(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 424 119**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.08.2010 E 10748193 (9)**

(97) Fecha y número de publicación de la concesión europea: **17.07.2013 EP 2471211**

(54) Título: **Gestión segura de claves en sistema de conferencia**

(30) Prioridad:

28.08.2009 US 549907

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.09.2013

(73) Titular/es:

ALCATEL LUCENT (100.0%)
3, avenue Octave Gréard
75007 Paris, FR

(72) Inventor/es:

SUNDARAM, GANAPATHY S. y
CAKULEV, VIOLETA

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Gestión segura de claves en sistema de conferencia

Campo de la invención

La presente invención versa, en general, acerca de la seguridad de las comunicaciones y, más en particular, acerca de un protocolo seguro de gestión de claves para su uso en entornos de comunicaciones tales como un plano de medios de un sistema de comunicaciones multimedia y un sistema de llamadas de conferencia.

Antecedentes de la invención

Las aplicaciones multimedia existentes ofrecidas en un sistema de comunicaciones multimedia no soportan la seguridad en el plano de medios. La inquietud por la seguridad del plano de medios es un problema relativamente nuevo.

Las propuestas existentes en un sistema multimedia de comunicaciones tal como el subsistema multimedia de protocolo de Internet (IP) (IMS) se basan en algún tipo de procedimientos de claves simétricas basados en testigos, gestionados usando un servidor de gestión de claves que potencialmente crea y distribuye claves. El Informe Técnico (TR) 33.828 de 3GPP (Proyecto de Asociación de 3ª Generación), cuya divulgación se incorpora por referencia al presente documento, presenta propuestas existentes para el cifrado del plano de medios de IMS. Sin embargo, estas soluciones existentes no son susceptibles de un cambio de escala (dado que el servidor debería estar muy disponible y conectado todo el tiempo), no proporcionan la autenticación de entidades y, además, depositan las claves en el servidor.

En cambio, las aplicaciones no IMS como SKYPE (nombre comercial de Skype Technologies S.A., de Luxemburgo) y otras aplicaciones multimedia clientes no centralizadas proporcionan privacidad entre extremos con autenticación y sin depósito de claves. Sin embargo, la solución se vale del uso de certificados que requieren una infraestructura de clave pública (PKI) de alta disponibilidad que es sumamente cara de gestionar. Además, la solución no cambia bien de escala para aplicaciones de conferencia en grupos ni permite la interceptación legal de comunicaciones en ausencia de una PKI.

El documento titulado “Identity-based Fault-Tolerant Conference Key Agreement” (IEEE Transactions on dependable and secure computing, IEEE Service Center, Nueva York, EE. UU. (2004-03-01), páginas 170-178, XP011123191) da a conocer un acuerdo de claves basado en identidades construido sobre criptografía de curva elíptica. Es resistente a los diferentes ataques de clave provenientes de conferenciantes maliciosos y requiere pocos costes de comunicación.

Además, existen inquietudes similar de la seguridad en la gestión de claves en sistemas de conferencia en los que los partícipes participan en sesiones de llamadas a través de un servidor de conferencia.

Así, existe la necesidad de una solución de gestión segura de claves para su uso en entornos de comunicaciones tales como un plano de medios de un sistema multimedia de comunicaciones y un sistema de llamadas de conferencia.

Resumen de la invención

Los principios de la invención proporcionan uno o más protocolos seguros de gestión de claves para su uso en un entorno de comunicaciones como un sistema de conferencia.

Por ejemplo, en un aspecto, un procedimiento para la gestión de una conferencia entre dos o más partícipes en un sistema de comunicaciones comprende las siguientes etapas. Se lleva a cabo una operación de intercambio autenticado de claves basado en identidades entre un elemento de gestión de la conferencia del sistema de comunicaciones y cada uno de los dos o más partícipes que buscan participar en la conferencia, estando cifrados los mensajes intercambiados entre el elemento de gestión de la conferencia y los dos o más partícipes en función de las respectivas identidades de los destinatarios de los mensajes, y recibiendo, además, el elemento de gestión de la conferencia, procedente de cada partícipe, durante la operación de autenticación de claves, un componente de clave aleatoria que se calcula en función de un número aleatorio seleccionado por el partícipe.

El elemento de gestión de la conferencia envía a cada partícipe un conjunto que comprende los componentes de clave aleatoria calculados por los partícipes. El elemento de gestión de la conferencia recibe de cada partícipe un componente de clave aleatoria de grupo, siendo calculado el componente de clave aleatoria de grupo por cada partícipe mediante un cálculo en función del número aleatorio usado por el partícipe durante la operación de autenticación de claves y los componentes de clave aleatoria calculados por un subconjunto de otros partícipes de los dos o más partícipes que buscan participar en la conferencia.

