(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 589 112**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.11.2007 PCT/SE2007/050927**

(87) Fecha y número de publicación internacional: **04.06.2009 WO09070075**

(96) Fecha de presentación y número de la solicitud europea: **30.11.2007 E 07852199 (4)**

(97) Fecha y número de publicación de la concesión europea: **29.06.2016 EP 2215769**

(54) Título: **Gestión de claves para comunicación segura**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.11.2016

(73) Titular/es:

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

(72) Inventor/es:

BLOM, ROLF;
CHENG, YI;
LINDHOLM, FREDRIK;
MATTSSON, JOHN;
NÄSLUND, MATS y
NORRMAN, KARL

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Gestión de claves para comunicación segura

Campo de la invención

La invención se encuentra en el campo de establecer una comunicación segura entre puntos finales. En particular, la invención elimina el requisito de que ambos puntos finales utilicen el mismo tipo de credenciales básicas.

Antecedentes de la invención

Muchas tecnologías de acceso tales como GSM, WCDMA, WLAN, WiMAX proporcionan una seguridad básica para el primer salto, es decir, la comunicación entre el dispositivo de usuario y un punto de acceso de la red. La comunicación puede utilizar la capa 2 o la capa 3 de la pila de protocolos. SRTP (RFC3711) y MIKEY (RFC3830) son ejemplos de protocolos para la seguridad de medios y la gestión de claves. MIKEY puede basarse tanto en claves previamente compartidas como en PKI. Adicionalmente, MIKEY puede integrarse en una señalización de configuración de sesión (SIP o RTSP) mediante el uso de RFC4567.

No obstante, la seguridad básica proporcionada por estas tecnologías de acceso no siempre puede considerarse lo suficientemente segura. De hecho, algunas tecnologías de acceso no proporcionan ninguna seguridad básica, p. ej., 802.3/Ethernet o DSL.

Por lo tanto, hay una necesidad de proporcionar mecanismos de seguridad adicionales o mejorados en muchas tecnologías de acceso.

Un problema con los abordajes existentes a la gestión de claves se refiere a la presunción de que ambos puntos finales utilizan el mismo tipo de credenciales básicas. No obstante, esta presunción no siempre resulta acertada, como es el caso en, p. ej., la convergencia fijo-móvil (FMC, por sus siglas en inglés). En la FMC, uno de los usuarios puede ser un suscriptor de 3GPP que utiliza una credencial basada en SIM, p. ej., SIM, USIM, ISIM y el otro puede ser, p. ej., un usuario de acceso por cable que implementa credenciales basadas en PKI.

También hay determinados problemas con la integración de la gestión de claves en los protocolos de señalización conocidos.

Otro ejemplo que presenta un problema se refiere a "medios previos", lo que significa que los medios pueden empezar a fluir desde el respondedor antes de haber finalizado las operaciones de gestión de claves según, p. ej., MIKEY a través de SIP. Por lo tanto, si bien MIKEY puede llevarse a cabo dentro de la banda con SIP, puede no haber ninguna clave disponible para proteger los primeros paquetes. La alternativa, el uso de la gestión de claves de medios dentro de la banda resolvería este problema, pero es desfavorable, p. ej., desde el punto de vista del firewall transversal. Además, no coincide con la práctica de la ingeniería de sonido el transporte de señalización en la vía de los medios.

Otro problema con los métodos conocidos para la gestión de claves se refiere a la “bifurcación”, donde el iniciador, p. ej., de una llamada de telefonía multimedia (MMTEL) puede no estar seguro de qué terminal utilizará para contestar el otro punto final. Aunque todas las terminales para contestar la llamada tengan una PKI activada, las terminales diferentes pueden utilizar distintas claves públicas y, por lo tanto, el iniciador puede no saber qué clave utilizar para una solicitud de invitación. Más precisamente, según métodos conocidos, la gestión de claves no puede iniciarse hasta que el respondedor haya contestado y tampoco puede determinarse una clave pública adecuada hasta entonces. Tal como se mencionó anteriormente, la gestión de claves de medios dentro de la banda puede paliar el problema, pero es desfavorable, como ya se mencionó.

Aun otro problema con métodos conocidos de gestión de claves es que algunos servicios de IMS son entre pares (P2P) mientras que otros proporcionan servicios grupales, p. ej., pulsa y habla por celular (PoC). Exigir que los usuarios gestionen claves grupales genera problemas y, de hecho, un usuario ni siquiera puede estar seguro de que todos los miembros del grupo contesten a una invitación y participen en la sesión. Por lo tanto, en este caso, es necesario realizar una distinción entre miembros que podrían encontrarse en una sesión grupal y los miembros que participan de la sesión grupal, dado que, p. ej., puede ser favorable distribuir claves de sesión solamente a los miembros que de hecho participan.

Un problema adicional con la técnica previa es que algunos servicios, p. ej., mensajería, pueden gestionarse de formas distintas, dependiendo de si el respondedor se encuentra en línea o no. Por ejemplo, un mensaje instantáneo (IM, por sus siglas en inglés) puede convertirse automáticamente en un mensaje diferido (DM, por sus siglas en inglés) para una entrega posterior, si el usuario no se encuentra en línea. El remitente puede no saber si la otra parte se encuentra en línea y, por lo tanto, puede no saber qué gestión de claves es adecuada al momento de enviar el mensaje. Las soluciones basadas en S/MIME podrían paliar la situación, pero S/MIME no es adecuado para medios en tiempo real tales como MMTEL. Por lo tanto, el abordaje de gestión de claves puede pasar a depender del servicio de IMS que se utilice, lo que no es deseable. Además, S/MIME carece de soporte para claves compartidas previamente (p. ej., SIM) y no proporciona protección contra la reproducción debido al hecho de que no hay ningún

concepto de sesión en el que puedan correlacionarse dos mensajes protegidos por S/MIME.

US-2007/0101122-A1 describe un abordaje para la generación de claves de sesión de aplicaciones dentro de un módulo seguro de una terminal de usuario. Se describe la arquitectura genérica de arranque (GBA, por sus siglas en inglés) en 3GPP2.

WO-2005/078988 describe el establecimiento de una clave de sesión secreta compartida entre dos elementos de red, es decir, no terminales de usuario, para una comunicación segura entre sí.

Compendio

Un objetivo general de la invención es superar las deficiencias de los métodos conocidos de establecer una comunicación segura entre una parte iniciador y una parte respondedora mediante el establecimiento de claves compartidas entre los puntos finales que podrían utilizarse de forma directa para la protección de medios o formar la base del establecimiento de claves de extremo a extremo.

Es un objeto establecer claves para la comunicación segura entre la parte iniciante y respondedora que proporcionen una independencia del tipo de credenciales utilizado por la parte respectiva para la gestión de seguridad.

Según la invención, un servidor de gestión de claves, KMS (por sus siglas en inglés), con la capacidad de establecer una clave compartida con un dispositivo de usuario, proporciona al usuario un asiento e información de generación de claves como respuesta a una solicitud de clave. Habiendo recibido dicha información, un primer usuario calcula una clave de sesión y transmite el asiento a una segunda parte en una solicitud de comunicación. Como respuesta a la recepción del asiento, la segunda parte establece una comunicación segura con la misma entidad de KMS u otra, y proporciona el asiento. Como respuesta a esto, el mismo KMS u otro devuelve información de generación de claves. En función de dicha información de generación de claves, tanto la primera como la segunda parte generan una clave de sesión en común.

La integridad del asiento se encuentra protegida, de manera favorable, por la entidad de KMS emisora y puede incluir además metadatos, por ejemplo, identidades de partes implicadas, momento de creación, número de secuencia, tiempo de validez, tipo de uso, tal como pulsa y habla por celular o telefonía, tipo de comunicación, p. ej., entre pares o comunicación grupal. Además, el asiento puede incluir copias de claves de sesión y otra información que requiera encriptarse, por ejemplo, para proteger la privacidad.

En una realización de la invención, la capacidad de establecer una clave compartida se basa en el procedimiento de GBA donde una funcionalidad de BSF de red y usuario se proporcionan con un secreto compartido básico, p. ej., un secreto basado en SIM/USIM/ISIM. La entidad de KMS, de acuerdo con esta realización, actúa como una entidad de NAF hacia la entidad de BSF.

Según otra realización, las claves de sesión generadas por la primera y segunda partes respectivas son distintas, y mediante estas se dispone una parte intermediaria para generar ambas claves para una comunicación segura con cada una de la primera y segunda parte, donde la parte intermediaria es capaz de procesar un mensaje de la primera a la segunda parte, primero, al decodificar el mensaje y, luego del procesamiento, volver a encriptar el mensaje. En particular, la generación de claves en la parte intermediaria se basa en un asiento recibido de la primera parte que, luego de la generación de la clave, se reenvía a la segunda parte para una generación correspondiente de una clave de sesión.

