinar simultáneamente la autenticidad del parámetro de respuesta y verificar el segundo parámetro de PFS usando el segundo código de verificación.

Como se muestra esquemáticamente en la Fig. 16, el segundo dispositivo de red puede, a su vez, en algunas realizaciones comprender una unidad 14 de envío para enviar un desafío al primer dispositivo de red.

Puede comprender además una unidad 144 de suministro para proporcionar un valor para que el primer parámetro de PFS se obtenga a través de generarlo al menos basado en el valor x, una unidad generadora para generar el código de verificación del desafío usando el primer parámetro de PFS y una unidad de envío para enviar el valor al primer dispositivo de red.

En una realización, las unidades corresponden a instrucciones de software. En otra realización, las unidades se implementan como unidades de hardware en uno o más circuitos de hardware, como ASIC o FPGA.

Mientras la invención se ha descrito en relación con lo que actualmente se considera las realizaciones más prácticas y preferidas, debe entenderse que la invención no se limita a las realizaciones descritas, sino que, por el contrario, se pretende abarcar diversas modificaciones y disposiciones equivalentes. Por lo tanto, la invención solo está limitada por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un dispositivo (40) de comunicación para comunicarse con un dispositivo (44) de red de una red (36) de comunicación, estando el dispositivo (40) de comunicación operativo para:

recibir un desafío (RAND), un primer parámetro (PFS1) de secreto perfecto hacia adelante, PFS, y un primer código de verificación (VC1; VC1A; VC1B) para el primer parámetro (PFS1) de PFS del dispositivo (44) de red, en donde el primer código de verificación (VC1A; VC1B) comprende un código de autenticación de mensajes basado en al menos el primer parámetro (PFS1) de PFS;

reenviar un derivado de dicho desafío a un módulo (48) de identidad;

recibir al menos un parámetro de resultado (CK/IK, RES) como respuesta del módulo (48) de identidad;

determinar, basándose en dicho parámetro de resultado (CK/IK, RES) si dicho primer parámetro (PFS1) de PFS es auténtico; y

generar y enviar un segundo parámetro (PFS2) de PFS al dispositivo (44) de red si dicha determinación es que el primer parámetro (PFS1) de PFS es auténtico.

2. Un dispositivo (40) de comunicación para comunicarse con un dispositivo (44) de red de una red (36) de comunicación, estando el dispositivo (40) de comunicación operativo para:

recibir un desafío (RAND), un primer parámetro (PFS1) de secreto perfecto hacia adelante, PFS, y un primer código de verificación (VC1; VC1A; VC1B) para el primer parámetro (PFS1) de PFS del dispositivo (44) de red, en donde el primer código de verificación (VC1A; VC1B) comprende un código de autenticación de mensajes basado en al menos el primer parámetro (PFS1) de PFS;

reenviar dicho desafío a un módulo (48) de identidad;

recibir al menos un parámetro de resultado (CK/IK, RES) como respuesta del módulo (48) de identidad;

determinar, basándose en dicho parámetro de resultado (CK/IK, RES) si dicho primer parámetro (PFS1) de PFS es auténtico; y

generar y enviar un segundo parámetro (PFS2) de PFS al dispositivo (44) de red si dicha determinación es que el primer parámetro (PFS1) de PFS es auténtico.

3. El dispositivo (40) de comunicación según la reivindicación 1 o 2, estando además operativo para generar una clave de sesión (K') para la comunicación entre el dispositivo (40) de comunicación y el dispositivo (44) de red, estando dicha clave de sesión basada en al menos los valores (x, y) usados para generar el primer y segundo parámetro (PFS1, PFS2) de PFS.

4. El dispositivo (40) de comunicación según la reivindicación 3, en donde la clave de sesión se basa en el primer parámetro (PFS1) de PFS y un exponente (y) del segundo parámetro (PFS2) de PFS.

5. El dispositivo (40) de comunicación según cualquiera de las reivindicaciones 1 a 4, en donde el dispositivo de comunicación comprende un equipo móvil (46) que está operativo para recibir el desafío (RAND), realizar dicho reenvío, recibir el al menos un parámetro de resultado, determinar si el primer parámetro (PFS1) de PFS es auténtico y generar y enviar un segundo parámetro (PFS2) de PFS.

6. El dispositivo (40) de comunicación según cualquier reivindicación anterior, en donde el dispositivo de comunicación comprende el módulo (48) de identidad, dicho módulo (48) de identidad comprende una clave y un medio de procesamiento criptográfico.

7. El dispositivo (40) de comunicación según cualquier reivindicación anterior, en donde el primer y segundo parámetro de PFS son parámetros Diffie-Hellman.

