(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 526 703**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.08.2006 E 06779195 (4)**

(97) Fecha y número de publicación de la concesión europea: **26.11.2014 EP 1946479**

(54) Título: **Seguridad de comunicación**

(30) Prioridad:

25.08.2005 GB 0517592

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.01.2015

(73) Titular/es:

VODAFONE GROUP PLC (100.0%)
VODAFONE HOUSE THE CONNECTION
NEWBURY, BERKSHIRE RG14 2FN, GB

(72) Inventor/es:

HOWARD, PETER THOMAS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Seguridad de comunicación

Campo de la invención

La presente invención se refiere a un método y aparato para establecer un canal de comunicación seguro entre un primer dispositivo y un segundo dispositivo a través de una red de comunicación.

Antecedentes de la invención

El proyecto de cooperación de tercera generación (3GPP) ha definido recientemente un nuevo concepto conocido como IMS (Subsistema Multimedia basado en IP). El objetivo del IMS es permitir a usuarios tales como operadores de red de telefonía móvil proporcionar servicios a sus abonados tan eficiente y eficazmente como sea posible. Por ejemplo, la arquitectura IMS soporta los siguientes tipos de comunicación: voz, vídeo, mensajería instantánea, "presencia" (disponibilidad de un usuario para contactar), servicios basados en localización, correo electrónico y web. Otros tipos de comunicación van a ser añadidos probablemente en el futuro.

Esta colección diversa de dispositivos de comunicación requiere una gestión de sesión eficiente debido al número de diferentes aplicaciones y servicios que se desarrollarán para soportar estos tipos de comunicación. El 3GPP ha elegido el Protocolo de Inicio de Sesiones (SIP) para gestionar estas sesiones.

El protocolo SIP es un protocolo basado en sesión diseñado para establecer sesiones de comunicación basadas en IP entre dos o más puntos finales o usuarios. Una vez que se ha establecido una sesión SIP, se puede llevar a cabo una comunicación entre estos puntos finales o usuarios usando una variedad de protocolos diferentes (por ejemplo aquellos diseñados para difusión en forma continua de audio y vídeo). Estos protocolos se definen en los mensajes de inicio de sesión SIP.

Con IMS, los usuarios ya no están restringidos a una llamada de voz o sesión de datos separada.

Se pueden establecer sesiones entre dispositivos móviles que permiten una variedad de tipos de comunicación a ser usados y medios a ser intercambiados. Las sesiones son dinámicas en su naturaleza por que se pueden adaptar para satisfacer las necesidades de los usuarios finales. Por ejemplo, dos usuarios podrían iniciar una sesión con un intercambio de mensajes instantáneos y entonces decidir que desean cambiar a una llamada de voz, posiblemente con vídeo. Esto es todo posible dentro de la estructura IMS. Si un usuario desea enviar un fichero a otro usuario y los usuarios ya tienen una sesión establecida entre sí (por ejemplo, una sesión de voz) la sesión se puede redefinir para permitir que tenga lugar un intercambio del fichero de datos. Esta redefinición de sesión es transparente para el usuario final.

Además del uso de Redes de Acceso Radio UMTS (UTRAN) para acceder a una llamada basada en IMS, también se puede acceder a una llamada basada en IMS mediante redes de acceso alternativas, tales como WLAN, conexiones de banda ancha fijas y similares.

Hay tres planos de operación distintos en la arquitectura IMS: el plano de aplicaciones, el plano de control y el plano de medios.

El plano de aplicaciones incluye distintos tipos de servidores de aplicaciones que son todos entidades SIP. Estos servidores alojan y ejecutan servicios.

El plano de control maneja la señalización de sesión e incluye distintas funciones para procesar el flujo de tráfico de señalización, tales como Funciones de Control de Sesión de Llamada (CSCF), Servidor de Abonado Local (HSS), Función de Control de Pasarela de Medios (MGCF) y Controlador de Funciones de Recursos de Medios (MRFC). Se proporcionan servicios solicitados por el abonado usando protocolos tales como SIP y Diameter.

El plano de medios transporta los flujos de medios directamente entre abonados.

La arquitectura de seguridad IMS actual especificada en la TS 33.203 define un mecanismo para proteger el plano de control IMS. Actualmente, la protección en el plano de medios se basa en los mecanismos de seguridad de red de portador subyacente. Para acceso IMS sobre redes de acceso de Red de Acceso Radio de Borde GSM (GERAN) o UTRAN, esta puede ser suficiente debido a que los mecanismos de seguridad de acceso de GERAN y UTRAN proporcionan un buen nivel de seguridad. No obstante, para acceso IMS sobre banda ancha fija y WLAN, puede ser insuficiente la seguridad de red de portador subyacente.

Hay dos posibles soluciones para proporcionar un canal de comunicación seguro entre un primer dispositivo y un segundo dispositivo. La seguridad se puede proporcionar en el camino entre cada dispositivo y su pasarela de acceso respectiva a un núcleo IMS (este camino que es la parte más vulnerable del canal de comunicación) o se suministra seguridad ventajosamente de una forma extremo a extremo entre los dispositivos respectivos. El planteamiento extremo a extremo es ventajoso debido a que se usa menos recurso de red ya que no se requiere cifrado/descifrado y descifrado/cifrado repetidos en cada pasarela a diferencia de cuando la seguridad se termina en

las pasarelas de acceso respectivas). El planteamiento extremo a extremo también evita restricciones en el encaminamiento del plano de medios.

Aunque es deseable el suministro del canal de comunicación extremo a extremo seguro entre los dispositivos respectivos para impedir interceptación no autorizada y la revelación de los datos transmitidos en el canal de comunicación, también es deseable permitir la interceptación e interpretación de datos transmitidos en el canal de comunicación seguro en circunstancias especiales. Tal "interceptación legal" puede ser deseable en el nombre de las autoridades del gobierno para detectar actividades ilegales.

La WO 03/049357 describe un planteamiento de permitir interceptación legal usando un "valor inicial" aleatorio (es decir un valor aleatorio), que se genera por un nodo de red y usa por los terminales finales para calcular claves de cifrado. También, el Manual de Criptografía Aplicada de Menezes, Oorschot y Vanstone, publicado por CRC Press Series sobre Matemáticas Discretas y sus Aplicaciones, 1997, XP002409097, ISBN: 0-8493-8523-7 proporciona antecedentes sobre técnicas de gestión de claves conocidas.

Compendio de la invención

La invención se define en las reivindicaciones adjuntas.

Para una mejor comprensión de la presente invención, se describirán ahora realizaciones con referencia a los dibujos anexos, en los que:

La Figura 1 muestra esquemáticamente los elementos de comunicación proporcionados para permitir a los terminales respectivos comunicar entre sí;

La Figura 2 muestra esquemáticamente la comunicación entre los terminales respectivos en el plano de medios y en el plano de control;

La Figura 3 muestra el mecanismo por el cual se acuerda una clave entre un terminal móvil y una función de aplicaciones de red usando la arquitectura de autenticación genérica del 3GPP; y

La Figura 4 muestra el mecanismo para proporcionar comunicaciones del plano de medios protegidas entre los terminales respectivos e intercambio de claves entre esos terminales usando seguridad del plano de control.

En los dibujos elementos iguales se designan de manera general con el mismo signo de referencia.

La Figura 1 muestra esquemáticamente una red de comunicación. El terminal 1A se registra con el núcleo de red IMS 3A. El terminal 1A puede ser un teléfono celular o móvil de mano, un asistente digital personal (PDA) o un ordenador portátil equipado con una tarjeta de datos o módulos 3G incorporados y una SIM. El terminal 1A comunica inalámbricamente con el núcleo de red 3A a través de una red de acceso radio (RAN) 5A, que comprende, en el caso de una red UMTS, una estación base (Nodo B) y un controlador de red radio (RNC). Las comunicaciones entre el terminal 1A y la red 3A se encaminan desde la red de acceso radio 5A a través del nodo de soporte GPRS de servicio (SGSN) 7A y el nodo de soporte GPRS pasarela (GGSN) 9A, que se puede conectar por un fijo (enlace por cable) al núcleo de red 3A. El GGSN 9A permite comunicaciones basadas en IP con la red central 3A.