En aun otra realización, la segunda parte se ve representada por un grupo de segundas partes y la parte intermediaria, mediante el uso de un asiento, genera primero una clave maestra y, en base a la clave maestra, genera claves de sesión individuales y asientos para cada miembro del grupo de segundas partes. La parte intermediaria, luego de la generación de la clave, reenvía el asiento a cada una de las segundas partes, y cada una de ellas, luego, genera claves individuales correspondientes de sesión. El grupo de segundas partes puede obtenerse en la parte intermediaria al resolver una identidad de grupo o identificar un grupo predefinido tal como lo especificó la primera parte.

En aun otra realización, la parte intermediaria no procesa información recibida de la primera parte y, por lo tanto, no precisa generar claves separadas para la comunicación con cada una de la primera y segunda partes. En esta realización, la parte intermediaria reenvía el asiento recibido de la primera parte a cada una de las segundas partes del grupo, mediante lo cual la primera y cada una de las segundas partes pueden generar una clave de sesión compartida para una comunicación segura de extremo a extremo. Con la finalidad de eliminar la posibilidad de interceptar el asiento en una parte intermediaria y utilizar el asiento interceptado para solicitar una funcionalidad de KMS para resolver el asiento en una clave de sesión, se proporciona a la entidad de KMS una funcionalidad para verificar que un usuario, para el cual se resuelve un asiento, es un miembro del grupo.

Un mensaje de la primera parte destinado a una segunda parte puede almacenarse en una entidad de red para una entrega diferida. Por ejemplo, la parte intermediaria puede descubrir que al menos una segunda parte no está registrada en la red y puede, por lo tanto, almacenar un mensaje para una entrega posterior, junto con un asiento.

Una vez registrada la al menos una segunda parte, la entidad de red que almacena temporalmente un mensaje puede continuar el protocolo tal como se describió anteriormente y finalmente empujar el mensaje y asiento asociado hacia la parte destinataria.

Según una realización, la invención se implementa en un entorno de IMS 3GPP.

Según un aspecto, se proporciona un método para establecer una comunicación segura entre partes de una red de comunicación, en el que cada parte es capaz de realizar un procedimiento de arranque en función de credenciales locales, donde el arranque crea una clave compartida entre cada parte y una función de arranque asociada. El método comprende las etapas de:

- recibir en la parte iniciadora la primera información de clave, en función de un procedimiento de arranque inicial, y un asiento como respuesta a la solicitud de una primera funcionalidad de gestión de claves;

- almacenar dicha primera información de clave en dicha primera funcionalidad de gestión de clave y hacer referencia a dicha primera información de clave con un identificador incluido en dicho asiento;

- generar, a partir de la primera información de clave, la primera clave de sesión;

- enviar el asiento a al menos una parte respondedora;

- reenviar de la al menos una parte respondedora el asiento o partes del mismo a la segunda funcionalidad de gestión de claves;

- comunicar a la segunda funcionalidad de gestión de claves con la primera funcionalidad de gestión de claves para resolver el asiento en la segunda información de clave, donde dicha comunicación incluye recuperar, en la primera funcionalidad de gestión de clave, la primera información de clave mediante el uso del identificador, y proporcionar a la segunda funcionalidad de gestión de claves información basada en la primera información de clave;

- recibir en la al menos una parte respondedora, de la segunda funcionalidad de gestión de claves, una segunda información de clave, y generar a partir de esta una segunda clave de sesión;

- el uso, de la parte emisora y al menos una parte respondedora, de la primera y segunda claves de sesión para una comunicación segura.

Según otro aspecto de la invención, se proporciona un aparato de gestión de claves. El aparato de gestión de claves brinda soporte a la generación de claves de sesión para una comunicación segura entre partes de una red de comunicaciones. El aparato tiene medios de procesamiento y comprende:

- medios para generar una primera información de clave y un asiento como respuesta a una solicitud de una primera parte, donde se hace referencia a la primera información de clave mediante un identificador incluido en el asiento;

- medios para la comunicación del asiento a la primera parte,

- medios para almacenar la primera información de clave y el identificador,

- medios para comunicarse con un segundo aparato de gestión de claves para resolver un asiento recibido en una segunda información de gestión de claves, donde dicha comunicación incluye recuperar la primera información de clave mediante el uso del identificador, y proporcionar a la segunda funcionalidad de gestión de claves información basada en la primera información de clave.

Descripción detallada.

La siguiente descripción establece detalles específicos, tales como realizaciones, procedimientos, técnicas, etc. particulares, con fines explicativos y no taxativos. En algunas instancias, se omiten descripciones detalladas de métodos, interfaces, circuitos y dispositivos conocidos, a fin de no complicar la descripción con detalles innecesarios. Adicionalmente, se muestran bloques individuales en algunos de los dibujos. Podrá observarse que las funciones de dichos bloques pueden implementarse mediante el uso de circuitos individuales de hardware, mediante el uso de programas de software y datos, junto con un microprocesador digital programado de manera adecuada o computadora de uso general, mediante el uso de circuitos integrados específicos de la aplicación y/o mediante el uso de uno o más procesadores de señal digital.

Con la finalidad de ilustrar la gestión de claves de seguridad, se utiliza la arquitectura 3GPP GBA/GAA. No obstante, se aprecia fácilmente a partir de la descripción que puede utilizarse cualquier otro método para gestionar claves de seguridad que proporcione la generación de una clave compartida entre un UE de usuario y un servidor de aplicación, p. ej., NAF 160. Por ejemplo, un UE que soporta credenciales basadas en PKI podría utilizar TLS para crear una clave compartida con el servidor de la aplicación. En una arquitectura a base de nombre de

usuario/contraseña, podría utilizarse el estándar PKCS#5 para establecer una clave compartida, etc.

La Figura 1 ilustra el despliegue de la técnica previa de GBA/GAA a través de un proxy de autenticación 160 que actúa como una función de aplicación de red NAF (por sus siglas en inglés) contra la infraestructura GBA/GAA. Una función genérica de servidor de arranque 110 BSF y un equipo de usuario 101 UE autentican de forma manual mediante el uso del protocolo AKA de UMTS. El UE se comunica con la BSF a través de una interfaz 120 Ub. El UE y un sistema de suscriptor doméstico 130 (HSS, por sus siglas en inglés) comparten una clave que es la base del HSS para generar un vector de autenticación proporcionado a la BSF a través de la interfaz 170 Zh. Según el protocolo AKA, la BSF envía al UE un desafío y el UE devuelve una respuesta a la BSF. La autenticación se verifica mediante de la comparación por parte de la BSF de la respuesta del UE con una respuesta esperada que proporcionó el HSS. Se inicia en la BSF una autenticación exitosa y se genera en el UE una clave compartida Ks. La BSF almacena la clave Ks y el B-TID de referencia asociado. El B-TID de referencia y otros datos, tales como la vida útil de la clave, se proporcionan después al UE en un mensaje de terminación. La BSF realiza una consulta en la función de localizador del suscriptor 140 SLF (por sus siglas en inglés) a través de la interfaz 191 Dz junto con la operación de la interfaz Zh para obtener el nombre del HSS que contiene los datos específicos requeridos del suscriptor. El UE puede conectarse simultáneamente a al menos un servidor de aplicación AS 150_n a través de un proxy de autenticación de la función de aplicación de red NAF 160. La conexión comprende una primera etapa de autenticación entre el UE y la NAF. Por lo tanto, el UE proporciona el B-TID de referencia al NAF que, mediante el uso del B-TID, solicita una clave (Ks_NAF) de la BSF a través de la interfaz 190 Zn. La clave Ks_NAF se deriva de la clave Ks. La misma clave puede derivarse en el UE. Luego se produce la autenticación, en función de la clave derivada Ks_NAF. La comunicación entre el UE y la NAF es a través de una interfaz Ua 180.

A fines ilustrativos, se utiliza en la siguiente descripción una señalización basada en SIP según IMS de 3GPP. No obstante, como comprende el experto en la técnica, la invención puede utilizar otros protocolos que sean capaces de cargar metadatos necesarios para la configuración de la sesión.

La Figura 2 ilustra elementos básicos de un subsistema de red principal CN (por sus sigas en inglés) de IMS y la conexión al servidor de la aplicación 210. Si bien la Figura 2 indica un servidor de aplicación ubicado dentro de una red doméstica, debe entenderse que la plataforma de servicio también puede ubicarse fuera de la red doméstica.

El subsistema de red principal multimedia IP (IM CN) permite que los operadores de línea fija y PLMN ofrezcan a sus suscriptores servicios multimedia basados y construidos sobre servicios, protocolos y aplicaciones de internet. La intención es que dichos servicios sean desarrollados por operadores de PLMN y otros proveedores terciarios, inclusive aquellos en el espacio de Internet que utilizan los mecanismos proporcionados por la Internet y el sistema de IMS. El sistema de IMS habilita la convergencia de las tecnologías de base web y de datos, mensajería, video y voz y el acceso a estas, para el usuario inalámbrico y de línea fija.