8. El dispositivo (40) de comunicación según cualquiera de las reivindicaciones 1 o 3 a 7, cuando depende de la reivindicación 1, en donde la derivada es un hash del desafío.

9. El dispositivo (40) de comunicación según cualquier reivindicación anterior, cuando está operativo para recibir el desafío (RAND), el primer parámetro (PFS1) de PFS y el primer código de verificación (VC1; VC1A; VC1B) está operativo para recibirlos en un mensaje (20) de solicitud de autenticación del dispositivo (44) de red, el mensaje de solicitud de autenticación también comprende un código de verificación del desafío (AUTN), cuando está operativo para recibir el al menos un parámetro de resultado (CK/IK, RES) está operativo para recibir un parámetro de respuesta (RES) como respuesta a dicho desafío, y cuando está operativo para generar y enviar el segundo parámetro (PFS2) de PFS está operativo para generar el segundo parámetro de PFS junto con un segundo código de verificación (VC2;

VC2A; VC2B) y enviarlos en un mensaje (24) de respuesta de autenticación que también comprende el parámetro de respuesta (RES).

10. Un método para un dispositivo (40) de comunicación en comunicación con un dispositivo (44) de red de una red (36) de comunicación, el método que es realizado por el dispositivo (40) de comunicación y que comprende:

recibir (64) un desafío (RAND), un primer parámetro (PFS1) de secreto perfecto hacia adelante, PFS, y un primer código de verificación (VC1; VC1A; VC1B) para el primer parámetro (PFS1) de PFS del dispositivo (44) de red, en donde el primer código de verificación (VC1A; VC1B) comprende un código de autenticación de mensajes basado en al menos el primer parámetro (PFS1) de PFS;

reenviar (65) un derivado de dicho desafío a un módulo (48) de identidad;

recibir (66) al menos un parámetro de resultado (CK/IK, RES) como respuesta del módulo (48) de identidad;

determinar, (68) basado en dicho parámetro de resultado (CK/IK, RES) si dicho primer parámetro (PFS1) de PFS es auténtico; y

generar (70) y enviar (72) un segundo parámetro (PFS2) de PFS al dispositivo (44) de red si dicha determinación es que el primer parámetro (PFS1) de PFS es auténtico.

11. Un método para un dispositivo (40) de comunicación en comunicación con un dispositivo (44) de red de una red (36) de comunicación, el método que es realizado por el dispositivo (40) de comunicación y que comprende:

recibir (64) un desafío (RAND), un primer parámetro (PFS1) de secreto perfecto hacia adelante, PFS, y un primer código de verificación (VC1; VC1A; VC1B) para el primer parámetro (PFS1) de PFS del dispositivo (44) de red, en donde el primer código de verificación (VC1A; VC1B) comprende un código de autenticación de mensajes basado en al menos el primer parámetro (PFS1) de PFS;

reenviar (65) dicho desafío a un módulo (48) de identidad;

recibir (66) al menos un parámetro de resultado (CK/IK, RES) como respuesta del módulo (48) de identidad;

determinar, (68) basado en dicho parámetro de resultado (CK/IK, RES) si dicho primer parámetro (PFS1) de PFS es auténtico; y

generar (70) y enviar (72) un segundo parámetro (PFS2) de PFS al dispositivo (44) de red si dicha determinación es que el primer parámetro (PFS1) de PFS es auténtico.

12. Un primer dispositivo (44) de red de una primera red (36) de comunicaciones, el primer dispositivo (44) de red que está operativo para:

obtener un desafío (RAND);

obtener un primer parámetro (PFS1) de secreto perfecto hacia adelante, PFS,

obtener un primer código de verificación (VC1; VC1A; VC1B) para el primer parámetro (PFS1) de PFS, en donde el primer código de verificación (VC1A; VC1B) comprende un código de autenticación de mensajes basado en al menos el primer parámetro (PFS1) de PFS;

enviar el desafío (RAND), el primer parámetro (PFS1) de PFS y el primer código de verificación (VC1; VC1A; VC1B) a un dispositivo (40) de comunicación;

recibir un segundo parámetro (PFS2) de PFS, un segundo código de verificación (VC2; VC2A; VC2B) y un parámetro de respuesta (RES) del dispositivo (40) de comunicación;

determinar la autenticidad del parámetro de respuesta; y

verificar el segundo parámetro (PFS2) de PFS basado en el segundo código de verificación (VC2; VC2A; VC2B).

13. El primer dispositivo (44) de red según la reivindicación 12, que está además operativo para calcular una clave de sesión (K') para la comunicación entre el dispositivo (40) de comunicación y el primer dispositivo (44) de red, dicha clave de sesión se basa al menos en los valores (x, y) usados para generar el primer y segundo parámetro (PFS1, PFS2) de PFS.