De la manera convencional, se pueden registrar una multiplicidad de otros terminales con el núcleo de red 3A. Estos otros terminales pueden comunicar con el núcleo de red 3A de una manera similar al terminal 1A, es decir a través de la red de acceso radio 5A, SGSN 7A y GGSN 9A. Alternativamente, los otros terminales pueden comunicar a través de una red de acceso diferente, tal como Internet de banda ancha o WLAN.

De manera similar, el terminal 1B se registra con el núcleo de red IMS 3B y comunica con el mismo a través de la RAN 5B, el SGSN 7B y el GGSN 9B.

Los núcleos de red respectivos 3A, 3B se conectan por el enlace de comunicación 11.

Cada uno de los terminales móviles 1A, 1B se dota con un módulo de identidad de abonado (SIM) 15 respectivo. Durante el proceso de fabricación de cada SIM, se almacena información de autenticación sobre el mismo bajo el control del núcleo de red 3A, 3B relevante. El núcleo de red 3A, 3B almacena en sí mismo detalles de cada uno de los SIM bajo su control en su Servidor de Abonado Local (HSS) 17A, 17B.

En la operación del núcleo de red 3A, el terminal 1A se autentica (por ejemplo, cuando el usuario activa el terminal en la RAN 5A con una vista para hacer o recibir llamadas) por el núcleo de red 3A enviando un desafío al terminal 1A que incorpora el SIM 15, en respuesta a lo cual el SIM 15 calcula una respuesta (dependiente de la información predeterminada mantenida en el SIM – típicamente un algoritmo de autenticación y una clave única Ki) y la transmite de vuelta al núcleo de red 3A. El HSS 17A incluye un procesador de autenticación que genera el desafío y que recibe la respuesta desde el terminal 1A. Usando la información almacenada previamente que concierne al contenido del SIM 15 relevante, el procesador de autenticación calculó el valor esperado de la respuesta desde el terminal móvil 1A. Si la respuesta recibida coincide con la respuesta calculada esperada, el SIM 15 y el terminal

asociado 1A se consideran que se autentican. La autenticación entre el terminal móvil 1B y el núcleo de red 3B ocurre de una manera similar.

Descrita hasta aquí está la conexión del plano de medios entre el terminal 1A y el núcleo de red 3A. Como se mencionó anteriormente, la plano de control maneja la señalización de sesión y se pretende que sea independiente del acceso – es decir la señalización de sesión del núcleo de red es la misma, con independencia de si se accede al núcleo de red a través de una red de telecomunicaciones móvil o celular (que comprende la RAN 5A, SGSN 7A y 9A) o accede a través de una conexión de banda ancha fija o conexión WLAN.

En el plano de control, el terminal 1A comunica, a través de la RAN 5A, SGSN 7A y GGSN 9A, inicialmente con la CSCF intermediaria (P-CSCF) 19A. La P-CSCF 19A asegura que el registro SIP se pasa al núcleo de red doméstica y que los mensajes de sesión SIP se pasan a la CSCF de servicio (S-CSCF) 21A correcta una vez que ha ocurrido el registro del terminal con su núcleo de red doméstica (3A en esta realización). El usuario se asigna a una P-CSCF 19A como parte del registro y proporciona una asociación IPsec de dos vías con el dispositivo 1A. Todo el tráfico de señalización atraviesa la P-CSCF 19A durante la duración de una sesión de comunicación.

La S-CSCF 21A interactúa con el HSS 17A para determinar la elegibilidad del servicio por el usuario desde el perfil de usuario. La S-CSCF 21A se asigna durante la duración del registro.

La S-CSCF 21A está siempre en el núcleo de red doméstica 1A del terminal. La P-CSCF 19A puede estar en la red doméstica o en un núcleo de red visitada.

La señalización del plano de control y la señalización del plano de medios siguen diferentes caminos, como se indicó anteriormente y como se muestra esquemáticamente en la Figura 2. Como se mencionó anteriormente, la arquitectura de seguridad IMS actual en la TS 33.203 protege solamente el plano de control IMS. Se supone que el plano de medios es seguro. Mientras que el plano de medios puede ser adecuadamente seguro en una red de acceso GERAN o UTRAN, esto puede no ser así para una red de acceso WLAN u otros tipos de red de acceso.

Brevemente, la seguridad del plano de control se proporciona por la S-CSCF 21A que ejecuta una autenticación basada en SIM y un acuerdo de claves con el cliente IMS presente en el terminal móvil 1A. Una clave de sesión se pasa a la P-CSCF 19A y usa para señalización de protección de integridad y confidencialidad entre el terminal 1A y la P-CSCF 19A usando IPsec. Opcionalmente, se puede usar IPsec con encapsulación UDP para acceso IMS sobre acceso no celular donde puede estar presente un traductor de direcciones de red (NAT).

El 3GPP especifica el uso de IPsec y especifica una infraestructura de clave pública (PKI) basada en solución de gestión de claves para establecer IPsec entre núcleos IMS. También es posible el uso de seguridad de capa de transporte (TLS).

Protocolos de seguridad para protección del plano de medios:

- Medios RTP de Protocolo de Transporte en Tiempo Real, por ejemplo:

  - SRTP (RFC3711)

- Medios no RTP, por ejemplo:

  - TLS/DTLS

  - IPsec

  - S/MIME

  - …

Gestión de claves:

- Inicio de diálogo en canal de señalización, por ejemplo:

  - MIKEY (RFC3830, draft-ietf-mmusic-kmgmt-ext)

  - Descripciones de Seguridad SDP (draft-ietf-mmusic-sdescriptions, etc.)

- Inicio de diálogo en canal de medios, por ejemplo:

  - ZRTP (draft-zimmermann-avt-zrtp)

  - EKT (draft-mcgrew-srtp-ekt)

  - RTP/DTLS (draft-tschofening-avt-rtp-dtls, etc.)

Se han propuesto diferentes protocolos de seguridad y esquemas de gestión de claves para proteger la comunicación de datos en el plano de medios. No obstante, como se trató anteriormente, puede ser deseable o un requisito para núcleos de red IMS facilitar una interceptación e interpretación legales de tales datos cifrados.

Por ejemplo, si un operador de núcleo de red IMS está asistiendo activamente en ayudar a los usuarios a cifrar medios IMS, entonces se podría requerir a ese operador proporcionar información para quitar ese cifrado para propósitos de interceptación e interpretación legales. El operador de red IMS doméstico para un usuario debe ser capaz de proporcionar información para quitar el cifrado proporcionado. Posiblemente cualquier operador de red IMS visitada también pudiera tener que proporcionar información para quitar el cifrado.

Los medios se pueden encaminar a través de una red que no opera la P-CSCF 19A y S-CSCF 21A implicadas. No obstante, se supone que no habrá requisitos sobre esa red que sean capaces de proporcionar información para quitar el cifrado.

También es ventajoso que los usuarios no sean capaces de determinar si sus comunicaciones están sometidas o no a interceptación e interpretación legales en cualquier momento particular. Se debería hacer difícil para un usuario hacer uso de capacidades de seguridad de medios proporcionadas por el operador mientras que al mismo tiempo elude la interceptación e interpretación legales de los medios.

La Figura 3 muestra esquemáticamente el procedimiento conocido de Arquitectura de Autenticación Genérica (GAA) del 3GPP para acordar una clave para uso entre el terminal 1A y una Función de Aplicaciones de Red (NAF) 30. La NAF 30 representa un servidor de aplicaciones genérico que proporciona cualquier tipo de servicio (aplicación) al terminal 1A.

El operador del núcleo de red IMS 3A, como se mencionó anteriormente, es capaz de autenticar los terminales móviles con el uso de información de autenticación almacenada en la SIM 15 del terminal. La GAA reutiliza esta información de autenticación para proporcionar un mecanismo independiente de la aplicación para dotar al terminal móvil 1A (cliente) y al servidor de aplicaciones (NAF 30) con un secreto (clave) compartido común en base a protocolos de Autenticación y Acuerdo de Claves (AKA) del 3GPP.