El elemento de gestión de la conferencia envía a cada partícipe un conjunto que comprende los componentes de clave aleatoria de grupo calculados por los partícipes de tal modo que cada partícipe pueda calcular la misma clave

de grupo para su uso en la comunicación con cada uno de los demás partícipes por medio del elemento de gestión de la conferencia.

En una realización, el elemento de gestión de la conferencia no es un partícipe participante en la conferencia y, por ello, es incapaz de calcular la clave de grupo. En otra realización, el elemento de gestión de la conferencia es un partícipe participante en la llamada de conferencia y, por ello, es capaz de calcular la clave de grupo.

En una realización, la clave de grupo calculada por cada partícipe se representa como $Na_i(Z_{i-1}) + (N-1)X_i + (N-2)X_{i+1} + \ldots + X_{i-2}$, representando N el número total de partícipes que buscan participar en la conferencia, representando a_i el número aleatorio seleccionado por el partícipe dado, representando Z_i el componente de clave aleatoria calculado por el partícipe dado, representando X_i el componente de clave aleatoria de grupo calculado por el partícipe dado, y representando i un número de ordenación de la conferencia para el partícipe dado en la conferencia de N partícipes, siendo i-1=N cuando i=1 e i+1=1 cuando i=N.

En una realización, el componente de clave aleatoria para un partícipe dado se calcula mediante un cálculo representado como a_iP, siendo a_i el número aleatorio seleccionado por el partícipe dado y siendo P un punto seleccionado de un grupo asociado con la operación de autenticación de claves basada en el cifrado de identidades.

En una realización, el componente de clave aleatoria de grupo para un partícipe dado se calcula mediante un cálculo representado como $a_i(a_{i+1}P - a_{i-1}P)$, siendo a_i el número aleatorio seleccionado por el partícipe dado, siendo $a_{i+1}P$ el componente de clave aleatoria enviado al elemento de gestión de la conferencia por el partícipe que sigue inmediatamente al partícipe dado en la ordenación de la conferencia, siendo $a_{i-1}P$ el componente de clave aleatoria enviado al elemento de gestión de la conferencia por el partícipe que precede inmediatamente al partícipe dado en la ordenación de la conferencia y siendo P un punto seleccionado de un grupo asociado con un protocolo de intercambio de claves criptográficas.

Debe apreciarse que aunque los principios de la invención son particularmente adecuados a un entorno de un subsistema multimedia de protocolo de Internet (IP) (IMS), no se pretende que la invención esté limitada de ese modo. Es decir, los principios de la invención son generalmente aplicables a cualquier sistema adecuado de comunicaciones en el que sea deseable proporcionar características de gestión segura de claves.

Estos y otros objetos, características y ventajas de la presente invención se harán evidentes a partir de la siguiente descripción detallada de realizaciones ilustrativas de la misma, que ha de leerse en conexión con los dibujos adjuntos.

Breve descripción de los dibujos

La FIG. 1A ilustra una metodología de adquisición de claves privadas según una realización de la invención;
la FIG. 1B ilustra una metodología de intercambio de claves autenticadas basado en identidades según una realización de la invención;
la FIG. 2 ilustra una metodología de ramificación de claves según una realización de la invención;
la FIG. 3 ilustra una metodología de redireccionamiento de llamadas según una realización de la invención;
la FIG. 4A ilustra una metodología de entrega diferida según una realización de la invención;
la FIG. 4B ilustra una metodología de entrega diferida según otra realización de la invención;
la FIG. 5 ilustra una metodología de interceptación legal según una realización de la invención;
la FIG. 6A ilustra una metodología de gestión de la conferencia según una realización de la invención;
la FIG. 6B ilustra la adición de un participante en una metodología de gestión de la conferencia según una realización de la invención;
la FIG. 6C ilustra la salida de un participante en una metodología de gestión de la conferencia según una realización de la invención;
la FIG. 7 ilustra una arquitectura de red para un protocolo seguro de gestión de claves según una realización de la invención basada en IMS;
la FIG. 8 ilustra una metodología de ramificación de claves según una realización de la invención basada en IMS;
la FIG. 9 ilustra una metodología de redireccionamiento según una realización de la invención basada en IMS;
la FIG. 10 ilustra una metodología de conferencia con tres participantes según una realización de la invención basada en IMS; y
la FIG. 11 ilustra una arquitectura genérica de soporte físico de una red de datos y de dispositivos de comunicaciones (cálculo) adecuada para implementar uno o más de los protocolos según realizaciones de la presente invención.

Descripción detallada de realizaciones preferentes

Según se usa en el presente documento, la expresión “sistema multimedia de comunicaciones” se define en general como cualquier sistema de comunicaciones capaz de transportar dos o más tipos de medios que implican, pero sin limitación, datos a base de texto, datos a base de gráficos, datos a base de voz y datos a base de vídeo.