14. El primer dispositivo (44) de red según la reivindicación 12 o 13, en donde la clave de sesión se basa en el segundo parámetro (PFS2) de PFS y un exponente (x) del primer parámetro (PFS1) de PFS.

15. El primer dispositivo (44) de red según cualquiera de las reivindicaciones 12-14, que cuando está operativo para obtener el desafío está operativo también para obtener un código de verificación del desafío (AUTN), que cuando está

operativo para enviar el desafío (RAND), el primer parámetro (PFS1) de PFS y el primer código de verificación (VC1; VC1A; VC1B) está operativo para enviarlos en un mensaje (20) de solicitud de autenticación junto con el código de verificación del desafío (AUTN) y que cuando está operativo para recibir el segundo parámetro (PFS2) de PFS, el segundo código de verificación (VC2; VC2A; VC2B) y el parámetro de respuesta (RES) está operativo para recibirlos en un mensaje (24) de respuesta de autenticación.

16. Un método para un primer dispositivo (44) de red de una primera red (36) de comunicación, el método que es realizado por el primer dispositivo (44) de red y que comprende las etapas de:

obtener (74) un desafío (RAND),

obtener (76) un primer parámetro (PFS1) de secreto perfecto hacia adelante, PFS, obtener (78) un primer código de verificación (VC1; VCiA; VC1B) para el primer parámetro de PFS, en donde el primer código de verificación (VC1A; VC1B) comprende un código de autenticación de mensajes basado en al menos el primer parámetro (PFS1) de PFS;

enviar (80) el desafío (RAND), el primer parámetro (PFS1) de PFS y el primer código de verificación (VC1; VC1A; VC1B) a un dispositivo (40) de comunicación;

recibir (82) un segundo parámetro (PFS2) de PFS, un segundo código de verificación (VC2; VC2A; VC2B) y un parámetro de respuesta (RES) del dispositivo (40) de comunicación;

determinar (84) la autenticidad del parámetro de respuesta; y

verificar (86) el segundo parámetro (PFS2) de PFS basado en segundo código de verificación (VC2; VC2A; VC2B).

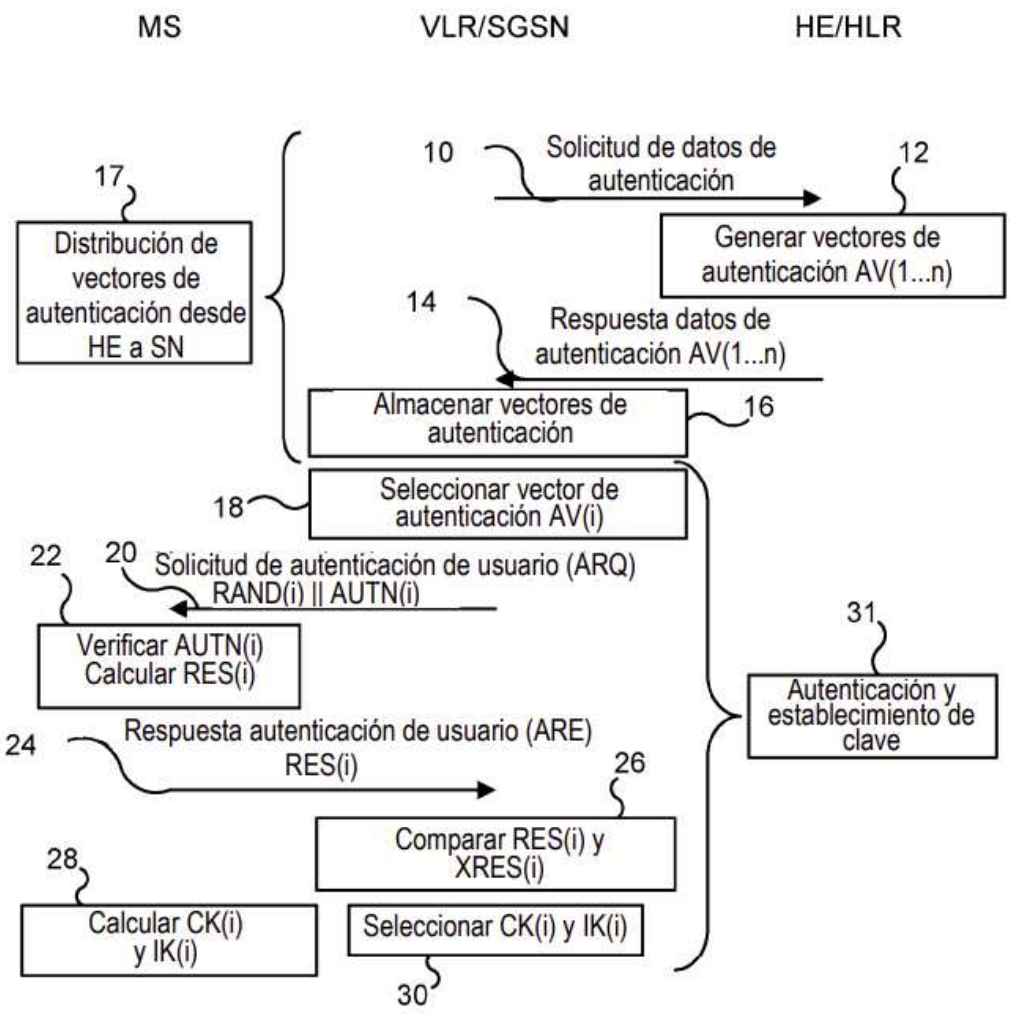
MS
VLR/SGSN
HE/HLR
10
Solicitud de datos de autenticación
12
Generar vectores de autenticación AV(1...n)
17
Distribución de vectores de autenticación desde HE a SN
14
Respuesta datos de autenticación AV(1...n)
Almacenar vectores de autenticación
16
18
Seleccionar vector de autenticación AV(i)
22
20
Solicitud de autenticación de usuario (ARQ)
RAND(i) || AUTN(i)
31
Verificar AUTN(i)
Calcular RES(i)
Autenticación y establecimiento de clave
24
Respuesta autenticación de usuario (ARE)
RES(i)
26
Comparar RES(i) y XRES(i)
28
Calcular CK(i) y IK(i)
Seleccionar CK(i) y IK(i)
30