Una Función de servidor de Secuencia de Inicialización (BSF) 32 genérica se proporciona en el núcleo de red IMS 3A. Cuando el terminal 1A interactúa con la NAF 30 la primera vez, se realiza una autenticación de secuencia de inicialización. El terminal móvil 1A envía una petición adecuada a la BSF 32. La BSF 32 recupera datos de autenticación para el SIM 15 asociado con el terminal 1A (vectores AKA) desde el HSS 17A. El terminal 1A y la BSF 32 entonces acuerdan sobre las claves de sesión. Las claves de sesión se pasan desde la BSF 32 a la NAF 30 y se usan posteriormente para proteger la comunicación entre el terminal móvil 1A y la NAF.

El secreto (clave) compartido se obtiene por un procedimiento conocido, que se trata ahora brevemente en más detalle.

Cuando el terminal 1A interactúa con la NAF 30 la primera vez, realiza la autenticación de secuencia de inicialización. El terminal 1A envía una petición a la BSF 32. La BSF 32 recupera un conjunto completo de ajustes de seguridad de usuario de la Arquitectura de Secuencia de Inicialización Genérica (GBA) y un vector de autenticación (RAND, AUTN, XRES, IK, CK) desde el HSS 17A. Entonces la BSF 32 reenvía el RAND y AUTN al terminal 1A. El terminal 1A envía el RAND y AUTN al SIM 15 que calcula IK, CK, MAC y RES y comprueba la MAC para verificar que los parámetros vienen desde una red autorizada. Después el SIM 15 genera la clave Ks concatenando la IK y CK. El valor RES se envía a la BSF 32 donde autentica el terminal 1A. La BSF 32 calcula la clave Ks también y genera el B-TID que se envía al terminal 1A para indicar el éxito de la autenticación. Adicionalmente la BSF 32 suministra el tiempo de vida (periodo de validez) de la Ks. El terminal 1A (o SIM 15) y la BSF 32 almacenan la clave Ks con el B-TID asociado para uso adicional, hasta que el tiempo de vida de la Ks ha expirado o hasta que se actualiza la clave Ks. En caso de la expiración de la Ks o una actualización de claves requerida de la NAF 30 (petición de renegociación de secuencia de inicialización), el procedimiento de secuencia de inicialización tiene que ser iniciado de nuevo.

Después de la terminación del Modo de Secuencias de Inicialización, las claves específicas de la NAF 30 se calcularán en un procedimiento llamado Modo de Derivación de Claves. Son posibles dos variantes GBA_ME y GBA_U. A continuación describimos la variante GBA_ME.

Tanto el terminal 1A como la BSF 32 usan la Ks para derivar la clave material Ks_NAF. La función de derivación de claves de estas claves es KDF=[Ks, “gba-me”, RAND, IMPI, NAF_ID]. La BSF 32 envía la Ks_NAF a la NAF 30 la cual entonces puede configurar una comunicación segura con el terminal 1A en base a estas claves compartidas. El terminal 1A almacena la Ks_NAF con los B_TID y NAF_ID correspondientes en su memoria para sesiones adicionales.

Después de que se ha completado la secuencia de inicialización, el terminal 1A y una NAF 30 pueden ejecutar un protocolo específico de aplicación donde la autenticación de mensajes se basará en esas claves de sesión generadas durante la autenticación mutua entre el terminal 1A y la BSF 32.

Cuando un terminal 1A inicia una sesión adicional con la NAF 30, se reutilizarán las claves almacenadas. El terminal 1A suministra el B-TID a la NAF 30. Por medio del B-TID, la NAF 30 recupera la identidad del usuario y la Ks_NAF correspondiente desde la BSF. Finalmente el terminal 1A y la BSF 30 pueden autenticar uno al otro usando la Ks_NAF compartida.

La Codificación de Internet Multimedia (MIKEY) se describirá ahora. MIKEY es un esquema de gestión de claves que se puede usar para aplicaciones en tiempo real.

En MIKEY diferentes claves de cifrado de tráfico (TEK) para cada sesión en la llamada se derivan de una clave de generación de TEK común (TGK), por ejemplo la TEK1 para secuencia de vídeo, la TEK2 para secuencia de audio, etc. El protocolo MIKEY tiene un máximo de dos pases – y se puede integrar en oferta/respuesta SDP sin idas y vueltas extra. MIKEY se puede transportar en SDP y RTSP según el draft-ietf-mmusic-kmgmt-ext. MIKEY ofrece tres métodos de gestión de claves:

- Clave precompartida

  - El iniciador genera la TGK la cual se protege usando una clave precompartida

- Cifrado RSA

  - El iniciador genera la TGK la cual se protege usando una clave pública del receptor

  - El iniciador debe traer un certificado del respondedor por adelantado

- Diffie Hellman

  - Tanto el iniciador como el respondedor contribuyen a la TGK

  - Los certificados del iniciador y del respondedor se pueden transportar en mensajes MIKEY

  - Proporciona confidencialidad directa perfecta

MIKEY solamente soporta SRTP pero se puede extender para soportar otros protocolos de seguridad

Se puede obtener más información acerca de MIKEY en el documento RFC 3830 del IETF, que se incorpora completamente en la presente memoria por referencia.

Se describirá ahora el establecimiento de canales de comunicación extremo a extremo seguros en el plano de medios.

Clave extremo a extremo protegida usando seguridad del plano de control IMS.

Con referencia a la Figura 2, se describirá ahora el procedimiento cuando se establece un canal de comunicación IMS entre el terminal 1A y el terminal 1B. El terminal 1A pertenece a (es decir se registra con y/o es un abonado de) el núcleo de red 3A y se registra sobre la S-CSCF 21A a través de la P-CSCF 19A. De manera similar, el terminal 1B pertenece a (es decir se registra con y/o es un abonado de) el núcleo de red 3B y se registra sobre la S-CSCF 21B a través de la P-CSCF 19B. Para los propósitos de seguridad del plano de medios, cada red tiene un centro de gestión de claves (KMC) 40A, 40B, respectivo que se podrían considerar como servidores de aplicaciones SIP.

Durante el establecimiento de un canal de comunicación, la S-CSCF 21A y la S-CSCF 21B interceptan el flujo de señalización y solicitan el KMC 40A y KMC 40B respectivamente para ayudar a establecer un canal o canales de medios de protección extremo a extremo. Se podrían integrar mensajes de petición de establecimiento de asociación de seguridad con la señalización de establecimiento de llamada, es decir una gestión SIP INVITE. Después del establecimiento de llamada, el canal de medios extremo a extremo se podría proteger usando una asociación de seguridad acordada.

Por ejemplo, la asociación de seguridad se podría proporcionar por el siguiente mecanismo de gestión de claves.

1. Para cada llamada de medios, el KMC 40A genera un componente de clave K1. K1 se transmite al terminal 1A sobre el canal del plano de control IMS protegido entre el terminal 1A y la P-CSCF 19A. El KMC 40B también genera un componente de clave similar K2, que se transmite al terminal 1B sobre el canal protegido entre el terminal 1B y la P-CSCF 19B.

2. El terminal 1A y el terminal 1B intercambian los componentes de claves K1 y K2 sobre el canal del plano de control IMS protegido.

Las claves K1 y K2 se pueden usar de varias formas:

(A) El terminal móvil 1A transmite datos en el plano de medios usando la clave K1. El terminal 1B es capaz de descifrar este mensaje debido a que la clave K1 se ha transmitido a él sobre el canal del plano de control IMS. De

manera similar, el terminal 1B cifra sus comunicaciones en el plano de medios al terminal 1A usando su clave K2. El terminal 1A es capaz de descifrar estas comunicaciones debido a que la clave K2 se ha proporcionado al terminal 1A sobre el canal del plano de control IMS.