Según se usa en el presente documento, la expresión “plano de medios” se define en general como la porción funcional del sistema multimedia de comunicaciones según el cual se intercambian los uno o más tipos de medios entre dos o más partícipes en una sesión de llamadas. Esto se contrapone a “plano de control”, que es la porción funcional del sistema multimedia de comunicaciones según el cual se lleva a cabo la negociación/programación de llamadas para establecer la sesión de llamadas. Ejemplos de aplicaciones del plano de medios con los que pueden usarse las técnicas de la invención incluyen, sin limitación, la voz sobre IP (VoIP), la mensajería instantánea (IM), la IM de vídeo/audio y la compartición de vídeo. Se entiende que el plano de medios contiene tráfico de la capa de aplicaciones.

Según se usa en el presente documento, el término “clave” se define en general como un parámetro de entrada en un protocolo criptográfico con fines, sin limitación, como la autenticación de entidades, la privacidad, la integridad de mensajes, etc.

Para facilitar la referencia, la descripción detallada se divide como sigue. La sección I describe principios generales del cifrado basado en identidades y de operaciones de intercambio autenticado de claves basado en identidades. La sección II describe soluciones seguras de gestión de claves según principios ilustrativos de la invención en un contexto de un entorno general de comunicaciones. La sección III describe soluciones seguras de gestión de claves según principios ilustrativos de la invención en un contexto de un entorno de un subsistema multimedia de protocolo de Internet (IP) (IMS). La sección IV describe un sistema ilustrativo de cálculo para implementar uno o más protocolos seguros de gestión de claves según la invención.

I. El cifrado basado en identidades (IBE) y el intercambio autenticado de claves basado en identidades (IBAKE)

Antes de una explicación de realizaciones ilustrativas de la invención de técnicas seguras de gestión de claves, se proporcionan principios generales de IBE y de IBAKE.

A. Cifrado basado en identidades

Boneh y Franklin presentaron un protocolo de cifrado basado en identidades (IBE) (véase Dan Boneh, Matthew K. Franklin, “Identity-Based Encryption from the Weil Pairing” Advances in Cryptology - Proceedings of CRYPTO 2001 (2001), cuya divulgación se incorpora por referencia al presente documento). Este protocolo de cifrado criptográfico asimétrico permite que los participantes usen una “identidad” (por ejemplo: una identidad de correo electrónico o un nombre de dominio) como clave pública y elimina la necesidad de una estructura a gran escala de clave pública, que a menudo se asocia con procedimientos de cifrado de clave pública como el RSA (Rivest, Shamir y Adleman). El enfoque al problema dado por Boneh y Franklin usa mapas bilineales sobre una curva elíptica en un campo finito y recurre al problema de Diffie-Hellman bilineal de toma de decisiones.

El IBE implica las siguientes herramientas y los siguientes parámetros matemáticos:

Sea E una curva elíptica sobre un campo finito F, y sea P un punto de orden primo grande.
Sea E x E - → G un mapa bilineal en E. El ejemplo típico es el emparejamiento de Weil, y, por ende, G será el grupo de raíces enésimas de unidad, siendo n una función del número de puntos en E sobre F.
Sea s un entero positivo distinto de cero y sea a un secreto guardado en una función de generación de claves (KGF). Este es un secreto de todo el sistema y no se revela fuera de la KGF.
Sea P_{pub} = sP la clave pública del sistema que es conocida a todos los participantes. Recuérdese que sP denota un punto en E, dado que E es un grupo.
Sea H_1 una función de clave calculada conocida que toma una cadena y la asigna a un punto en la curva elíptica; es decir $H_1(A) = Q_A$ en E —siendo A habitualmente la identidad—, y también es la clave pública de A.
Sea $d_A = sQ_A$ la clave privada calculada por la KGF y entregada únicamente a A.
Sea H_2 una función de clave calculada conocida que toma un elemento de G y lo asigna a una cadena.
Sea m un mensaje que tiene que ser cifrado y enviado a A. La función de cifrado descrita por Boneh y Franklin es la siguiente:

Sea $g_A = e(Q_A, P_{pub})$, y sea r un número aleatorio.

$Cifrado_A(m) = (rP, m \text{ xor } H_2(g_A^r))$; en otras palabras, la salida del cifrado de m tiene dos coordenadas u y v, siendo u = rP y $v = m \text{ xor } H_2(g_A^r)$. Obsérvese que “xor” se refiere a la función lógica O exclusiva.

Para descifrar (u, v), A recupera m usando la siguiente fórmula:

$$m = v \text{ xor } H_2\left(e\left(d_A, u\right)\right).$$

La prueba de la fórmula es un ejercicio sencillo de mapas bilineales, y el hecho de que A tiene el secreto d_A (clave privada conocida solo para A, pero no para otros participantes). Obsérvese también que la KGF que calculó d_A en primer lugar también puede descifrar el mensaje, dando como resultado que la KGF sea de hecho un servidor de depósito de claves.