El Proxy-CSCF (P-CSCF) 220 es el primer punto de contacto dentro del sistema de IMS que responde al mensaje SIP INVITE del UE. Su dirección puede ser descubierta por el UE 101 mediante el uso de un mecanismo de descubrimiento. El P-CSCF se comporta como un Proxy, es decir, acepta solicitudes y los revisa de forma interna o los reenvía hacia la servidora de CSCF, S-CSCF 230. La S-CSCF enruta la solicitud de SIP hacia el servidor de aplicación de red doméstica 210.

A continuación se describe una primera realización con referencia a la Figura 3. En la Figura 3, los números similares corresponden a las entidades de las Figuras 1 y 2. Se muestra en la Figura 3 dos entidades de usuario UE_A y UE_B capaces de realizar un arranque según el método de GBA/GAA con las funciones respectivas de arranque BSF_A, 110_A y BSF_B 110_B. No obstante, como comprende el experto en la técnica, puede utilizarse cualquier otro medio disponible para la creación de una clave compartida con un servidor de este tipo. Por lo tanto, el arranque puede basarse en una credencial de identificación, p. ej., SIM, USIM, ISIM o PKI, o nombre de usuario/contraseña. El arranque produce que cada UE y BSF asociada puedan determinar una clave compartida Ks_A, respectivamente Ks_B. Los usuarios A y B desean establecer una comunicación ilustrada en 320. Según la invención, un servidor de gestión de claves KMS_A y KMS_B, indicado mediante 310_A y 310_B, respectivamente, soporta a cada UE.

Según la invención, los usuarios A y B pueden basar su gestión de seguridad respectiva en credenciales distintas, p. ej., basada en una tarjeta de identidad tal como una tarjeta *SIM (SIM, USIM, ISIM), usuario/contraseña, clave pública PKI o contraseña.

La señalización de redes entre dominios entre las entidades de gestión de claves KMS, que se indica en 330, puede asegurarse mediante el uso, p. ej., de TLS o IPsec. La señalización puede encriptarse y/o puede tener una protección de integridad.

Las interfaces usuales de GBA/GAA Ua, Ub, Zn se indican en la Figura 3 que se corresponde con la Figura 1.

Se hace referencia ahora a la Figura 4, que muestra un diagrama de señales según una realización de la invención. En la Figura 4, las entidades de la estructura de IMS y la estructura de GBA/GAA se indican tal como se explicó con respecto a las Figuras 1-3. A fines de simplicidad, el usuario A también se denota como UE_A de manera intercambiable.

A continuación, (x)k denota la protección de x mediante la clave K. Por protección se entiende protección de la integridad y/o confidencialidad, y dicha protección de confidencialidad puede aplicarse únicamente a partes de un mensaje x.

Se realizan ahora las etapas 1 y 2 según la técnica previa.

En la etapa 1, el usuario A se registra en IMS.

En la etapa 2, el usuario A realiza un arranque de GBA, mediante el cual se genera una clave Ks_A y se comparte entre A y BSF_A. En esta etapa, BSF_A proporciona A con una B-TID_A de referencia. La etapa 2 incluye la subetapa 2:1 en la cual KMS_A recibe de A la B-TID de referencia que se utiliza luego para capturar de BSF_A una clave KA = Ks_KMS_A derivada de Ks_A. El usuario A calcula la misma clave sabiendo Ks_A y otra información ingresada en la derivación. Por lo tanto, A y KMS_A comparten una clave KA que puede utilizarse para una comunicación segura.

Se realizan etapas correspondientes del lado B indicadas en la Figura 4 con los mismos números de referencia, donde se generan las entidades correspondientes, es decir, Ks_B, B-TID_B y KB = Ks_KMS_B.

Cabe destacar que B, como usuario, puede tener varios dispositivos, cada uno de los cuales puede utilizarse para la comunicación. No obstante, la clave KB es válida únicamente para un dispositivo en particular que realizó un arranque según las etapas 1 y 2. El caso de que B pueda utilizar varios dispositivos puede llevar a un problema de bifurcación que se trata adicionalmente en una realización alternativa. Para la presente primera realización, se asume que B responde a una invitación de comunicación mediante el uso de un solo dispositivo.

En 3, el usuario A decide comunicarse con el usuario B.

En la etapa 4, A envía una solicitud de clave al servidor de gestión de claves KMS_A según la invención. La clave generada en esta etapa se utiliza posteriormente para una comunicación segura de extremo a extremo con B. La solicitud de clave tiene el formato:

$$\text{GET key info} = (\text{Id\_A, Id\_B, key\_type, param, ...})_{KA}\text{, B-TID\_A}$$

En donde Id_A e Id_B son entidades que identifican a los usuarios A y B respectivamente, key_type es el tipo de clave solicitada, p. ej., una clave para la comunicación de punto a punto o una clave para comunicación grupal. Id_A puede tener la forma de un identificador global, por ejemplo, Id_A = A®op.com. Finalmente, param denota cualquier otro parámetro que pueda incluirse en el mensaje. El mensaje se encripta mediante la clave KA generada anteriormente. Además, se incluye la B-TID de referencia en el mensaje, lo que permite que KMS_A obtenga la clave KA de BSF_A según el procedimiento de GBA/GAA. De manera alternativa, en un abordaje no basado en GBA del arranque, podría utilizarse algún otro identificador de clave si Id_A no determina la clave KA de forma única. Cabe destacar que nada se menciona en la presente sobre el tipo de credencial que utiliza el receptor B y, por lo tanto, el método según la invención no depende del tipo de credencial en el remitente A o receptor B.

En 5, KMS_A responde a A con el mensaje “RETURN key info” de la forma:

$$\text{RETURN key info} = (\text{Key\_info\_A, VOUCHER})_{KA}$$

En donde Key_info_A comprende una clave K_{AB} o material de generación de claves que permite que A calcule, en la etapa 6, una clave K_{AB}. La entidad VOUCHER (asiento), según la invención, comprende información que habilita a KMS_B volver a generar, posteriormente, la misma clave K_{AB} que permite que A y B se comuniquen de forma segura. Para que KMS_B sepa sobre KMS_A, el asiento incluye Id_A.

Además, la integridad del asiento está protegida y al menos partes de este pueden encriptarse. Por ejemplo, pueden derivarse de la clave KA claves de integridad y confidencialidad.

La clave K_{AB}, por ejemplo, puede generarse como una función criptográfica de KA y las identidades de A y B y/o un nonce. En este caso, Key_info_A contendría dicho nonce. De manera alternativa, K_{AB} puede ser una clave completamente aleatoria, en cuyo caso Key_info_A comprende la clave K_{AB} en sí.

Según la presente realización, la información del asiento incluye un puntero, por ejemplo B-TID, para la recuperación de la clave K_{AB} o material de claves almacenado en KMS_A. Puede incluirse otra información en el asiento, tal como, p. ej., la información de tipo de clave, tal como comunicación entre pares o grupal, identidad de las partes involucradas, emisor del asiento, es decir, identidad de KMS_A, momento de emisión o número de secuencia, tiempo de validez, tipo de uso, tal como pulsar por celular (PoC) o telefonía multimedia (MMTEL).

En la etapa 7, A dirige una INVITACIÓN de SIP al usuario B que, según la infraestructura de IMS, pasa P-CSCF, S-CSCF que da servicio a A y llega a S-CSCF que da servicio a B. En la etapa 8, el mensaje de invitación se reenvía al usuario B. El mensaje de invitación incluye al menos el asiento. Otra información de este mensaje puede incluir información del tipo de clave.

En la etapa 9, el usuario B reenvía el asiento en un mensaje de "GET key info" a KMS_B para la regeneración, a partir de este, de la clave K_{AB}, donde el mensaje, por ejemplo, tiene la forma:

GET key info = VOUCHER, B-TID_B

Aquí, B-TID_B es la referencia de GBA/GAA para autenticar al usuario B y establecer una clave KB para una comunicación segura entre el usuario B y KMS_B de la misma forma que se mencionó anteriormente con respecto a la etapa 4.

En la etapa 9:1 se produce la comunicación entre KMS_A y KMS_B, en donde KMS_A soporta a KMS_B en la generación de la clave K_{AB}. Según la primera realización, el asiento incluye un puntero generado por KMS_A en la etapa 5 y la habilitación de KMS_A para que recupere material de claves, el mismo que se devolvió en la etapa 5 al usuario A. Dicho puntero puede incluirse en una solicitud de clave comunicada en la etapa 9:1 con la forma:

Aquí, el puntero se extrae del asiento en KMS_B y se utiliza para recuperar material de claves en KMS_A. Id_B es un identificador del usuario B. La inclusión de Id_B en la solicitud de clave, mediante KMS_B, permite que KMS_A determine que es el usuario B deseado quien solicita una clave, es decir, que nadie más interceptó el asiento con la finalidad de obtener una clave para una comunicación segura con el usuario A, pretendiendo ser el usuario B.