Fig. 1

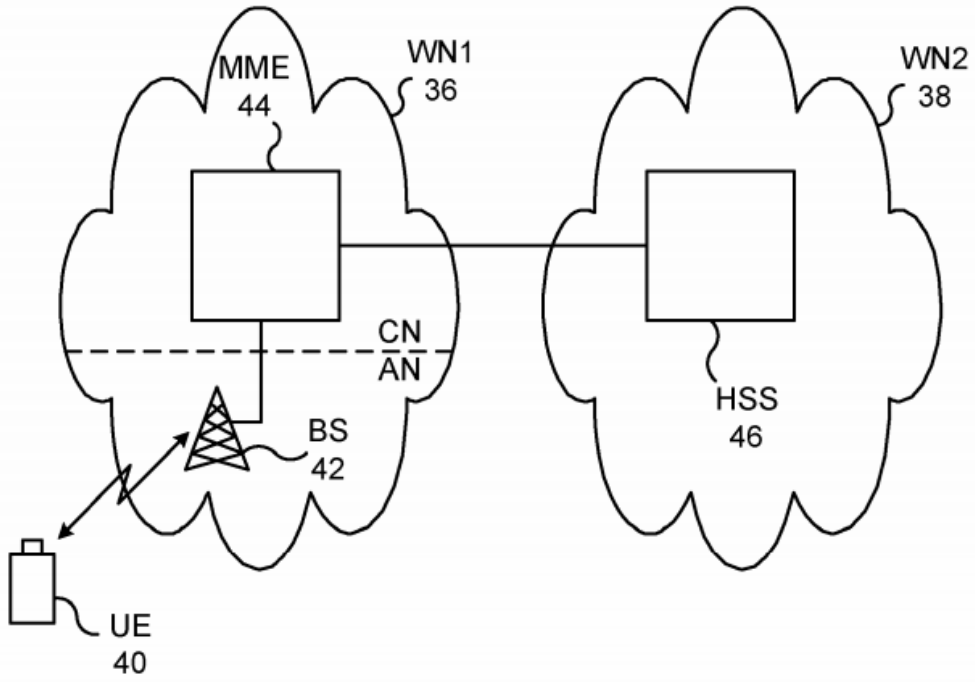

Fig. 2

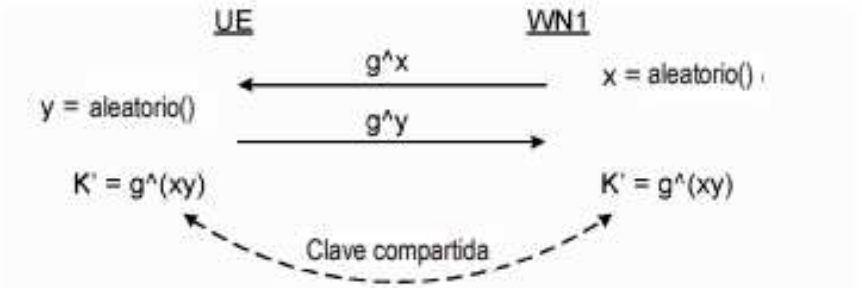

Fig. 3

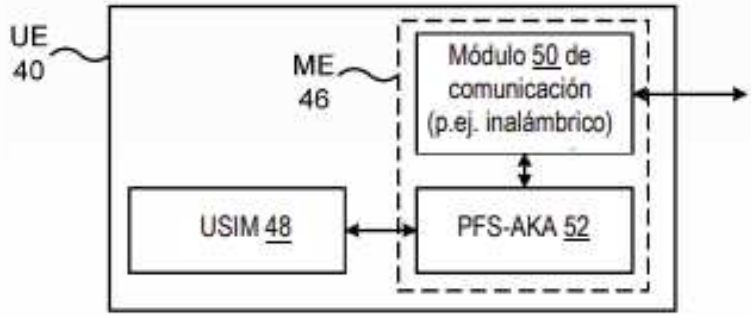

Fig. 4

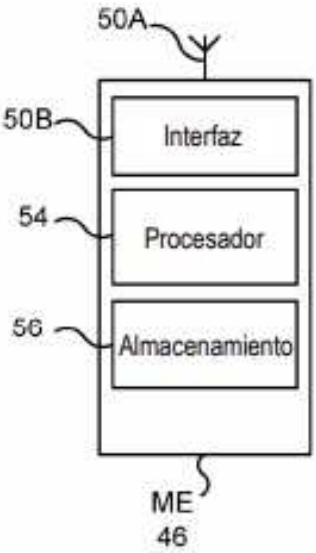

Fig. 5

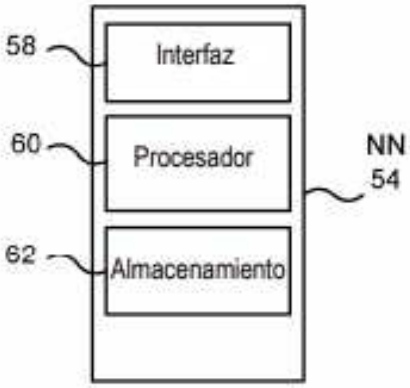