B. Intercambio autenticado de claves basado en identidades

Se describe el intercambio autenticado de claves basado en identidades (IBAKE) en la solicitud de patente estadounidense identificada por el nº de serie 12/372.242, presentada el 17 de febrero de 2009, cuya divulgación se incorpora por referencia al presente documento. El protocolo IBAKE permite que los dispositivos se autentiquen mutuamente entre sí y que deriven una clave que proporciona una perfecta confidencialidad a la ida y a la vuelta.

En la realización IBAKE aquí descrita, la configuración básica para este protocolo implica las estructuras y los parámetros matemáticos presentados más arriba en la subsección A. Recuérdese que este protocolo es asimétrico, pero no requiere ningún soporte de PKI; en vez de ello, el protocolo emplea un servidor autónomo que hace la función de generación de claves. A continuación se esbozan los detalles del protocolo:

Supongamos que A, B son las dos entidades (o partícipes, representando A un sistema de ordenadores de un primer partícipe y representando B un sistema de ordenadores de un segundo interlocutor) que intentan autenticarse y que acuerdan una clave.

Usaremos A y B para representar sus correspondientes identidades, que, por definición, también representan sus claves públicas.

Sean $H_1(A)=Q_A$ y $H_1(B)=Q_B$ los respectivos puntos en la curva elíptica correspondientes a las claves públicas. De hecho, también podríamos referirnos a Q_A y Q_B como claves públicas, dado que existe una correspondencia biunívoca entre las identidades y los puntos de la curva obtenidos aplicando H_1.

Sea x un número aleatorio escogido por A, y sea y un número aleatorio escogido por B.

Los intercambios de protocolo entre A y B comprenden las siguientes etapas:

A calcula xP (es decir, P sumada a sí misma x veces como un punto sobre E, usando la ley de aditiva sobre E), lo cifra usando la clave pública de B y lo transmite a B en una primera etapa. En esta etapa, el cifrado se refiere al cifrado basado en identidades descrito anteriormente en la subsección A.

Tras la recepción del mensaje cifrado, B descifra el mensaje y obtiene xP. Subsiguientemente, B calcula yP y cifra el par {xP, yP} usando la clave pública de A y luego lo transmite a A en una segunda etapa.

Tras la recepción de este mensaje, A descifra el mensaje y obtiene yP. Subsiguientemente, A cifra yP usando la clave pública de B y lo devuelve a B en una tercera etapa.

Tras esto, tanto A como B calculan xyP como clave de la sesión.

Obsérvese que A escogió x al azar y que recibió yP en la segunda etapa del intercambio de protocolo. Esto permite que A calcule xyP sumando yP consigo mismo x veces. Por su parte, B escogió y al azar y recibió xP en la primera etapa del intercambio de protocolo. Esto permite que B calcule xyP sumando xP consigo mismo y veces. Obsérvese que cualquier aplicación del protocolo puede utilizar datos de cabecera con identidades para garantizar el debido funcionamiento del protocolo. Esto es relativamente estándar y aplicable a casi cualquier intercambio de protocolo para el acuerdo de claves.

Obsérvese también que x es aleatorio, pero que xP no proporciona información alguna sobre x. Por lo tanto, xP es un componente de una clave basado en un secreto aleatorio escogido por A. Asimismo, y es aleatorio pero yP no proporciona información alguna sobre y. De ahí que yP sea un componente de una clave basado en un secreto aleatorio conocido únicamente por B.

Obsérvese además que xyP puede servir de clave de la sesión. Además, la clave de la sesión podría ser cualquier función conocida de xyP. Es decir, la clave de la sesión podría ser igual a f(xyP), siendo f conocida a ambos partícipes y no requiriéndose que sea secreta (es decir, es conocida al mundo). Un requisito práctico de f debería ser que f sea difícil de calcular sin conocimiento de x o y, y que el resultado sea de longitud satisfactoria desde una perspectiva criptográfica; por ejemplo, de aproximadamente 128 bits o más.

Algunas de las propiedades del protocolo IBAKE incluyen:

– Inmunidad al depósito de claves: Obsérvese que todas las etapas en el intercambio de protocolo están cifradas usando IBE. Por ello, está claro que la KGF puede descifrar todos los intercambios. Sin embargo, la KGF no puede calcular la clave de la sesión. Esto es debido a la dificultad del problema de la curva elíptica de Diffie-Hellman. En otras palabras, dados xP e yP, es difícil de realizar el cálculo de xyP.