(B) El terminal 1A y el terminal 1B ambos generan una clave compartida, K12 (K12 = KDF (K1, K2), donde KDF es una función de derivación de claves, por ejemplo K12 = K1 XOR K2), que se usa para proteger el canal extremo a extremo en el plano de medios.

(C) Alternativamente además, el KMC 40A y el KMC 40B intercambian K1 y K2, generan la clave compartida K12 y luego distribuyen la clave compartida K12 a los terminales 1A y 1B respectivos sobre el canal del plano de control IMS protegido.

(D) En otra alternativa, el terminal 1A y el terminal 1B usan el KMC 40A y el KMC 40B para intercambiar las claves del plano de control IMS existentes y para generar la clave de extremo a extremo combinándolas de alguna forma. Por ejemplo, la clave compartida K12 = KDF (CKA, IKA, CKB, IKB), donde KDF es una función de derivación de claves. Tal mecanismo es similar al mecanismo que fue propuesto originalmente, pero nunca estandarizado, para protección de la publicación 99 del UMTS de una forma extremo a extremo a nivel de portador, como se describe en el documento S3-010089 del 3GPP, que se incorpora aquí completamente por referencia.

Ventajosamente, la P-CSCF 19A, S-CSCF 21A, KMC 40A, P-CSCF 19B, S-CSCF 21B y KMC 40B pueden obtener las claves K1, K2 y K12 y estas se puede usar en interceptación e interpretación legales de los mensajes transmitidos entre los terminales 1A y 1B en el plano de medios.

Una desventaja de algunas de las disposiciones (A) a (D) tratadas anteriormente es que las claves K1, K2 y K12 se podrían interceptar por partes no autorizadas en alguna parte no protegida del plano de control IMS. Las claves obtenidas de esta manera se podrían usar entonces para descifrar los datos transmitidos en el plano de medios.

Clave extremo a extremo protegida usando seguridad por salto dedicada

La disposición descrita anteriormente en relación con la Figura 2 se modifica de manera que se establece una clave E_{KA} como se muestra en la Figura 4 en 48A entre el terminal 1A y el KMC 40A. La clave E_{KA} se establece usando la GAA como se describe con referencia a la Figura 3 (el KMC 40A que actúa como la NAF 30). De manera similar, un terminal móvil 1B establece en 48B una clave E_{KB} con su KMC 40B que usa GAA (el KMC 40B que actúa como una segunda NAF 30). El KMC 40A y el KMC 40B establecen una clave E_{KAB} 50 entre ellos usando, por ejemplo, seguridad de dominio de red/estructura de autenticación (NDS/AF) del 3GPP, como se define en la Especificación TR 33.810.

El terminal 1A entonces genera una clave extremo a extremo K1 para uso en asegurar las comunicaciones entre sí mismo y el terminal 1B. La clave K1 se cifra usando la clave E_{KA} para formar E_{KA} (K1) 52A, que entonces se transmite al núcleo IMS 3A y desde allí al KMC 40A. El KMC 40A entonces extrae la clave K1 usando la clave E_{KA} y cifra la clave K1 con la clave establecida entre el KMC 40A y el KMC 40B, para crear el paquete E_{KAB} (K1) 54. Este paquete se envía al núcleo de red 3A y desde allí al KMC 40A y desde allí al núcleo IMS 3B y desde allí al KMC 40B donde se descifra usando la clave E_{KAB}. La clave K1 se cifra entonces usando la clave E_{KB} establecida entre el KMC 40B y el terminal 1B y se transmite al núcleo IMS 3B y desde allí al terminal 1B en el paquete E_{KB} (K1) 56A. El terminal 1B usa su conocimiento de la E_{KB} para extraer K1 y almacenarla para uso futuro.

El terminal 1B establece una clave K2 para cifrar comunicaciones que desea enviar al terminal 1A. Esta clave K2 se transmite al núcleo de red 3B y desde allí al KMC 40B y desde allí al núcleo de red 3B y desde allí al núcleo de red 3A y desde allí al KMC 40A y desde allí al núcleo de red 3A y desde allí al terminal móvil 1A. En cada salto entre estos elementos, la clave K2 se cifra usando las claves relevantes establecidas usando GAA (E_{KB}, E_{KA}) y E_{KAB}, como se muestra en la Figura, para formar los paquetes E_{KB} (K2) 52B, E_{KAB} (K2) 54 y E_{KA} (K2) 56B. El terminal 1A usa su conocimiento de E_{KA} para extraer K2 y almacenarla para uso futuro.

Los datos transmitidos desde el terminal 1A al terminal 1B en el plano de medios entonces se pueden cifrar usando la clave K1. El terminal 1B es capaz de descifrar estos datos debido a que ha sido dotado con K1 en el proceso descrito anteriormente. De manera similar, los datos transmitidos en el plano de medios desde el terminal 1B al terminal 1A se cifran usando la clave K2 y estos datos se pueden descifrar por el terminal 1A debido a que la clave K2 se ha transmitido sobre el plano de control de la manera descrita anteriormente.

En esta disposición las claves K1 y K2, cuando se transmiten en el plano de control IMS se transmiten en forma cifrada (por las claves E_{KA}, E_{KB} y E_{KAB}). No obstante, ventajosamente, el KMC 40A y el KMC 40B pueden derivar las claves K1 y K2 a partir de su conocimiento de E_{KA} y E_{KB}, respectivamente y este se puede usar en la interceptación e interpretación legales de los mensajes transmitidos entre los terminales 1A y 1B en el plano de medios.

Una desventaja de esta adaptación es que se requieren numerosos pasos de cifrado y descifrado para transmitir las claves K1 y K2 entre los terminales 1A y 1B en el plano de control.

MIKEY basada en certificado con clave extremo a extremo revelada al núcleo de red

De la manera descrita anteriormente en relación con la Figura 4 se establece una clave compartida E_{KA} entre el terminal 1A y el KMC 40A usando GAA y de manera similar se establece una clave compartida E_{KB} entre el terminal 1B y el KMC 40B. Cada terminal también tiene un par de claves y adquiere un certificado por ejemplo desde su KMC 40A, 40B respectivo.

Los certificados se usan para establecer claves extremo a extremo para seguridad del plano de medios usando cifrado RSA de MIKEY o por el método Diffie-Hellman de una manera conocida.

Según un rasgo importante de esta realización, se añaden Campos de Recuperación de Claves (KRF) a los intercambios del plano de control para permitir que sean puestas a disposición claves extremo a extremo para los núcleos IMS 3A, 3B con el propósito de interceptación e interpretación legales.

Cifrado RSA de MIKEY

De la manera convencional, los terminales móviles 1A y 1B cada uno se dota con un par de claves pública privada respectivas. La clave pública del terminal 1A y la clave pública para el terminal 1B se ponen a disposición libremente, de manera que el terminal móvil 1A tiene conocimiento de la clave pública del terminal 1B y el terminal móvil 1B tiene conocimiento de la clave pública del terminal 1A. La clave privada del terminal móvil 1A es conocida solamente por el terminal 1A y la clave privada del terminal 1B es conocida por el terminal 1B.

Los certificados certifican la autenticidad de la clave pública del terminal 1A y el terminal 1B. Los certificados se adquieren del KMC 40A y 40B, respectivamente, usando GAA. Como se describió anteriormente, la GAA genera una clave compartida E_{KA} entre el terminal 1A y su KMC 40A. De manera similar, la GAA genera una clave compartida E_{KB} entre el terminal 1B y el KMC 40B.

Como se mencionó anteriormente, el método de cifrado MIKEY se describe en el documento RFC 3830.

En la realización, el terminal 1A, que actúa como el “iniciador”, genera un mensaje de inicio MIKEY, como sigue:

I_MESSAGE = HDR, T, RAND,

[IDi]CERTi], [IDr], {SP}, KEMAC,

[CHASH], PKE, SIGNi, KRFi

El último campo de este mensaje, KRFi, es un campo de recuperación de claves.