Fig. 6

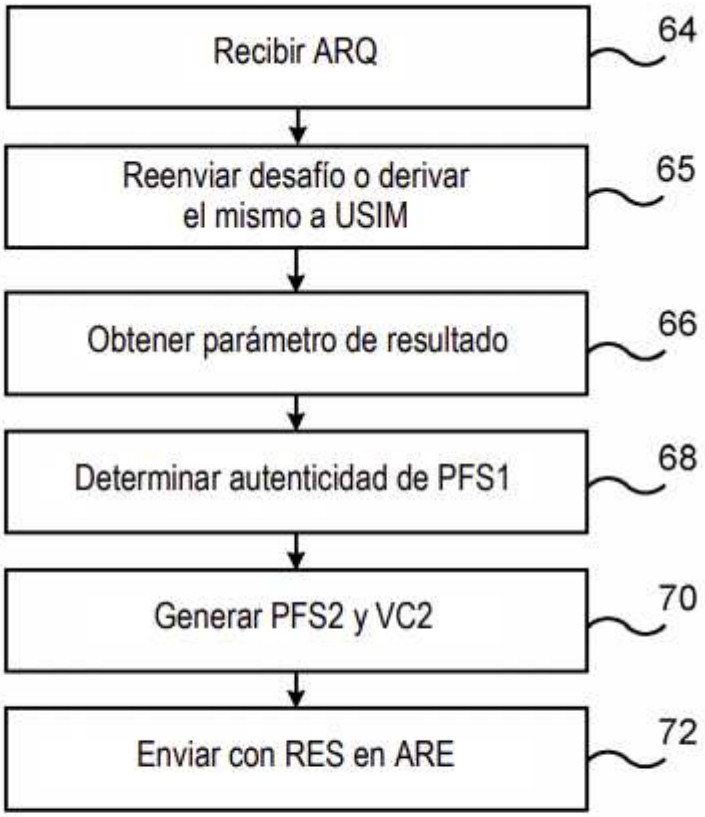
Recibir ARQ
64
Reenviar desafío o derivar el mismo a USIM
65
Obtener parámetro de resultado
66
Determinar autenticidad de PFS1
68
Generar PFS2 y VC2
70
Enviar con RES en ARE
72