– Acuerdo de claves mutuamente autenticado: Obsérvese que todas las etapas del intercambio de protocolo están cifradas usando IBE. En particular, solo B puede descifrar el contenido del mensaje enviado por A en las etapas primera y tercera y, asimismo, solo A puede descifrar el contenido del mensaje enviado por B en la segunda etapa. Además, al final de la segunda etapa, A puede verificar la autenticidad de B, dado que xP pudo haber sido enviado en la segunda etapa únicamente después del desciframiento del contenido de la primera etapa por parte de B. Asimismo, al final de la tercera etapa, B puede verificar la autenticidad de A, dado que yP pudo haber sido devuelto en la tercera etapa únicamente después de descifrar correctamente el contenido de la segunda etapa y esto solo es posible por parte de A. Por último, tanto A como B pueden acordar la misma clave de sesión. En otras palabras, el protocolo es un protocolo de acuerdo de claves de autenticación mutua basado en IBE. Aunque la descripción anterior proporciona la motivación de la seguridad del protocolo, puede proporcionarse fácilmente una prueba criptográfica de la segunda. La dificultad del protocolo se vale de la dificultad del problema de la curva elíptica de Diffie-Hellman, que está influenciada por la elección de la curva elíptica.
– Perfecta confidencialidad en la ida y en la vuelta: Dado que x e y son aleatorios, xyP es siempre nuevo y no tiene ninguna relación con ninguna sesión pasada ni futura entre A y B.
– Ausencia de contraseñas: El protocolo IBAKE no requiere ningún intercambio fuera de línea de contraseñas ni claves secretas entre A y B. De hecho, el procedimiento es claramente aplicable a dos partícipes cualesquiera que se comuniquen por vez primera a través de cualquier red de comunicaciones. El único requisito es garantizar que tanto A como B sean conscientes de la clave pública del otro; por ejemplo, a través de un servicio de directorio.

II. Gestión segura de claves y extensiones ilustrativas

Se ha constatado que Internet ha evolucionado rápidamente de ser una red de datos de esfuerzo razonable a convertirse en una red IP (protocolo de Internet) multiservicio con soporte para diversas clases de tráfico, incluido el multimedia. Esto, unido al rápido crecimiento de las redes inalámbricas móviles, ha creado retos tecnológicos. Desde la perspectiva de la tecnología, un reto medular que se ha abordado razonablemente bien es la separación de las funciones de control de la llamada, consistentes en señalización para establecer llamadas a partir de tráfico de la capa de aplicaciones a menudo denominado “plano de medios”. Los protocolos de control de llamadas como el H323 (véase, por ejemplo, la Recomendación H.323 de la Sección de Estandarización de la Unión Internacional de Comunicaciones (ITU-T), cuya divulgación se incorpora por referencia al presente documento), el protocolo de inicio de sesiones o SIP (véase, por ejemplo, la IETF RFC 3261 del Grupo de Trabajo de Ingeniería en Internet, cuya divulgación se incorpora por referencia al presente documento) y el IMS (véanse, por ejemplo, las especificaciones técnicas del 3GPP TS 23.218, TS 23.228, TS 24.228, TS 24.229 y TS 24.930, cuyas divulgaciones se incorporan por referencia al presente documento) han sido estandarizados por diversas organizaciones como la IETF y el 3GPP y están en diversas fases de adopción en redes fijas y móviles.

Simultáneamente, se han incorporado mecanismos elaborados para garantizar la señalización en diversos niveles. Sin embargo, en el plano de medios, aunque protocolos como la seguridad de la capa de transporte o TLS (véase, por ejemplo, la IETF RFC 2246, cuya divulgación se incorpora por referencia al presente documento), el protocolo seguro de transporte en tiempo real o SRTP (véase, por ejemplo, la IETF RFC 3711, cuya divulgación se incorpora por referencia al presente documento), y las extensiones multifuncionales seguras de correo en Internet o SMIME (véase, por ejemplo, la IETF RFC 2633, cuya divulgación se incorpora por referencia al presente documento) proporcionan formatos de contenedor para diversas aplicaciones, las soluciones de seguridad en el plano de medios carecen de procedimientos coherentes y estandarizados para soportar una gestión de claves entre extremos en la capa de aplicaciones.

Los principios de la invención abordan fundamentalmente este tema. En particular, los principios de la invención proporcionan una aplicación escalable y un marco de gestión segura de claves agnóstico de los protocolos para el plano de medios. En un marco ilustrativo, las soluciones de la invención utilizan el protocolo asimétrico (por ende, de clave pública) de intercambio autenticado de claves basado en identidades (IBAKE) descrito en lo que antecede en la sección I.B. Las realizaciones ilustrativas describen mecanismos de intercambio de claves para soportar diversas características como, por ejemplo, aplicaciones de comunicaciones seguras en el plano de medios entre dos partícipes, conferencia segura entre partícipes múltiples, ramificación segura de llamadas, desvío seguro de llamadas y de entrega segura diferida. Además de proporcionar un marco escalable para la gestión segura de claves, algunos aspectos ejemplares del diseño y el marco incluyen:

– El uso de servidores de gestión de claves (KMS) autónomos que reducen muchísimo la complejidad del soporte de red requerido. Recuérdese que los protocolos asimétricos en un entorno de claves públicas siempre requieren un soporte elaborado de una infraestructura de claves públicas (PKI) para la gestión de certificados, incluida su revocación. Los servidores de gestión de claves basados en claves simétricas son, por definición, servidores que están “siempre conectados”, con sincronización y actualizaciones constantes. Al eliminar el requisito de estar “siempre conectados”, el marco de los presentes inventores reduce muchísimo los costes y asiste a la escalabilidad.
– La eliminación de cualquier depósito pasivo de claves, que es inherente en los protocolos basados en identidades. Recuérdese que los protocolos de claves simétricas con un servidor de gestión de claves no

pueden eliminar este problema. Recuérdese también que los protocolos existentes de cifrado basado en identidades (descrito en lo que antecede en la sección I.A.) adolecen de problemas de depósito de claves, un problema que se resuelve usando IBAKE (descrito en lo que antecede en la sección I.B.).

– El marco del protocolo soporta inherentemente la autenticación mutua de las entidades implicadas en el intercambio de claves, unido a una perfecta confidencialidad.
– Las realizaciones ilustrativas de la invención reutilizan arquitecturas existentes de elementos de red y, en la medida de lo posible, reutilizan formatos existentes de contenedores de protocolos. Por ejemplo, en aplicaciones de conferencia, las realizaciones ilustrativas reutilizan el servidor de conferencia para permitir la conferencia, pero garantizan que el servidor de conferencia no averigüe la clave de grupo usada para la comunicación (a no ser que también sea un partícipe de la conferencia, tal como se explicará en lo que sigue).
– Aunque los principios de la invención eliminan el depósito pasivo de claves, los protocolos de la invención también proporcionan un soporte impecable para descubrir claves cuando hay un requisito legal de interceptar llamadas por parte de las fuerzas de aplicación de la ley.

En realizaciones ilustrativas basadas en un marco criptográfico asimétrico basado en identidades, cada participante tiene una clave pública y una clave privada. La clave pública está basada en la identidad. La clave privada corresponde a la clave pública y es emitida por un servidor o un servicio de gestión de claves (KMS). Los participantes pueden obtener claves privadas del KMS de forma autónoma. Únicamente a título de ejemplo, los participantes se ponen en contacto con su KMS una vez al mes (más en general, durante el transcurso de un abono) para obtener claves privadas. Las claves privadas también puede ser obtenidas en función de la frecuencia de uso. Se da por sentado que existe una asociación de seguridad entre el KMS y el participante. El cifrado y el desciframiento de los mensajes durante el intercambio de claves se basan en IBE. Obsérvese que se da por sentado que los parámetros públicos del KMS están a disposición del público (por ejemplo, en línea en un sitio de la red mundial).

En general, una metodología segura de gestión de claves según una realización ilustrativa de la invención comprende dos etapas principales. En una primera etapa, los participantes (partícipes) obtienen claves privadas de un servicio de claves como un KMS. En la segunda etapa, se lleva a cabo un intercambio autenticado de claves basado en identidades entre dos o más partícipes que buscan comunicarse en una sesión de llamadas a base de multimedia. Los mensajes intercambiados entre los dos o más partícipes se cifran en función de las respectivas identidades de los destinatarios del mensaje. Además, los mensajes cifrados intercambiados entre los partícipes contienen identidades asociadas con los partícipes.

La FIG. 1A muestra la primera etapa de la metodología segura de gestión de claves, es decir, la adquisición de la clave privada. Según se muestra, cada uno de los dispositivos 102 de comunicaciones (más en general, dispositivos de cálculo) de dos partícipes solicita y obtiene claves privadas (o secretas) de un respectivo KMS 104. El intercambio 106 de claves privadas se lleva a cabo según un protocolo seguro de comunicaciones. Ejemplos de protocolo seguro de comunicaciones incluyen, sin limitaciones, la seguridad del protocolo de Internet o IPSec (véanse, por ejemplo, IETF RFC 2406, IETF RFC 2409, IETF RFC 4306 e IETF RFC 4308, cuyas divulgaciones se incorporan por referencia al presente documento) y la seguridad de la capa de transporte o TLS (véase, por ejemplo, la IETF RFC 2246, cuya divulgación se incorpora por referencia al presente documento). Puede usarse la arquitectura genérica de arranque o GBA (véase, por ejemplo, la memoria técnica (TS) 33.220 de 3GPP, cuya divulgación se incorpora por referencia al presente documento) para determinar una clave para usarla en el protocolo seguro de comunicaciones entre cada partícipe y el KMS. En un ejemplo, se podría tener una aplicación ejecutándose en el dispositivo cliente que se conecta con el servidor KMS y usa TLS en la capa de aplicaciones (por encima del protocolo de control de transporte o TCP; véanse, por ejemplo, W. Richard Stevens. TCP/IP Illustrated, Tomo 1: The Protocols, ISBN 0-201-63346-9; W. Richard Stevens y Gary R. Wright. TCP/IP Illustrated, Tomo 2: The Implementation, ISBN 0-201-63354-X; W. Richard Stevens. TCP/IP Illustrated, Tomo 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols, ISBN 0-201-63495-3, cuyas divulgaciones se incorporan por referencia al presente documento), que usa la clave GBA o IPSec en la capa de red con la clave GBA como clave compartida de antemano.