El mensaje de inicio MIKEY incluye los siguientes elementos convencionales:

Carga Útil de Cabecera Común (HDR)

T es la marca de tiempo de 64 bit enviada por el Iniciador

Carga Útil de RAND (RAND)

Carga Útil de ID de Iniciador (IDi)

Carga Útil de Certificado de Iniciador (CERTi)

Carga Útil de ID de Respondedor (IDr)

Carga Útil de Política de Seguridad (SP)

Carga Útil de Transporte de Datos de Claves (KEMAC)

Carga Útil de Generación de Claves Cert de clave de firma de Iniciador (CHASH)

Carga Útil de Datos de Envoltura (PKE)

La SIGNi es una firma que cubre el mensaje MIKEY entero, usando la clave de firma del Iniciador.

El objetivo principal del mensaje del Iniciador es transportar una o más TGK y un conjunto de parámetros de seguridad al Respondedor de una manera segura. Esto se hace usando un planteamiento de envoltura donde las TGK se cifran (y protege la integridad) con claves derivadas de una “clave de envoltura” elegida aleatoriamente/seudoaleatoriamente. La clave de envoltura se envía al Respondedor cifrada con la clave pública del Respondedor.

La PKE contiene la clave de envoltura cifrada: PKE = E(PKr, env_key). Se cifra usando la clave pública del Respondedor (PKr). Si el Respondedor posee varias claves públicas, el Iniciador puede indicar la clave usada en la carga útil CHASH.

La KEMAC contiene un conjunto de subcargas útiles cifradas y una MAC:

KEMAC = E(encr_key, IDi || {TGK}) || MAC

(enc_key es una clave de cifrado de la clave de envoltura derivada de la clave de envoltura).

La primera carga útil (IDi) en la KEMAC es la identidad del Iniciador (no un certificado, sino generalmente el mismo ID que el especificado en el certificado). Cada una de las siguientes cargas útiles (TGK) incluye una TGK elegida aleatoria e independientemente por el Iniciador (y otros posibles parámetros relacionados, por ejemplo, el tiempo de vida de la clave). La parte cifrada entonces es seguida por una MAC, la cual se calcula sobre la carga útil KEMAC, usando una clave de autenticación auth_key.

El campo de recuperación de claves KRFi añadido al mensaje del iniciador comprende la TGK (o clave de envoltura) protegida usando la clave compartida del Iniciador E_{KA} obtenida usando GAA.

El mensaje de verificación del respondedor convencional se modifica ligeramente y se explica más adelante:

R_MESSAGE =

HDR, T, [IDr], V, KRFr

El objetivo principal del mensaje de verificación del Respondedor es obtener autenticación mutua. El mensaje de verificación, V, es una MAC calculada sobre el mensaje entero del Respondedor, la marca de tiempo (la misma que la que fue incluida en el mensaje del Iniciador) y las dos identidades de las partes, usando la clave de autenticación, auth_key.

El campo final, KRFr es un campo de recuperación de claves y comprende la TGK (o clave de envoltura) protegida bajo la clave compartida del respondedor E_{KB} generada usando GAA.

Debido a que las claves compartidas E_{KA} y E_{KB} se conocen por el KMC 40A y el KMC 40B, respectivamente, el KMC relevante puede descifrar los campos de recuperación de claves KRFi/KRFr para obtener la TGK (o clave de envoltura) y permitir por ello la interceptación e interpretación ilegales de los datos transmitidos en el plano de medios. La TGK (o clave de envoltura) se puede usar para recuperar las TEK. Las TEK entonces se pueden usar para descifrar el tráfico del plano de medios.

Los usuarios de los terminales 1A y 1B no son conscientes de que el tráfico del plano de medios está sometido a interceptación e interpretación legales.

El terminal 1A (el Iniciador) necesita recuperar el certificado del terminal 1B (el respondedor) antes de que se permita el establecimiento de llamada.

Método Diffie Hellman

Como se conocerá por los expertos en la técnica, en el método de cifrado Diffie Hellman (DH), el terminal 1A y el terminal 1B cada uno tiene un valor privado DH respectivo a, b. En la forma convencional el terminal 1A transmite un valor público DH al terminal 1B transmitiendo el valor g^a. De manera similar, el terminal 1B transmite un valor público DH al terminal 1A transmitiendo el valor g^b. El terminal 1A entonces genera una clave privada elevando el valor recibido g^b a la potencia a – es decir calculando $(g^b)^a$. De manera similar, el terminal 1B genera una clave privada elevando el valor recibido g^a a la potencia b, es decir calcula el valor $(g^a)^b$. Debido a que el valor $(g^a)^b$ es el mismo que el valor $(g^b)^a$, ambos terminales 1A y 1B ahora tienen una clave DH privada o secreta compartida. La clave DH se usa como la TGK.

Una fortaleza del método de cifrado de Diffie Hellman es que, si o bien el valor (g^a) o bien el valor (g^b) o ambos se interceptan cuando se transmiten por los terminales, esto no permitirá la derivación de la clave secreta compartida o privada.

Para el método de Diffie Hellman, el campo de recuperación de claves se debe generar de una forma diferente.

Por consiguiente, el mensaje iniciador de MIKEY estándar para Diffie Hellman se modifica como sigue:

I_MESSAGE = HDR, T, RAND,

[IDi]CERTi], [IDr], {SP}, DHi,

SIGNi, KRFi

Los mensajes del Respondedor se modifican como sigue:

R_MESSAGE =

HDR, T, [IDr]CERTr], IDi,

DHr, DHi, SIGNr, KRFr

De la manera convencional, el campo DHi en el mensaje del iniciador y en el mensaje del respondedor contiene el valor público DH del iniciador. El campo DHr en el mensaje del respondedor contiene el valor público DH del respondedor. Esto permite a cada terminal 1A y 1B derivar la clave DH privada o secreta; esto se usa como la TGK.

Según esta realización, el campo de recuperación de claves, KRFi, se añade al mensaje del iniciador. El campo KRFi contiene la clave privada DH del iniciador a cifrada usando la clave compartida E_{KA} generada usando GAA.

De manera similar, el campo final KRFr del mensaje del respondedor incluye la clave privada DH del respondedor b cifrada usando la clave E_{KB} generada usando GAA.

Tal disposición permite al núcleo de red del iniciador 3A obtener una clave privada DH del iniciador a descifrando el campo de recuperación de claves, KRFi y permite al núcleo de red del respondedor 3B obtener la clave privada DH del respondedor (o la TGK) descifrando el campo de recuperación de claves, KRFr. El núcleo de red del iniciador 3A entonces puede combinar la clave privada DH a con el valor público DH del respondedor g^b para derivar la TGK la cual a su vez se puede usar para recuperar las TEK y permitir una interceptación e interpretación legales del tráfico del plano de medios.

Como alternativa a lo anterior los campos de recuperación de claves se pueden generar cifrando la TGK o las TEK, en lugar de la clave privada DH, con E_{KA} para KRFi y E_{KB} para KRFr.

En esta realización también, los usuarios de los terminales 1A y 1B no son conscientes de si están sometidos o no a interceptación e interpretación legales de su tráfico del plano de medios.

Algunas posibles variantes para soportar clientes corporativos (u otros grupos de usuarios cerrados) se tratan brevemente más adelante:

- Un usuario podría usar un portal PKI corporativo o KMC corporativo en lugar del proporcionado por el operador de red

- La comunicación con el portal PKI o KMC se asegura usando GAA

  - Seguridad proporcionada por el operador – USIM/ISIM de operador se usa para GAA

  - Seguridad proporcionada por la corporación – un ISIM corporativo en una UICC se usa para GAA

- Un ISIM “oculto” instalado en cada nueva UICC, pero solamente el suministrador de la UICC conoce la única clave del ISIM

- El operador “habilita” el ISIM a petición del cliente usando métodos OTA

- El operador proporciona infraestructura de GAA a la corporación de manera que puedan emitir claves y certificados para seguridad de medios IMS a sus empleados.