Fig. 7

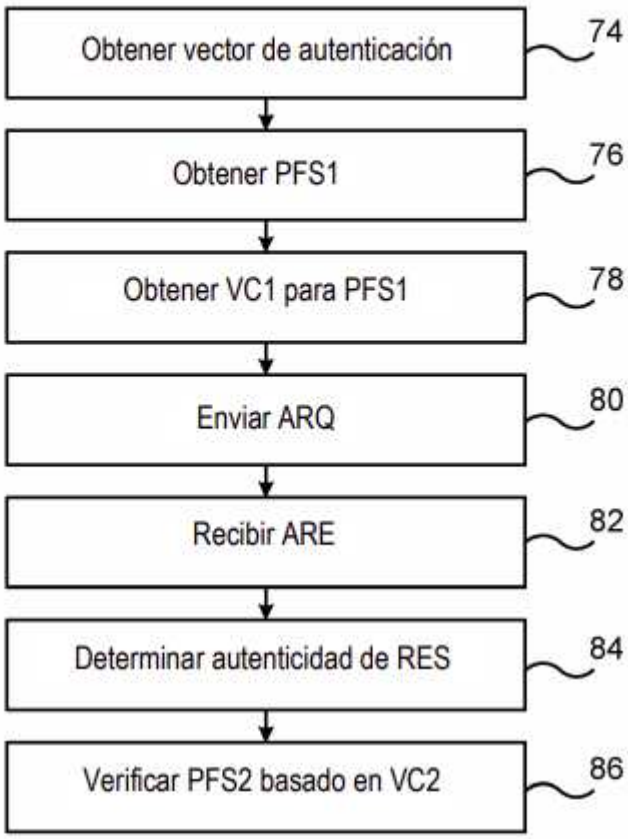
Obtener vector de autenticación
74
Obtener PFS1
76
Obtener VC1 para PFS1
78
Enviar ARQ
80
Recibir ARE
82
Determinar autenticidad de RES
84
Verificar PFS2 basado en VC2
86