Como respuesta a la solicitud de clave, KMS_A devuelve la información de claves Key_info_B que comprende la clave K_{AB} o la información de clave que, luego, reenvía KMS_B en la etapa 10 al usuario B para la generación de la clave K_{AB} en la etapa 11. La información de claves de la etapa 10 se encripta mediante el uso de la clave KB, por ejemplo, generada en la etapa 9. Si se entrega solamente material de claves en la etapa 10, se lleva a cabo una generación de clave en la etapa 11 y se genera una clave K_{AB}.

La etapa 11 implica que el usuario B devuelva una resputa OK de SIP 200 a la señal de invitación 7, tras la cual inicia la sesión entre A y B.

De manera favorable, según la primera realización, el puntero mencionado anteriormente comprende la entidad B-TID_A.

Si la información de tipo de clave especifica una comunicación de punto a punto, la clave que se devuelve a KMS_B en la etapa 9:1 es suficiente y no es necesario un procesamiento posterior de claves.

Se conoce a partir del estándar de GBA/GAA que la B-TID de referencia puede tener una vida útil. Por lo tanto, en una realización alternativa, el KMS_A mantiene el estado al almacenar al menos una B-TID utilizada anteriormente y el material de clave correspondiente con la finalidad de gestionar el caso en que el usuario A haya realizado un nuevo arranque y generado una nueva B-TID.

Con respecto a la Figura 5, se describe una segunda realización con respecto al caso de que la información de claves (info de claves) indique que se solicita una clave grupal. En la Figura 5, se inserta un intermediario entre los lados A y B. Preferiblemente, el intermediario se divide en un intermediario de parte A IM_A y un intermediario de parte B IM_B. Por ejemplo, la parte respectiva puede comprender un servidor de pulsar para hablar por celular, denotado servidor de PoC. En la Figura 5, la anotación B de la parte receptora representa ahora un grupo de usuarios donde cada uno tiene una identidad individual ID_B_k. Además, a fines de simplicidad, se asume que cada usuario en el lado B se conecta a la misma BSF_B y al mismo KMS_B, aunque cada usuario puede utilizar funcionalidades separadas de BSF y KMS.

En la Figura 5, las referencias a señales similares indican señales similares de la Figura 4, aunque las partes del mensaje de la señal pueden ser ligeramente distintas, tal como se explica en mayor detalle más adelante.

Las etapas 1, 2, 2:1 y 3 son idénticas a las etapas correspondientes según la primera realización, con la excepción de que en la etapa 3, la denominada parte B ahora representa a un grupo identificado con una identidad grupal G_{ID}.

En la etapa 4, el mensaje GET ahora incluye G_{ID}. En la etapa 5 se devuelve un asiento y material de claves, p. ej., una clave maestra K, para la generación, en la etapa 6, de una clave de sesión K_{IMA}; de manera alternativa, la clave de sesión se incluye en el mensaje devuelto. Cabe destacar que dicha clave de sesión será utilizada posteriormente por A para la comunicación con el intermediario, p. ej., IM_A, en vez de directamente con los participantes del grupo. La clave maestra y otra información pueden protegerse con la clave KA generada en las etapas de arranque 2, 2:1.

En la etapa 7:1, similar a la etapa 7 de la Figura 4, se envía al grupo un mensaje de INVITE a través del intermediario o, de manera alternativa, a la parte IM_A del intermediario. El mensaje de invitación incluye el asiento y otra información que comprende al menos G_{ID}.

En la etapa 8:1, el intermediario IM_A, al reconocer que ID_A del asiento es una clave grupal, reenvía el asiento a KMS_A y solicita material de claves, tras lo cual KMS_A devuelve a IM_A dicha clave maestra K. Adicionalmente, la clave de sesión K_{IMA} se devuelve o se genera en IM_A a partir de la clave maestra.

En la etapa 8:2, IM_A resuelve la identidad del grupo proporcionada en el mensaje de invitación en un grupo de

identidades de usuario ID_B_k y genera, a partir de la clave maestra K, una clave de sesión individual K_{IMB} para cada miembro del grupo. Se entiende que se genera una clave individual K_{IMB} para cada B_k. Además, de no recibirse desde KMS_A, la clave de sesión K_{IMA} se genera a partir de la clave maestra K. Cabe destacar que el intermediario puede precisar soporte de un servidor de gestión de grupos asociado, que no se muestra, para recuperar los miembros individuales del grupo de la ID grupal.

La clave individual K_{IMB} puede calcularse como K_{IMB} = F(K, "X") en donde "X" denota algún identificador característico de la parte X que representa al grupo B_k.

Las claves de sesión K_{IMA} y K_{IMB} se utilizan luego para proteger los enlaces de comunicación A - intermediario, respectivamente, intermediario - B.

En la etapa 7, el intermediario IM_A envía un mensaje INVITE de SIP a todos los miembros del grupo que incluyen el asiento. Según la infraestructura de IMS, el mensaje pasa S-CSCF y luego, en la etapa 8, a través P_CSCF hacia la red que da servicio al receptor B_k. El mensaje 7 corresponde a dicho mensaje de la Figura 4, aunque, en la presente realización, el remitente es el intermediario en vez del usuario A.

En la etapa 9, que corresponde a la etapa 9 de la Figura 4, cada receptor B_k entra en contacto con un KMS_B de servicio para resolver el asiento en claves adecuadas.

En la etapa 9:1, similar a la primera realización, se produce una comunicación entre KMS_A y KMS_B, en donde KMS_A devuelve la clave K_{IMB} o, de manera alternativa, la clave maestra K, a KMS_B y de ahí se reenvía, en la etapa 10, a cada miembro del grupo, protegida con la clave del miembro individual del grupo KB_k indicada, a fines de simplicidad, como la clave KB en la Figura 5. El mensaje 10 corresponde al mismo mensaje de la Figura 4. Debería entenderse que la etapa 10 se repite para todos los miembros del grupo B_k. Las claves KB se calculan de forma correspondiente a KA y se asume que cada B_k llevó a cabo un arranque con una funcionalidad BSF asociada. En el caso en que KMS_A devuelva la clave maestra K, cada B_k calcula a partir de la clave correspondiente K_{IMB}.

En la etapa 11 se devuelve una señal OK 200 como respuesta a las señales respectivas de invitación 7:1, 7 y 8, tras lo cual puede iniciar la sesión entre A - IM - B_k (k = 1, 2, ...).

Ahora, A puede comunicarse con los miembros del grupo B_k, tras lo cual A encripta la comunicación mediante el uso de la clave K_{IMA} hacia el intermediario, donde el mensaje de decodifica y posiblemente se procesa, p. ej., se transcodifica antes de reenviarse, se vuelve a encriptar con la clave K_{IMB}, individualmente para todos los B_k.

De manera alternativa, $K_{IMA} = K_{IMB}$.

Según una alternativa de la segunda realización, la etapa 8:1 no incluye la clave K_{IMA} ni la clave maestra K. Por lo tanto, en esta realización, el intermediario no puede decodificar la comunicación de la parte iniciadora A para su procesamiento. Por consiguiente, la etapa de reencripción de la comunicación con la clave K_{IMB} no es pertinente. Por lo tanto, el intermediario, en este caso, actúa básicamente para resolver una identidad grupal en miembros individuales de un grupo respondedor para proporcionar un mensaje de INVITE a cada miembro y, posteriormente, para reenviar la comunicación de A a cada B_k sin ningún procesamiento posterior de la información.

Una alternativa de la segunda realización comprende calcular claves separadas para un vínculo superior, hacia el intermediario, respectivamente un vínculo inferior, en dirección del intermediario hacia los usuarios A y B. Dicha clave maestra K puede ser la base para la generación de claves.

Según una realización alternativa de la segunda realización, el tipo de clave indica una clave grupal ad hoc mediante la cual, en la etapa 8:1, IM_A solicita el material de claves K y genera, en la etapa 8:2, un grupo de identidades de usuario ID_B_k a partir de la enumeración de las partes proporcionada en el mensaje de invitación 7:1 de A. Finalmente, IM_A genera, a partir de la clave maestra K, una clave individual KB_k para cada miembro del grupo ad hoc especificado por el usuario A.