- El suministrador de la UICC entrega claves únicas ISIM directamente a la corporación para cargar en la infraestructura de GAA

  - Las claves ISIM no se revelan al operador IMS

- La interceptación legal se podría soportar si se necesitan monitorizar comunicaciones de empleado o cumplir con la legislación

- La infraestructura de GAA también se podría usar para emitir otros tipos de certificados, por ejemplo para acceso VPN corporativo.

REIVINDICACIONES

1. Un método de establecimiento de un canal de comunicación extremo a extremo seguro para enviar mensajes seguros entre un primer dispositivo (1A) y un segundo dispositivo (1B), cada dispositivo que está asociado con un núcleo de red de comunicación (3A, 3B) y en donde al menos uno de los dispositivos incluye datos de seguridad para generar tales mensajes seguros, el método que incluye:

establecer una conexión del plano de control entre el primer dispositivo (1A) y el núcleo de red de comunicación (3A), la conexión del plano de control que está protegida por una arquitectura de seguridad preestablecida;

intercambiar de manera segura información de claves entre el primer dispositivo (1A) y el núcleo de red de comunicación (3A) usando la conexión del plano de control y su arquitectura de seguridad correspondiente,

por lo cual dicha información de claves es utilizable para permitir al núcleo de red de comunicación (3A, 3B) obtener los datos de seguridad y por consiguiente interpretar los mensajes seguros interceptados enviados entre los dispositivos primero y segundo (1A, 1B).

2. El método según la reivindicación 1, en donde los mensajes se envían en un plano de medios.

3. El método según la reivindicación 1 o 2, en donde el paso de intercambiar de manera segura información de claves entre el primer dispositivo (1A) y el núcleo de red de comunicación (3A) incluye establecer una primera clave E_{KA} entre el primer dispositivo (1A) y el primer centro de gestión de claves, KMC, (40A) del núcleo de red de comunicación (3A) y el método además incluye:

establecer un canal de comunicación extremo a extremo seguro entre el primer dispositivo (1A) y el segundo dispositivo (1B) generando, en el primer dispositivo (1A), una clave extremo a extremo K1 y cifrar la clave extremo a extremo K1 usando la primera clave E_{KA} para formar una clave extremo a extremo cifrada $E_{KA}(K1)$;

transmitir la clave extremo a extremo cifrada $E_{KA}(K1)$ desde el primer dispositivo (1A) al primer KMC (40A);

transmitir la clave extremo a extremo K1 desde el primer KMC (40A) a un segundo KMC (40B) del núcleo de red de comunicación (3B);

establecer una segunda clave E_{KB} entre el segundo dispositivo (1B) y el segundo KMC (40B) usando una conexión del plano de control y su arquitectura de seguridad correspondiente, de manera que la segunda clave E_{KB} es utilizable para transmitir la clave extremo a extremo K1 desde el segundo KMC (40B) al segundo dispositivo (1B).

4. El método según la reivindicación 3, que además comprende:

en el segundo dispositivo (1B), generar una clave extremo a extremo K2 y cifrar la clave extremo a extremo K2 usando la segunda clave E_{KB} para formar una clave extremo a extremo cifrada $E_{KB}(K2)$;

transmitir la clave extremo a extremo cifrada $E_{KB}(K2)$ desde el segundo dispositivo (1B) al segundo KMC (40B);

transmitir la segunda clave K2 desde el segundo KMC (40B) al primer KMC (40A);

en el primer KMC (40A), cifrar la clave extremo a extremo K2 usando la primera clave E_{KA} para formar una clave extremo a extremo cifrada $E_{KA}(K2)$;

transmitir la clave extremo a extremo cifrada $E_{KA}(K2)$ desde el primer KMC (40A) al primer dispositivo (1A); y

en el primer dispositivo (1A), descifrar la clave extremo a extremo cifrada E_{KA} (K2) usando la primera clave E_{KA} para determinar la clave extremo a extremo K2.

5. El método de la reivindicación 4 en donde el canal de comunicación extremo a extremo seguro que se establece es un plano de medios IMS y el método además incluye:

en el primer dispositivo (1A), cifrar datos usando la clave extremo a extremo K1 y transmitir los datos cifrados al segundo dispositivo (1B) en el plano de medios IMS;

en el segundo dispositivo (1B), recibir los datos cifrados desde el primer dispositivo (1A) en el plano de medios IMS y usar la clave extremo a extremo K1 para descifrar los datos;

en el segundo dispositivo (1B), cifrar datos usando la clave extremo a extremo K2 y transmitir los datos cifrados al primer dispositivo (1A) en el plano de medios IMS; y

en el primer dispositivo (1A), recibir los datos cifrados desde el segundo dispositivo (1B) en el plano de medios IMS y usar la clave extremo a extremo K2 para descifrar los datos cifrados.

6. El método según cualquier reivindicación precedente, en donde la arquitectura de seguridad es como se define en la TS 33.203 del 3GPP.

7. El método según cualquier reivindicación precedente, en donde el núcleo de red de comunicación es el núcleo de red de un Subsistema Multimedia basado en IP, IMS y los mensajes seguros se envían entre el primer y segundo dispositivo a través de un plano de medios IMS.

8. El método según cualquier reivindicación precedente, en donde al menos uno de los dispositivos primero y segundo (1A, 1B) comprende un terminal móvil de comunicaciones celulares.

9. El método según una cualquiera de las reivindicaciones 3 a 5 en donde establecer la primera clave E_{KA} entre el primer dispositivo (1A) y el primer KMC (40A) comprende usar un procedimiento de arquitectura de autenticación genérica, GAA, en el que el primer KMC (40A) actúa como una función de aplicaciones de red, NAF.

10. El método según la reivindicación 4 o 5, en donde establecer la segunda clave E_{KB} entre el segundo dispositivo (1B) y el segundo KMC (40B) comprende usar un procedimiento de arquitectura de autenticación genérica, GAA, en el que el segundo KMC (40B) actúa como una función de aplicaciones de red.

11. El método según la reivindicación 9, en donde el procedimiento de GAA se usa para acordar la primera clave E_{KA} entre el primer dispositivo (1A) y el primer KMC (40A) e incluye realizar una autenticación entre el primer dispositivo (1A) y el núcleo de red de comunicación (3A) reutilizando información de autenticación usada previamente para autenticar el primer dispositivo (1A) durante un procedimiento de Autenticación y Acuerdo de Claves, AKA, de red.

12. El método según la reivindicación 11, en donde la información de autenticación usada en el procedimiento de GAA se refiere a información de autenticación almacenada en un Módulo de Identidad de Abonado, SIM, asociado con el primer dispositivo (1A).

13. El método según la reivindicación 10, en donde el procedimiento de GAA se usa para acordar la segunda clave E_{KB} entre el segundo dispositivo (1B) y el segundo KMC (40B) e incluye realizar una autenticación entre el segundo dispositivo (1B) y el núcleo de red de comunicación (3B) reutilizando una información de autenticación usada previamente para autenticar el segundo dispositivo (1B) durante un procedimiento de Autenticación y Acuerdo de Claves, AKA, de red.

14. El método según la reivindicación 13 en donde la información de autenticación usada en el procedimiento de GAA se refiere a información de autenticación almacenada en un Módulo de Identidad de Abonado, SIM, asociado con el segundo dispositivo (1B).

15. El método según cualquier reivindicación precedente, en donde el canal de comunicación extremo a extremo seguro se asegura usando el protocolo MIKEY y el método además incluye:

transmitir una comunicación de iniciación MIKEY entre los dispositivos primero y segundo (1A, 1B) que incluye un campo de recuperación de claves que contiene una clave para el cifrado MIKEY que se cifra usando la información de claves, de manera que el núcleo de red de comunicación (3A, 3B) puede descifrar el campo de recuperación de claves para obtener la clave de cifrado MIKEY a fin de permitir al núcleo de red de comunicación (3A, 3B) interpretar los mensajes interceptados asegurados usando cifrado MIKEY enviados entre los dispositivos primero y segundo (1A, 1B).