Fig. 8

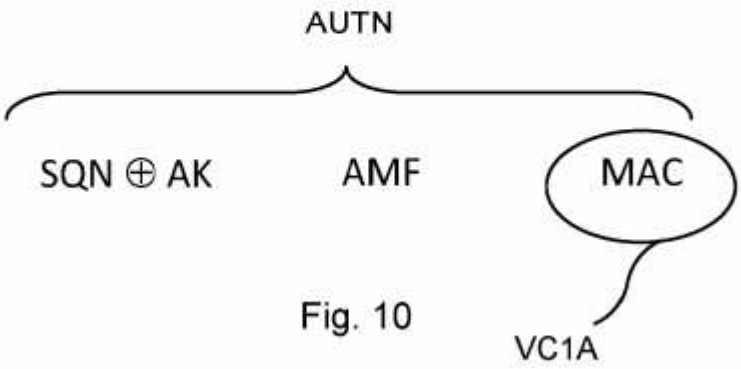
AUTN
SQN ⊕ AK
AMF
MAC
VC1A

Fig. 10

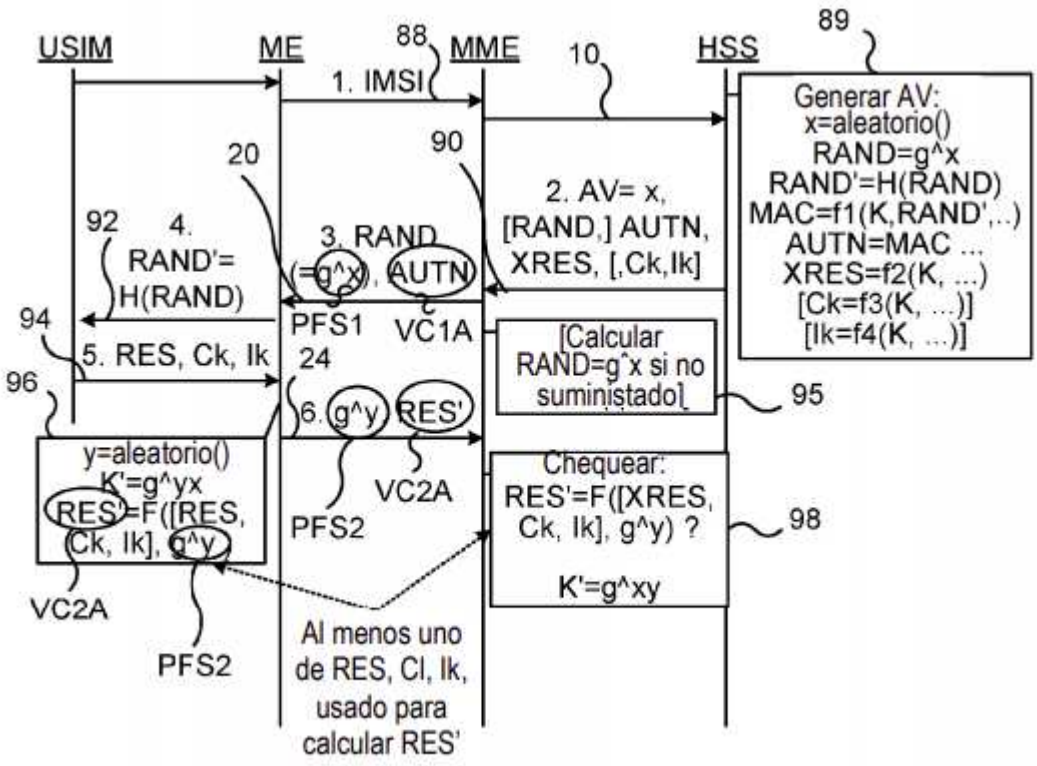
USIM
ME
88
MME
10
HSS
89
1. IMSI
Generar AV:
x=aleatorio()
RAND=g^x
RAND'=H(RAND)
MAC=f1(K,RAND',..)
AUTN=MAC ...
XRES=f2(K, ...)
[Ck=f3(K, ...)]
[Ik=f4(K, ...)]
20
90
2. AV= x,
[RAND,] AUTN,
XRES, [,Ck,Ik]
92
4.
RAND'=
H(RAND)
3. RAND
(=g^x), AUTN
94
PFS1
VC1A
[Calcular
RAND=g^x si no
suministado]
95
5. RES, Ck, Ik
24
96
6. g^y
RES'
y=aleatorio()
K'=g^yx
RES'=F([RES,
Ck, Ik], g^y)
VC2A
Chequear:
RES'=F([XRES,
Ck, Ik], g^y) ?
98
K'=g^xy
PFS2
VC2A
PFS2
Al menos uno
de RES, CI, Ik,
usado para
calcular RES'

Fig. 9

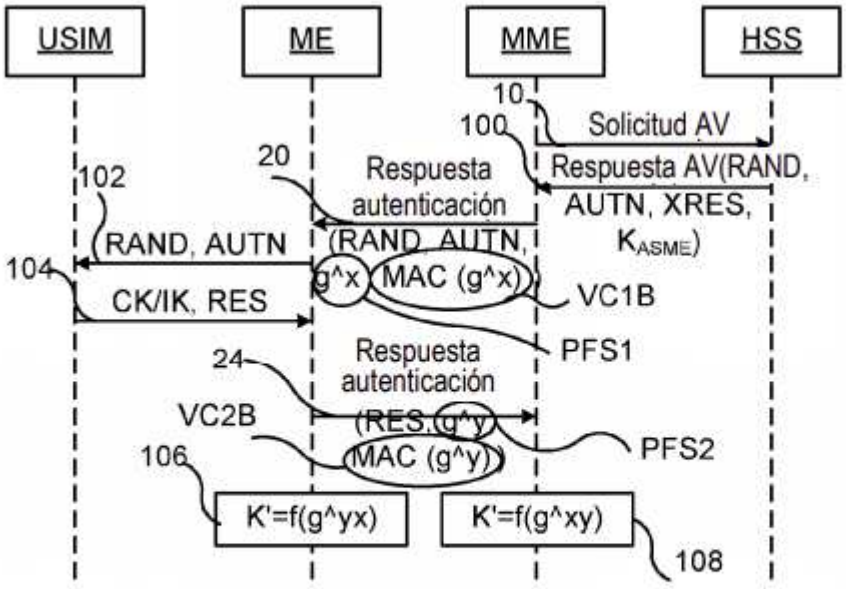
USIM
ME
MME
HSS
10
100
Solicitud AV
20
Respuesta
autenticación
Respuesta AV(RAND,
AUTN, XRES,
K_{ASME})
102
RAND, AUTN
(RAND, AUTN,
g^x, MAC (g^x))
104
CK/IK, RES
VC1B
PFS1
24
Respuesta
autenticación
VC2B
(RES, g^y,
MAC (g^y))
PFS2
106
K'=f(g^yx)
K'=f(g^xy)
108