Obsérvese que se considera que el dispositivo de la izquierda es el iniciador (I) y que el de la derecha es el contestador (R). Esta designación proviene del hecho de que el dispositivo de la izquierda busca iniciar una sesión de llamadas multimedia con el dispositivo de la derecha.

Según se muestra, cada dispositivo proporciona un identificador con su petición al KMS, a la que el KSM responde con una clave privada (secreta). En el caso del dispositivo iniciador 102-1, se proporciona un identificador al KMS 104-I, y, como respuesta, se proporciona al dispositivo una clave privada I-SK. En el caso del dispositivo contestador 102-R, se envían dos identificador separados al KMS 104-R, concretamente R y R1. Como respuesta, el KMS proporciona al partícipe que responde dos claves privadas, R_SK y R1_SK. Por supuesto, cada partícipe puede solicitar y obtener más o menos claves privadas en función de alguna programación de adquisición de claves privadas. Esta puede ser una programación en función del tiempo (por ejemplo, un periodo de un mes), una programación basada en la frecuencia de las sesiones (por ejemplo, cuando hace falta para realizar una llamada) y una programación basada en un abono (por ejemplo, el partícipe se abona al servicio de claves del KMS durante algún tiempo o en función de una incidencia de una condición de fin del abono).

Además, ha de apreciarse que un partícipe dado pueda tener múltiples identidades públicas. Por ejemplo, el partícipe B ("Roberto") puede tener dos identidades: roberto@trabajo.com y roberto@casa.com. Para estas dos identidades, puede haber dos claves públicas diferentes y, así, dos claves privadas diferentes.

La FIG. 1B muestra la segunda etapa de la metodología segura de gestión de claves, es decir, el intercambio autenticado de claves. En esta realización, el intercambio autenticado de claves se basa en IBAKE (descrito en lo que antecede en la sección I.B.). Dado que el formato preferido del intercambio de mensajes entre el primer partícipe y el segundo partícipe se basa en un formato de codificación multimedia en Internet (MIKEY), el protocolo global seguro de intercambio de claves de las FIGURAS 1A y 1B es denominado protocolo MIKEY-IBAKE en el presente documento.

De nuevo, se da por sentado que el dispositivo de la izquierda es el partícipe que inicia o iniciador, 102-I, y que el dispositivo de la derecha es el partícipe que responde o contestador, 102-R. Las etapas del intercambio autenticado de claves siguen etapas similares a las del protocolo IBAKE.

Se da por sentado que la clave pública I_PK del iniciador se calcula usando una función de clave calculada según se describa más arriba en la sección I. Asimismo, la clave pública R_PK del contestador se calcula de forma similar. Recuérdese que las claves privadas del iniciador y el contestador son I_SK y R_SK, respectivamente. Es decir, sean H_1(Initiator_ID)=I_PK y H_1(Responder_ID) =R_PK los respectivos puntos de la curva elíptica correspondientes a las claves públicas.

Sea *a* un número aleatorio escogido por el iniciador 102-I, y sea *b* un número aleatorio escogido por el contestador 102-R.

Los intercambios de protocolo entre 102-I y 102-R comprenden las etapas siguientes:

> El iniciador 102-I calcula un primer componente de clave aleatoria *a*P (es decir, P sumada a sí misma *a* veces como un punto en E, usando la ley aditiva en E), cifra el primer componente de clave aleatoria usando la clave pública (R_PK) del contestador y lo transmite al contestador 102-R en la etapa 110. En esta etapa, cifrado se refiere al cifrado basado en identidades descrito en la anterior subsección I.A. Obsérvese que también están incluidas en el mensaje cifrado en la etapa 110 las identidades del iniciador y del contestador (I_ID y R_ID, respectivamente).

Tras la recepción del mensaje cifrado, el contestador descifra el mensaje usando su clave privada (obtenida en la FIG. 1A) y obtiene *a*P. Subsiguientemente, el respondendor calcula un segundo componente de clave aleatoria *b*P, y cifra el par {*a*P, *b*P} usando la clave pública del iniciador y luego transmite el par al iniciador en la etapa 112. De nuevo, el mensaje cifrado de la etapa 112 incluye la identidades del iniciador y del contestador (I_ID y R_ID, respectivamente).

En la etapa 116, el contestador envía un mensaje de verificación al iniciador cifrado usando la clave pública del iniciador.