16. El método según cualquiera de las reivindicaciones 1 a 14 en donde el canal de comunicación extremo a extremo seguro se asegura usando un cifrado Diffie-Hellman y el método además incluye:

transmitir una comunicación de inicio Diffie-Hellman entre los dispositivos primero y segundo (1A, 1B) que incluye un campo de recuperación de claves que contiene una clave para el cifrado Diffie-Hellman que se cifra usando la información de claves, de manera que el núcleo de red de comunicación (3A, 3B) puede descifrar el campo de recuperación de claves para obtener la clave Diffie-Hellman a fin de permitir al núcleo de red de comunicación (3A, 3B) interpretar los mensajes interceptados asegurados usando cifrado Diffie-Hellman enviados entre los dispositivos primero y segundo (1A, 1B).

17. Un núcleo de red de comunicación (3A, 3B) para facilitar el establecimiento de una sesión de comunicación extremo a extremo segura para enviar mensajes seguros entre un primer dispositivo (1A) y un segundo dispositivo (1B), al menos uno de los dispositivos que está asociado con el núcleo de red y en donde al menos uno de los dispositivos (1A, 1B) incluye datos de seguridad para generar los mensajes seguros, el núcleo de red de comunicación (3A, 3B) que incluye:

medios configurados para establecer una conexión del plano de control con al menos uno del primer dispositivo (1A) y el segundo dispositivo (1B), la conexión del plano de control que está protegida por una arquitectura de seguridad preestablecida;

medios configurados para intercambiar de manera segura información de claves con al menos uno del primer dispositivo (1A) y el segundo dispositivo (1B) usando la conexión del plano de control y la arquitectura de seguridad correspondiente,

en donde la información de claves es utilizable por el núcleo de comunicación de red (3A, 3B) para interpretar mensajes seguros interceptados enviados entre los dispositivos primero y segundo (1A, 1B).

18. El núcleo de red de comunicación (3A) de la reivindicación 17, adaptado para realizar los métodos especificados en cualquiera de las reivindicaciones 1 a 14.

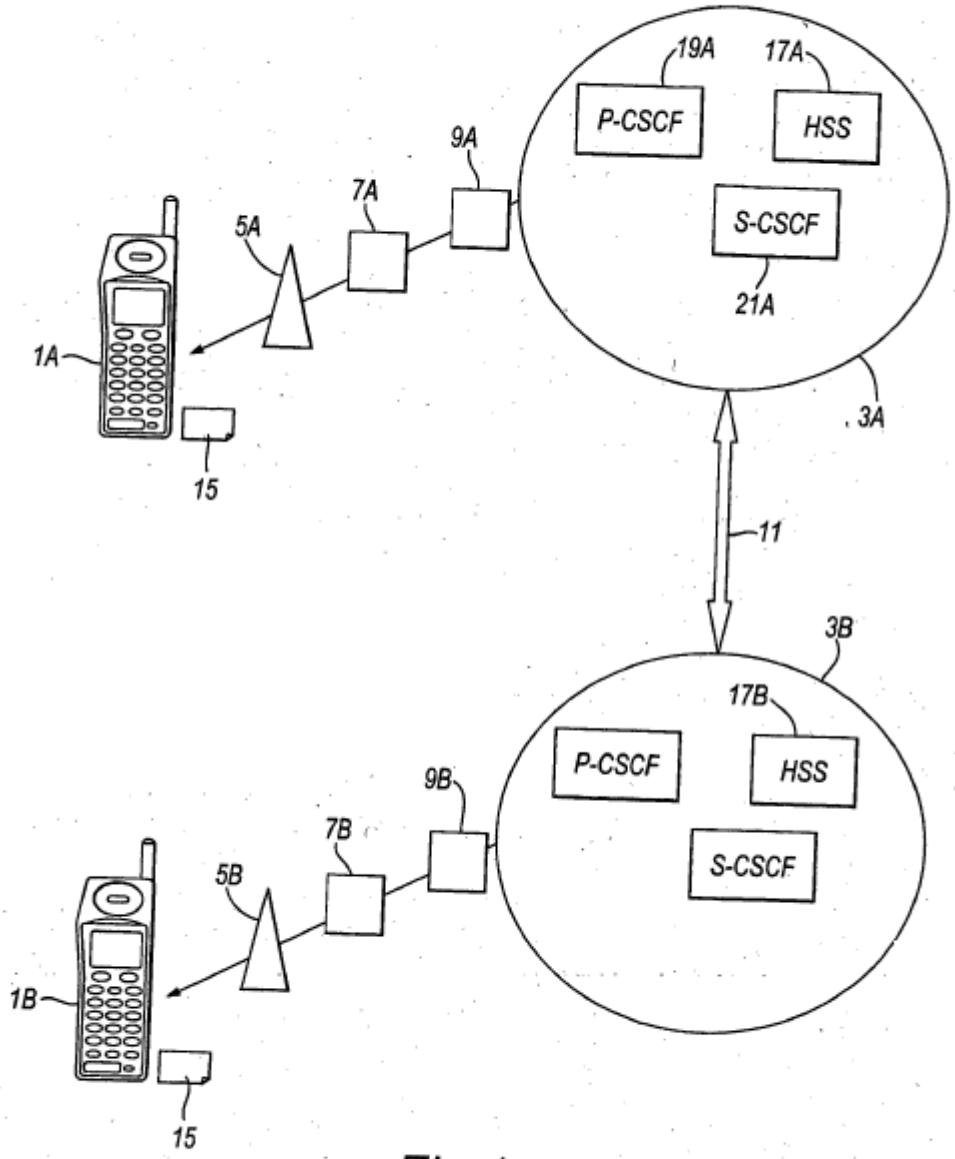
19A
17A
P-CSCF
HSS
9A
7A
5A
S-CSCF
21A
1A
3A
15
11
3B
17B
P-CSCF
HSS
9B
7B
S-CSCF
5B
1B
15

Fig.1

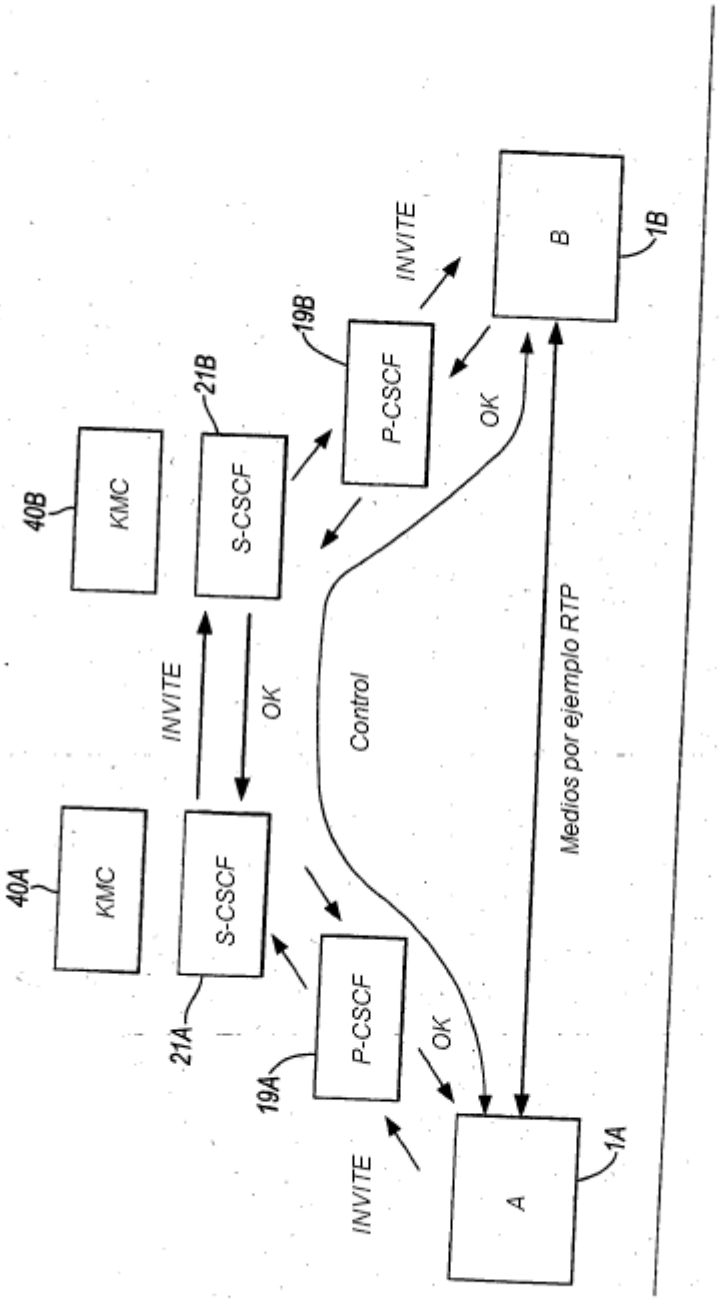
A
1A
B
1B
P-CSCF
19A
19B
S-CSCF
21A
21B
KMC
40A
40B
INVITE
OK
Control
Medios por ejemplo RTP