Según aun otra alternativa de la segunda realización, cada miembro del grupo obtiene una clave individual que puede además ser distinta para un vínculo superior, en dirección del usuario B hacia el intermediario IM_A, y un vínculo inferior, en dirección del intermediario IM_A al usuario B. Por ejemplo, IM_A puede realizar una personalización de claves según el esquema:

Aquí, "B_k" denota algunos datos característicos para el individuo B_k y K es la clave maestra definida anteriormente. Con la finalidad de que cada B_k genere la misma clave correspondiente, la señal de invitación de las etapas 7 y 8 incluye, de preferencia, la información característica "B_k" incluida adicionalmente in el mensaje de solicitud 10 a KMS_B, en donde, luego de esto, se realiza la personalización. La clave personalizada se proporciona finalmente al usuario B_k en la señal 10.

Según una alternativa de la realización anterior, el intermediario se comunica con el grupo de B_k a través de multidifusión. En este caso, todos los usuarios B_k deberían utilizar la misma clave grupal para recibir información de vínculo inferior. Por lo tanto, no se realiza en este caso ninguna personalización de vínculo inferior y todos los

usuarios B_k reciben la misma clave de vínculo inferior de KMS_A.

Según otra alternativa de la segunda realización, el intermediario no se encuentra incluido en el procesamiento, p. ej., transcodificación, de la comunicación del usuario A y, por lo tanto, no se le proporciona una capacidad de decodificar la carga comunicada por el usuario A. En este caso, por lo tanto, se omiten las etapas 8:1 y 8:2 y, en las etapas 7 y 8, el asiento simplemente se reenvía al grupo identificado por el intermediario IM_A mediante la resolución del identificador grupal. Se utiliza entonces del lado del receptor el mismo mecanismo de resolución de claves de la primera realización. Eficazmente, esto significa que los lados A y B se comunican de extremo a extremo sin la interferencia del intermediario.

Puede aparecer un problema general, p. ej., más probablemente en el caso de la multidifusión, y es que un usuario no autorizado que haya interceptado el vínculo de señalización o intermediario y haya obtenido el asiento podría reenviarlo a la funcionalidad KMS y solicitar que se resuelva. Por lo tanto, de preferencia, la funcionalidad KMS debería ser capaz de verificar que los usuarios para los cuales resuelve los asientos sean miembros autorizados del grupo. Por lo tanto, según esta realización alternativa, se incluye un identificador aleatorio único de usuario, u otro identificador único, en la señalización de SIP del intermediario con el asiento. Debido a la protección de la señalización de SIP, el identificador está protegido ante una parte externa que logra acceder al asiento y al identificador. La funcionalidad de KMS puede verificar que un identificador aleatorio no fue presentado ya por algún otro usuario.

Como alternativa, el identificador también puede ingresarse en la derivación de clave para los usuarios individuales.

Según la primera y segunda realizaciones, el material de claves obtenido en la señal de solicitud 4 puede incluir una o más claves de sesión K_{AB} o K_{IMA}. La una o más claves de sesión recibidas pueden utilizarse de forma directa o indirecta, p. ej., mediante el uso del protocolo MIKEY, para asegurar los datos de carga.

No obstante, en una alternativa de la primera y segunda realizaciones, la señal 5 puede incluir uno o más nonces de los cuales pueden derivarse las claves de sesión correspondientes, p. ej., de KA = Ks_KMS_A. El transporte de estos nonces, p. ej., incluido en el asiento, no precisa encriptarse.

Puede ocurrir un problema si el usuario A se desconecta o realiza un nuevo arranque, mediante el cual la clave anterior KA = Ks_KMS_A puede ya no ser válida, ya que puede producirse una clave KA' a partir del nuevo arranque. Cuando KMS_A recibe el asiento, la información de este no sería útil en la recreación de la clave de sesión K_{AB} o K_{IMA}.

Por lo tanto, en una alternativa de la primera y segunda realizaciones, KMS_A mantiene el estado y guarda las claves utilizadas anteriormente KA.

En aun otra alternativa, el asiento puede incluir una copia de la clave KA, en un campo de asiento protegido por una clave que sólo conoce KMS_A. En el último caso, solo precisan mantenerse las claves secretas y no hay necesidad de mantener el estado de usuario individual mediante KMS_A.

Según otra alternativa de la primera y segunda realizaciones, el S-CSCF de la etapa 7 de las Figuras 4 y 5, puede llevar a cabo las etapas 9 y 10 de las Figuras 4 y 5, en nombre del usuario B o, en el caso del grupo, cada usuario B_k, y reemplazar el asiento por la información de generación de clave e incluirla directamente en el mensaje de SIP reenviado en la etapa 8. De manera alternativa, la etapa 8 se lleva a cabo mediante algún otro método, p. ej., inserción de GBA, mediante la cual S-CSCF finaliza la señalización de SIP el enviar la señal 12.

En el caso particular de que cualquiera de B o B_k pueda responder a la señal INVITE de SIP 8 en cualquiera de varios dispositivos disponibles, deben tomarse algunas precauciones. En este caso, un dispositivo respondedor generó una clave particular KB' o KB_k' a partir de las etapas de arranque 1 y 2. Por lo tanto, la S-CSCF, sin saber qué dispositivo se utilizará para responder al mensaje de invitación, debe incluir todas las posibilidades al llevar a cabo la etapa 9 y repetir la etapa 9 para generar todas las claves individuales posibles K'_{IMB}. Por lo tanto, cuando la S-CSCF recibe finalmente la respuesta a la solicitud de INVITE de SIP 8, se prepara una clave adecuada K'_{IMB} y está lista para ser utilizada en la etapa 10.

Cabe destacar que las realizaciones alternativas descritas requieren un modelo de confianza distinto, en el sentido de que la S-CSCF sabe que debe confiarse en las claves para la protección de la comunicación del operador del centro de SIP. No obstante, esto es normalmente una presunción válida.

Otra alternativa de la primera y segunda realizaciones se refiere al servicio de mensajería, es decir, el usuario A envía un mensaje a B o a cada uno de B_k en el caso del grupo. El mensaje puede incluirse en el mensaje de invitación 7 o 7:1. Si la S-CSCF determina que al menos un recipiente no está registrado en la red, un mensaje de A puede almacenarse en un nodo de la red, por ejemplo, en el nodo de red S_CSCF, junto con el asiento, hasta que se registre como activo el receptor B o B_k. Luego, cuando B se registra en la red, la S-CSCF puede proseguir con el protocolo e insertar el asiento en B o B_k, por ejemplo, mediante el uso de inserción de GBA, e informar a B o B_k dónde encontrar el mensaje. Este abordaje es generalmente válido para cualquier servicio que pueda tratarse como un servicio diferido. Dado que A puede haberse desconectado y/o realizado un arranque nuevo, pueden utilizarse

mecanismos similares a los mencionados anteriormente para verificar que KMS_A sea capaz de recuperar la información correcta de generación de claves.

Si bien la Figura 3 indica interfaces específicas entre funcionalidades implicadas en el método según la invención, se comprende fácilmente que las interfaces pueden disponerse de forma distinta de varias formas, p. ej., tal como se indica en la Figura 6. En la Figura 6, las interfaces T_A y T_B1 corresponden a la interfaz conocida Ua según el método GBA. La interfaz T_B2 es una alternativa a T_B1, donde el usuario B se comunica con KMS_A en vez de con KMS_B.

K_AB1 indica una interfaz entre las funcionalidades de KMS necesarias para resolver un asiento.

K_AB2 es una interfaz de gestión de claves entre dominios entre KMS en el dominio de B y BSF en el dominio de A. KMS en el dominio de B puede utilizar esta interfaz para obtener ayuda en la resolución de un asiento en una clave.

K_AB3 es una interfaz de gestión de claves entre dominios entre el KMS en el dominio de A y BSF en el dominio de B.

Se comprende fácilmente que tanto la primera como la segunda realización proporcionan una intercepción legal en la funcionalidad de KMS. Una autoridad que conoce la clave KA puede generar la clave de sesión K_{AB} o, en la segunda realización, la clave K_{IMA}, lo que permite que la autoridad intercepte la comunicación de A hacia B o el intermediario.

Se ilustra en la Figura 7 un aparato según la invención que soporta la generación de claves de sesión para una comunicación segura entre partes en una red de comunicaciones.

En la Figura 7, en 710, se muestra una unidad de entrada/salida. El medio 710 puede comunicar información de clave con otras unidades de soporte o usuarios finales, por ejemplo, recibir del usuario final una solicitud de información de clave o un asiento para resolverlo en información de clave. El medio 710 proporciona además comunicación con una funcionalidad de arranque de soporte para recibir material de claves generado en un procedimiento de arranque.

El medio 720 proporciona la generación de información de claves tal como la derivación del material de claves a partir de información de arranque, por ejemplo, recibida de una funcionalidad de arranque.

El medio 730 procesa un asiento recibido para recuperar información de claves almacenada del almacenamiento 740. El medio 730 puede además resolver, posiblemente en comunicación con unidades de red de soporte, una identidad de grupo de usuarios en miembros individuales del grupo.