Fig. 11

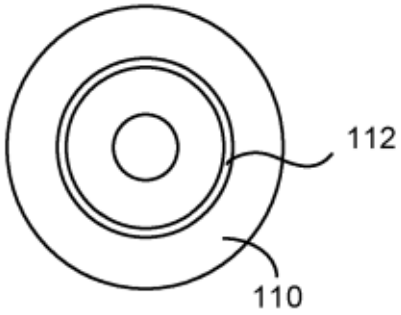

Fig. 12

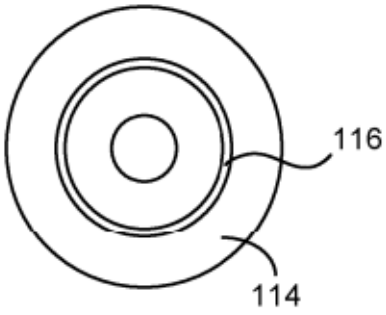

Fig. 13

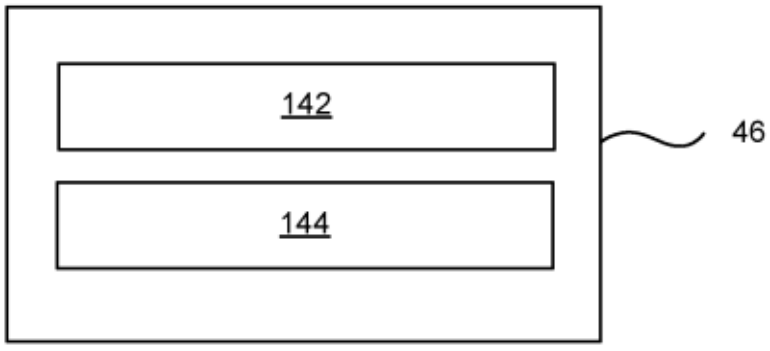

Fig. 16

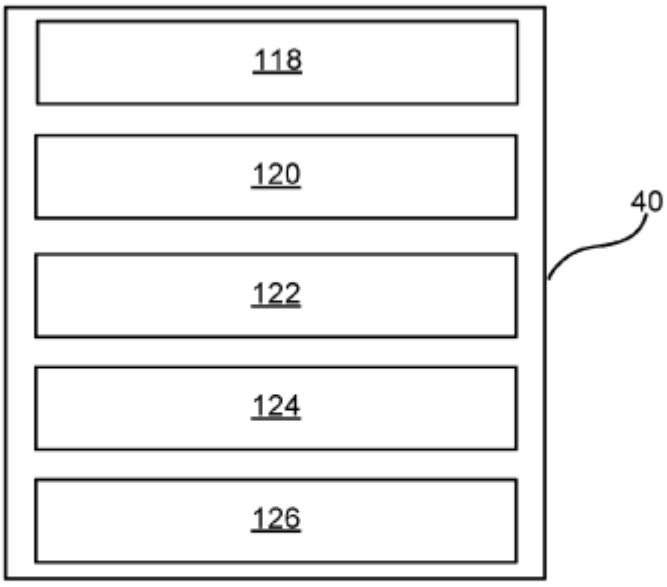

Fig. 14

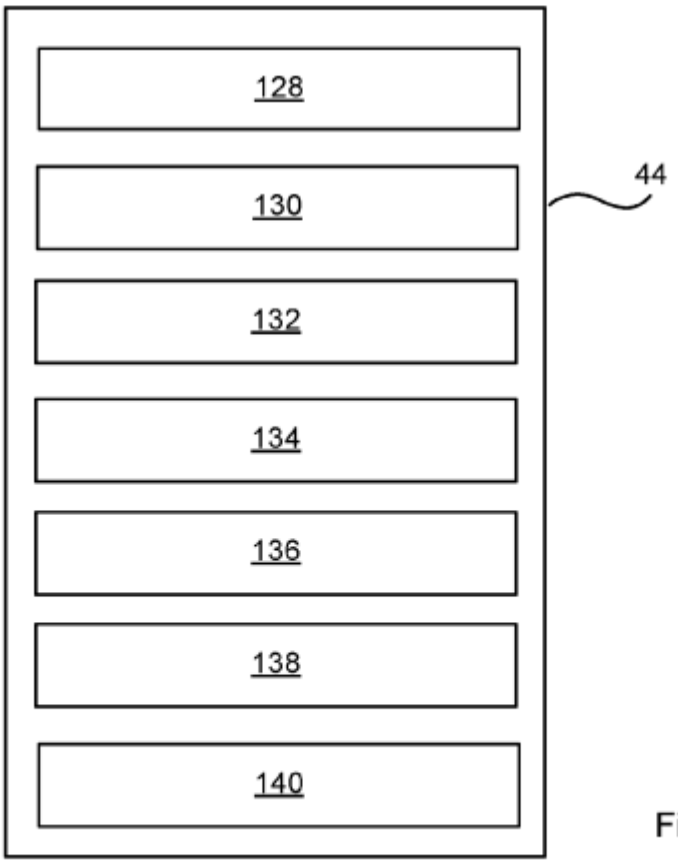

Fig. 15