Fig.2

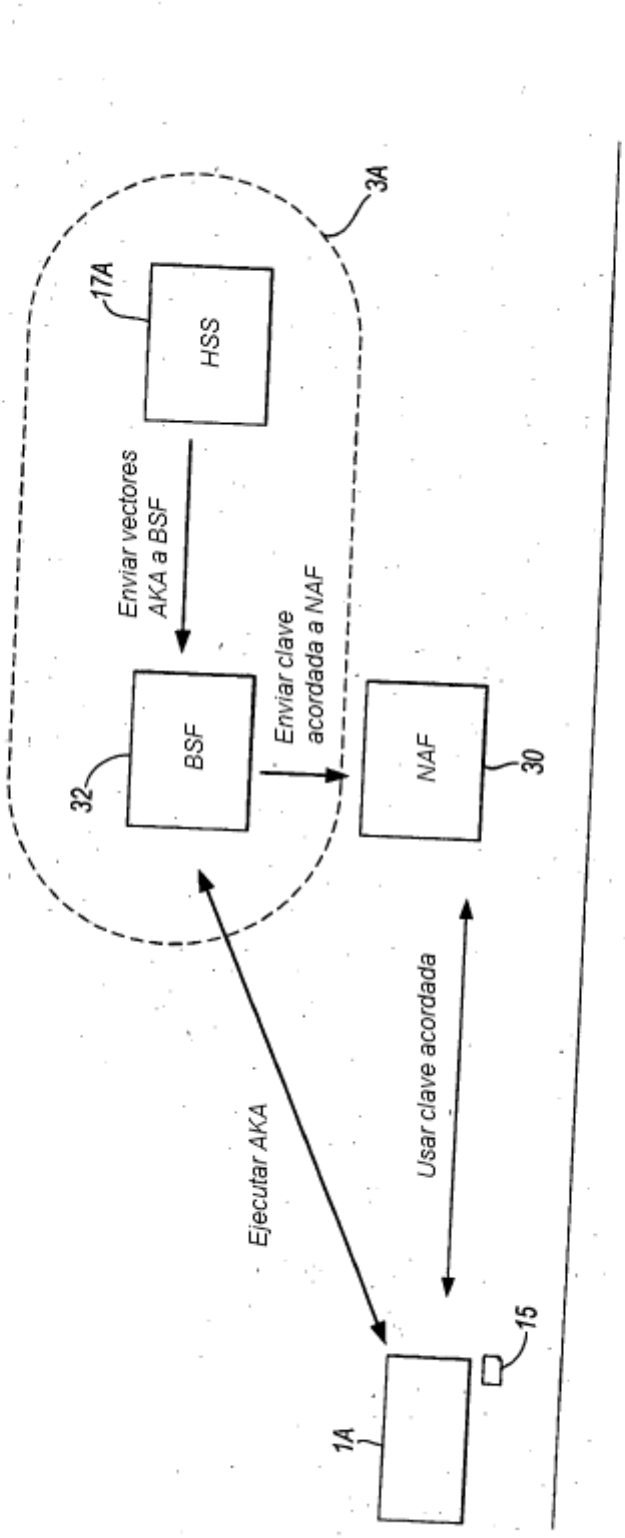
3A
17A
HSS
Enviar vectores AKA a BSF
Enviar clave acordada a NAF
BSF
32
NAF
30
Ejecutar AKA
Usar clave acordada
15
1A

Fig 3

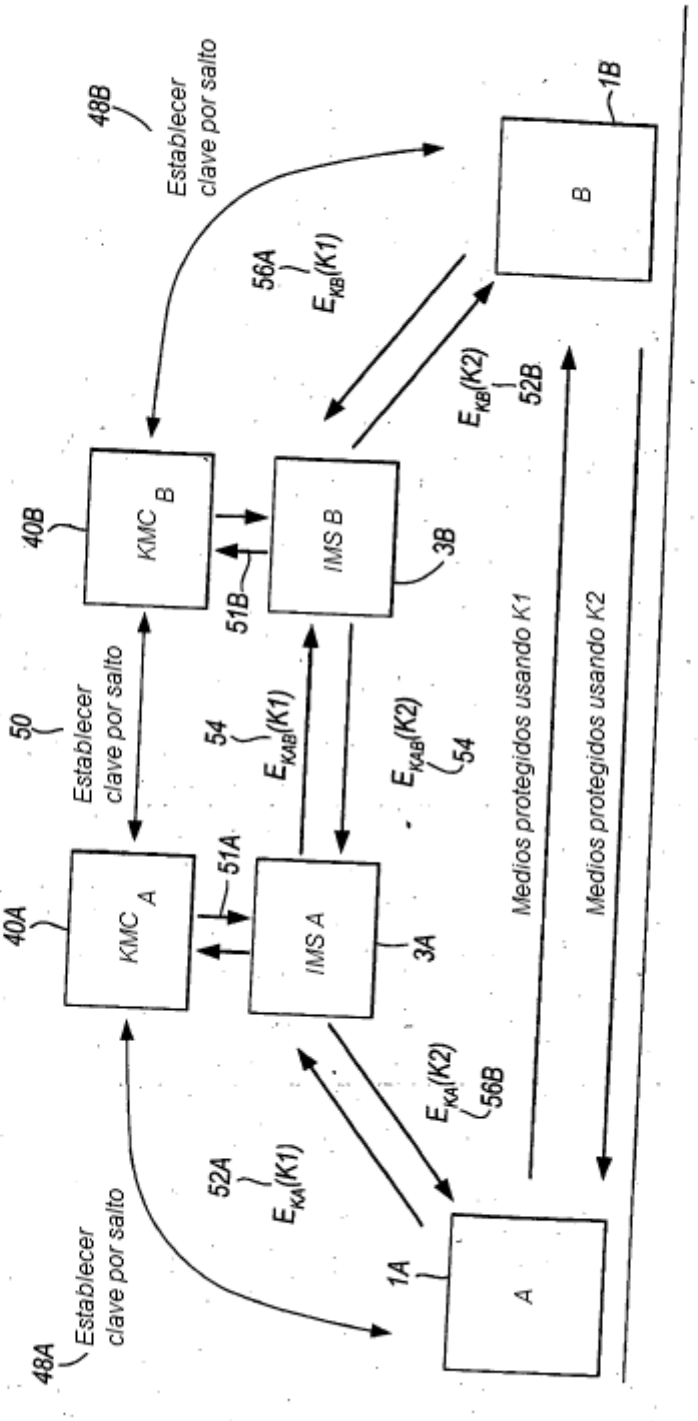
48B
Establecer clave por salto
1B
B
56A
$E_{KB}(K1)$
$E_{KB}(K2)$
52B
40B
KMC B
IMS B
3B
51B
50
Establecer clave por salto
54
$E_{KAB}(K1)$
$E_{KAB}(K2)$
54
40A
KMC A
51A
IMS A
3A
Medios protegidos usando K1
Medios protegidos usando K2
$E_{KA}(K2)$
56B
52A
$E_{KA}(K1)$
1A
A
48A
Establecer clave por salto

Fig. 4