En 750, el medio de procesamiento general proporciona el control necesario de los diversos procesos.

La invención descrita a modo de ejemplo no taxativo puede comprenderse fácilmente para proporcionar numerosas variaciones, p. ej., para implementar entidades funcionales, interfaces de comunicación y señalización.

REIVINDICACIONES

1. Un método para establecer una comunicación segura entre partes de una red de comunicación, en el que cada parte es capaz de realizar un procedimiento de arranque en función de credenciales locales, donde el arranque crea una clave compartida entre cada parte y una función de arranque asociada caracterizada por las etapas de:

- recibir en la parte iniciadora la primera información de clave, en función de dicho procedimiento de arranque, y un asiento como respuesta a la solicitud de sesión enviada a una primera funcionalidad de gestión de claves;

- almacenar dicha primera información de clave en dicha primera funcionalidad de gestión de clave, en donde se hace referencia a dicha información de clave con un identificador incluido en dicho asiento;

- generar, a partir de la primera información de clave, una primera clave de sesión;

- enviar el asiento a al menos una parte respondedora;

- reenviar de la al menos una parte respondedora el asiento o partes del mismo a una segunda funcionalidad de gestión de claves;

comunicar a la segunda funcionalidad de gestión de claves con dicha primera funcionalidad de gestión de claves para resolver el asiento en la segunda información de clave, en donde dicha comunicación incluye recuperar, en la primera funcionalidad de gestión de clave, la primera información de clave mediante el uso del identificador, y proporcionar a la segunda funcionalidad de gestión de claves información basada en la primera información de clave;

- recibir en la al menos una parte respondedora, la segunda funcionalidad de gestión de claves, dicha segunda información de clave, y generar a partir de esta una segunda clave de sesión;

el uso, de la parte emisora y al menos una parte respondedora, de la primera y segunda claves de sesión para una comunicación segura.

2. El método de la reivindicación 1, caracterizado por que el arranque se realiza según el método de GBA.

3. El método de la reivindicación 1, en donde la al menos una información de clave comprende una clave de sesión, mediante la cual se elimina la etapa de generación correspondiente.

4. El método de la reivindicación 1, caracterizado por que las etapas de recibir implican la protección de la información recibida mediante una clave que se deriva de dicha clave compartida creada durante el arranque de la parte respectiva con la función de arranque asociada.

5. El método de la reivindicación 1, caracterizado por que dicho almacenamiento comprende, además, almacenar la primera información de clave obtenida de al menos un procedimiento de arranque antes del inicial.

6. El método de la reivindicación 1, caracterizado por que dicho identificador comprende un nonce.

7. El método de la reivindicación 1, caracterizado por que dicho identificador comprende una dirección de referencia.

8. El método de la reivindicación 1, caracterizado por que la primera información de clave comprende una clave maestra y que al menos una parte respondedora comprende un intermediario que es el receptor en la etapa del envío y en las etapas posteriores antes de la etapa del reenvío:

- el reenvío del intermediario de al menos partes del asiento a la primera funcionalidad de gestión de claves;

- la recuperación en la primera funcionalidad de gestión de claves, mediante el uso del asiento, de la clave maestra K y el cálculo, a partir de esta, de la segunda información de clave para la al menos una parte respondedora;

- la recepción, en el intermediario, de una respuesta de la primera funcionalidad de gestión de claves que inicia el envío del asiento a la al menos una parte respondedora;

y adicionalmente el avance de dicha comunicación segura a lo largo de una vía desde la parte emisora hacia el intermediario, y desde este a la al menos una parte respondedora.

9. El método de la reivindicación 8, caracterizado por que el envío desde el intermediario se dirige a un grupo de al menos una parte respondedora determinada a partir de una identidad grupal proporcionada en el asiento.

10. El método de la reivindicación 8, caracterizado por que dicha respuesta incluye la clave maestra K que habilita al intermediario a generar claves de sesión para las partes emisora y respondedora.

11. El método de la reivindicación 10, caracterizado por que el intermediario decodifica, mediante el uso de la clave de sesión de la parte emisora, el procesamiento de la comunicación, seguido por la reencripción de la comunicación mediante el uso de la clave de sesión para cada una de las partes respondedoras.

12. El método de la reivindicación 9, caracterizado por que la primera funcionalidad de gestión de claves realiza una verificación de que un usuario, para el cual resuelve un asiento, es un miembro del grupo.

13. El método de cualquiera de las reivindicaciones que anteceden, caracterizado por que la entidad de red determina que al menos una parte respondedora no está registrada en la red, mediante lo cual se interrumpe el procesamiento y dicha entidad de red almacena información comunicada desde la parte emisora y el asiento pertinente hasta que se detecte un registro, tras lo cual dicha entidad de red continúa el procesamiento e inserta el asiento hacia la al menos una parte respondedora.

14. Un aparato de gestión de claves que brinda soporte a la generación de claves de sesión para una comunicación segura entre partes de una red de comunicaciones, en donde el aparato tiene medios de procesamiento y se caracteriza por:

- medios para generar una primera información de clave y un asiento como respuesta a una solicitud de una primera parte, donde se hace referencia a la primera información de clave mediante un identificador incluido en el asiento;

- medios para la comunicación del asiento a la primera parte,

- medios para almacenar la primera información de clave y el identificador,

- medios para comunicarse con un segundo aparato de gestión de claves para resolver un asiento recibido en una segunda información de gestión de claves, donde dicha comunicación incluye recuperar la primera información de clave mediante el uso del identificador, y proporcionar a la segunda funcionalidad de gestión de claves información basada en la primera información de clave.

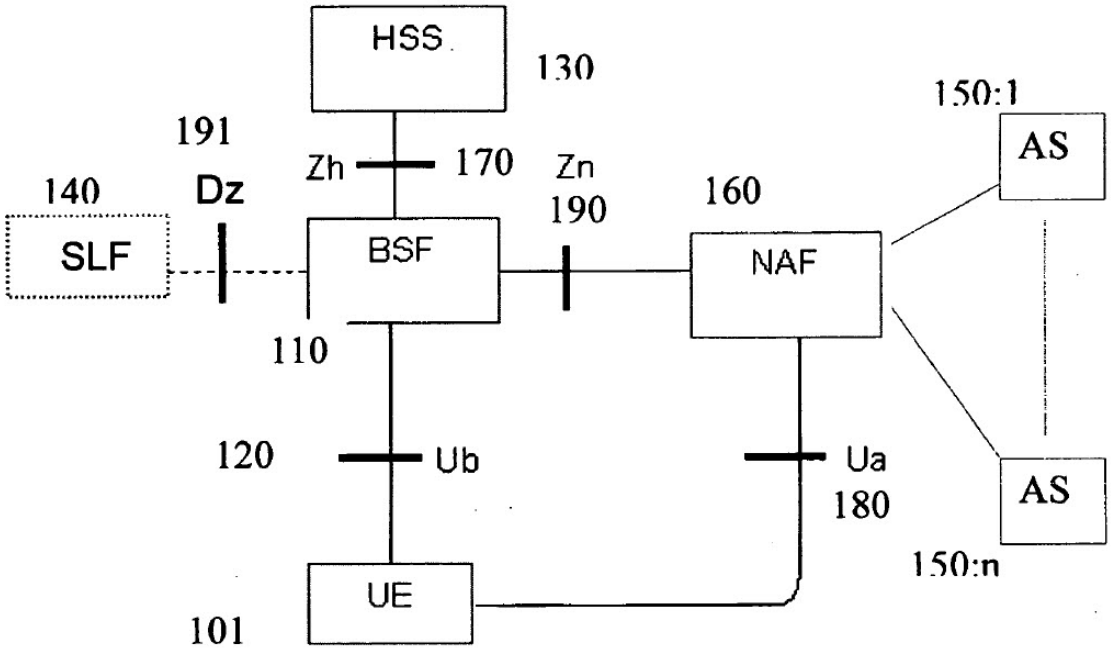
HSS
130
150:1
AS
191
Zh
170
Zn
190
160
140
Dz
SLF
BSF
NAF
110
120
Ub
Ua
180
AS
150:n
UE
101

Figura 1

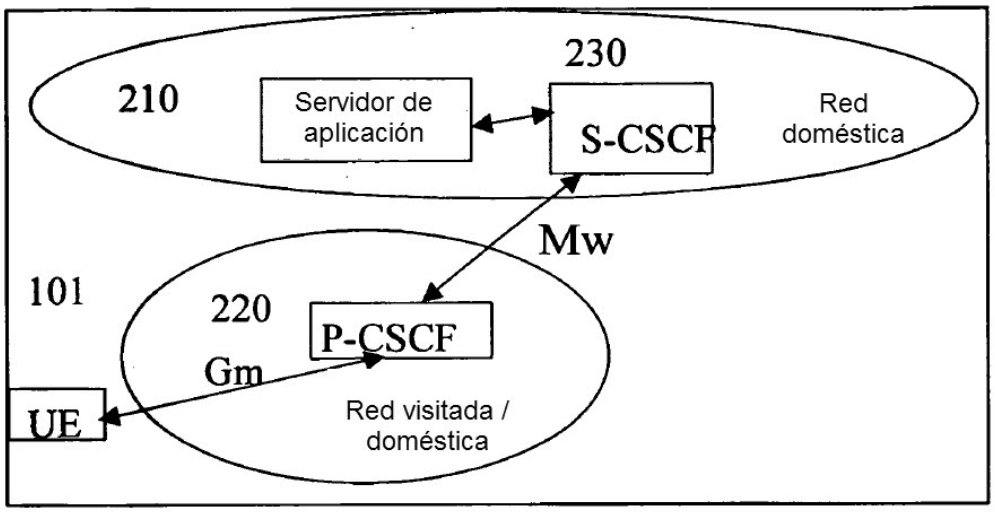

Figura 2

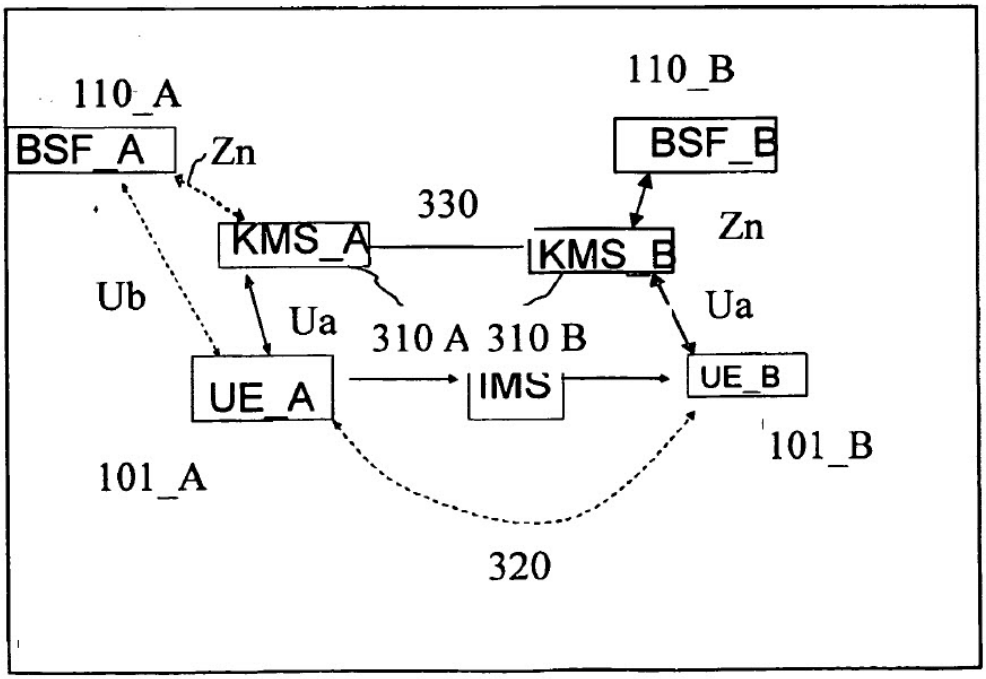

Figura 3

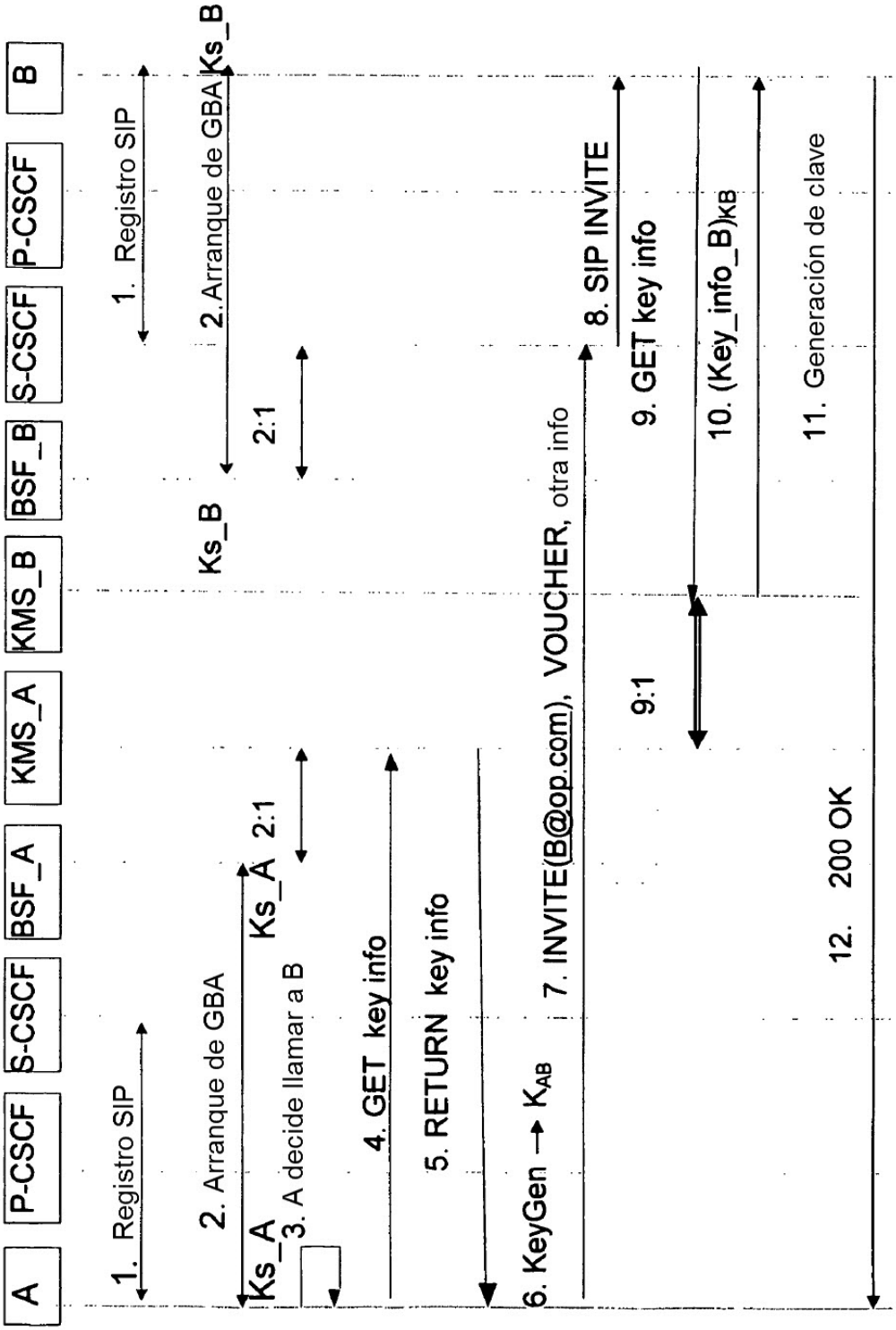
A
P-CSCF
S-CSCF
BSF_A
KMS_A
KMS_B
BSF_B
S-CSCF
P-CSCF
B
1. Registro SIP
1. Registro SIP
2. Arranque de GBA
Ks_A
Ks_A
2:1
3. A decide llamar a B
4. GET key info
5. RETURN key info
6. KeyGen → K_{AB}
7. INVITE(B@op.com), VOUCHER, otra info
2.Arranque de GBA
Ks_B
Ks_B
2:1
8. SIP INVITE
9. GET key info
9:1
10. (Key_info_B)$_{KB}$
11. Generación de clave
12. 200 OK

Figura 4

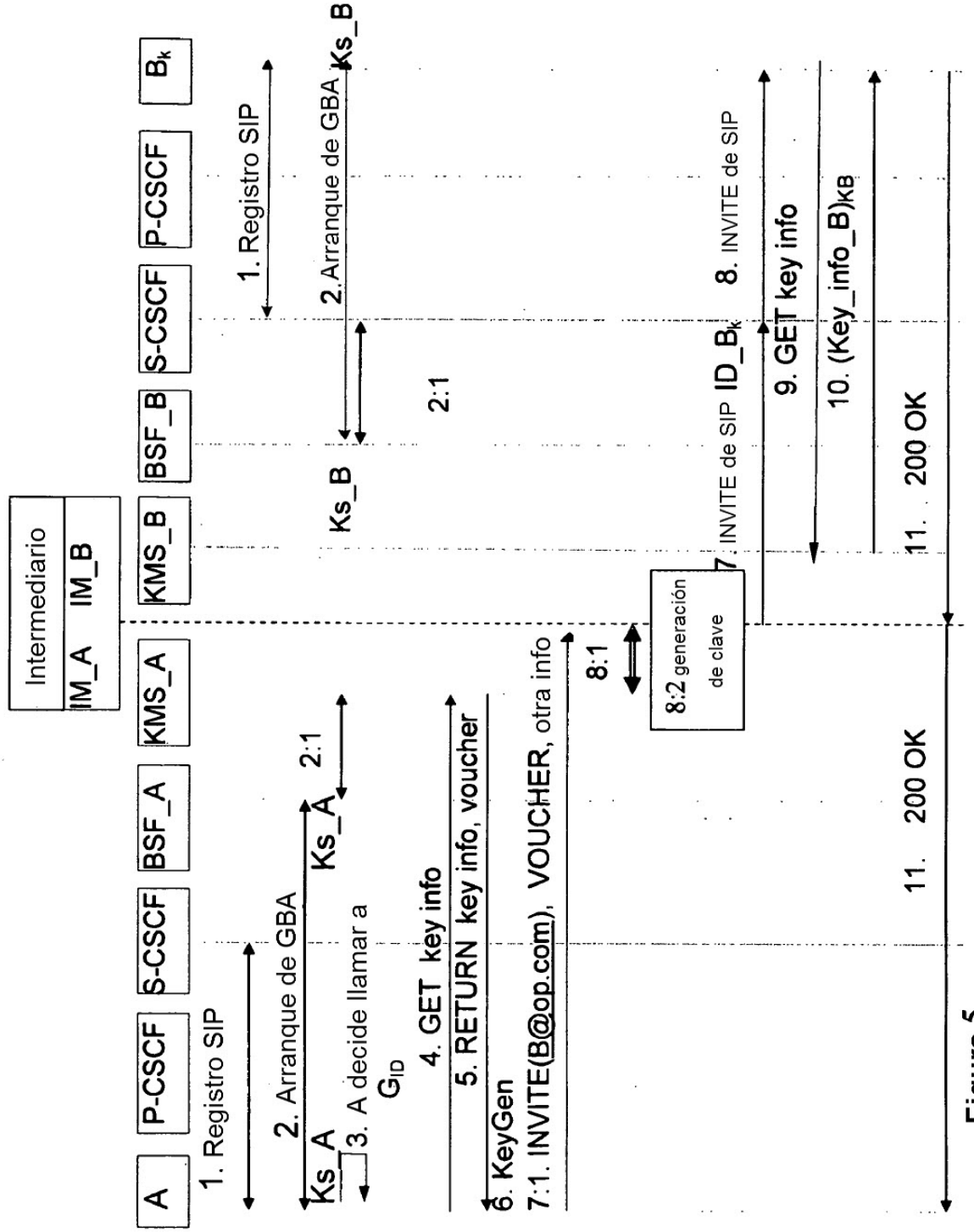
A
P-CSCF
S-CSCF
BSF_A
KMS_A
Intermediario
IM_A IM_B
KMS_B
BSF_B
S-CSCF
P-CSCF
Bk
1. Registro SIP
1. Registro SIP
2. Arranque de GBA
Ks_A
2:1
Ks_A
3. A decide llamar a
GID
2. Arranque de GBA
Ks_B
Ks_B
2:1
4. GET key info
5. RETURN key info, voucher
6. KeyGen
7:1. INVITE(B@op.com), VOUCHER, otra info
8:1
8:2 generación de clave
7. INVITE de SIP IDBk
8. INVITE de SIP
9. GET key info
10. (Key_info_B)KB
11. 200 OK
11. 200 OK

Figura 5

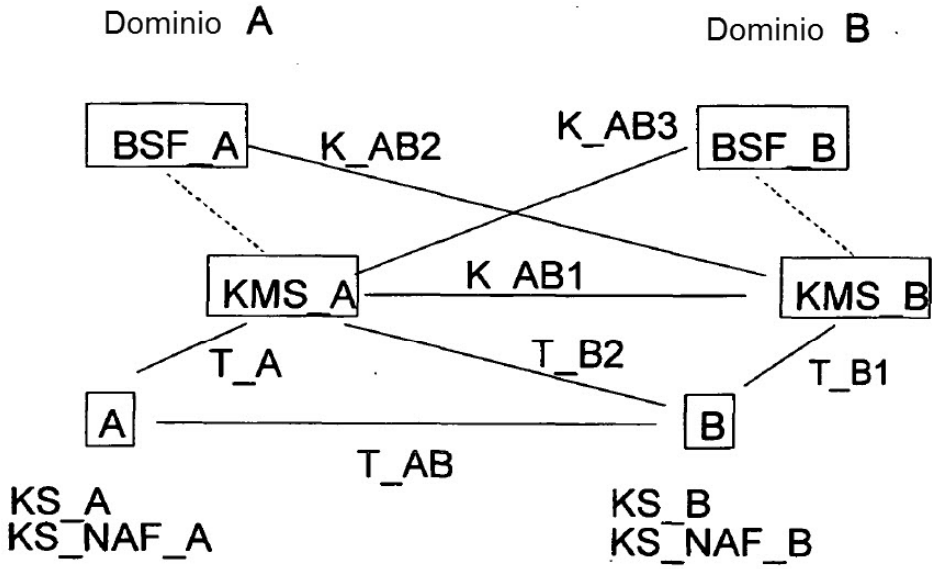
Dominio A
Dominio B
BSF_A
K_AB2
K_AB3
BSF_B
KMS_A
K_AB1
KMS_B
T_A
T_B2
T_B1
A
B
T_AB
KS_A
KS_NAF_A
KS_B
KS_NAF_B

Figura 6

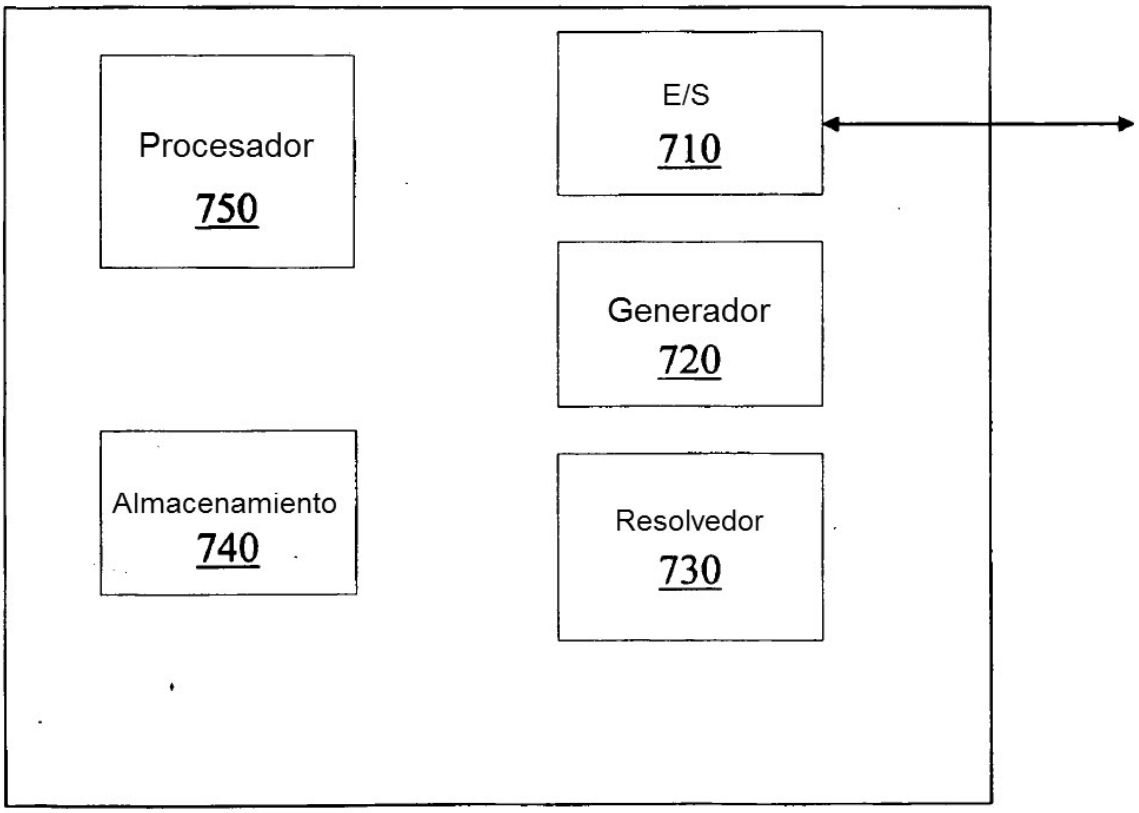
Procesador
750
E/S
710
Generador
720
Almacenamiento
740
Resolvedor
730

Figura 7