Tras esto, tanto el iniciador como el contestador calculan *ab*P como la clave segura de la sesión de llamadas que ha usarse para la comunicación segura entre sí durante la sesión de llamadas a través del plano de medios (capa de aplicaciones) de sistema multimedia de comunicaciones.

Obsérvese que el iniciador 102-I escogió *a* de forma aleatoria, y que recibió *b*P en la segunda etapa del intercambio de protocolo. Esto permite que el iniciador calcule *ab*P sumando *b*P consigo mismo *a* veces. Por su parte, el contestador 102-R escogió *b* de forma aleatoria, y recibió *a*P en la primera etapa del intercambio de protocolo. Esto permite que el contestador calcule *ab*P sumando *a*P consigo mismo *b* veces. Obsérvese también que *a* es aleatoria, pero *a*P no proporciona información alguna sobre *a*. Por lo tanto, se considera que *a*P es un componente de una clave basado en un secreto aleatorio escogido por el iniciador. Asimismo, *b* es aleatorio, pero *b*P no proporciona información alguna sobre *b*. Por ende, se considera que *b*P es un componente de una clave basado en un secreto aleatorio escogido por el contestador.

Con referencia ahora a la FIG. 2, se ilustra una extensión del protocolo MIKEY-IBAKE. Ha de entenderse que, dado que esta es una extensión del protocolo MIKEY-IBAKE descrito en lo que antecede, no se repiten, en aras de la simplicidad, todas las características del protocolo MIKEY-IBAKE. En esta realización particular, la FIG. 2 ilustra la ramificación. La ramificación es la entrega de una petición a múltiples ubicaciones. Esto puede ocurrir, por ejemplo, cuando el contestador tenga más de un dispositivo de comunicaciones (cálculo) en el que pueda participar en una sesión de llamadas multimedia. Un ejemplo de ramificación es cuando un partícipe tiene un teléfono de sobremesa, un cliente de ordenador personal (PC) y un terminal móvil, todos configurados para participar en el protocolo MIKEY-IBAKE. En general, la ramificación es una característica de un protocolo de inicio de sesiones multimedia que permite que una llamada entrante suene simultáneamente en varias extensiones. El primer teléfono en responder tomará entonces el control de la llamada.

Así, según se representa en la FIG. 2, el partícipe que responde tiene dos dispositivos 102-R1 y 102-R2 asociados consigo. Así, según se muestra, el dispositivo 102-R1 tiene una clave pública R1_PK y una clave secreta R1_SK. Además, el dispositivo 102-R1 conoce las claves pública y privada, R_PK y R_SK, del partícipe que responde. Asimismo, el dispositivo 102-R2 tiene una clave pública R2_PK y una clave secreta R2_SK. Además, el dispositivo 102-R2 conoce las correspondientes claves pública y privada, R_PK y R_SK.

En el escenario de ramificación, las etapas 210, 212, 214 y 216 del protocolo MIKEY-IBAKE son esencialmente iguales a las etapas 110, 112, 114 y 116 del protocolo MIKEY-IBAKE en el contexto general de la FIG. 1B, con las siguientes excepciones. Obsérvese que, dado que el mensaje enviado por el dispositivo 102-I en la etapa 210 está cifrado con R_PK, tanto el dispositivo R1 como el R2 pueden descifrar el mensaje (dado que ambos tienen R_SK). Sin embargo, dando por sentado que el partícipe que responde esté asociado en ese momento con el dispositivo R2 y no con el dispositivo R1, el mensaje de retorno en la etapa 212 incluye el componente de clave aleatoria b2P, calculado por R2 según IBAKE (siendo b2 el número aleatorio seleccionado por R2). Además, el mensaje cifrado de la etapa 212 incluye las identidades del iniciador, del contestador y del dispositivo R2 (I_ID, R_ID y R2_ID, respectivamente).

El dispositivo 102-I descifra el mensaje recibido de R2 usando su clave privada para obtener el b2P y las identidades incluidas en al mensaje. El iniciador identifica así que el mensaje de la etapa 212 vino de R2. Según el protocolo MIKEY-IBAKE, el iniciador envía entonces un mensaje, en la etapa 214, que incluye b2P, I_ID y R2_ID. El mensaje se cifra usando la clave pública de R2. Obsérvese que esto no puede ser descifrado por R1, dado que R1 solo tiene R_SK y R1_SK, pero no R2_SK. La etapa 216 es el mensaje de verificación, similar a la etapa 116 de la FIG. 1B. La clave de la sesión de llamadas puede ser calculada entonces en el dispositivo 102-I y en el dispositivo 102-R2 como ab2P.

La FIG. 3 ilustra una extensión del protocolo MIKEY-IBAKE a una característica de reselección de destinatario. Ha de entenderse que, dado que esta es una extensión del protocolo MIKEY-IBAKE descrito en lo que antecede, no se repiten, en aras de la simplicidad, todas las características del protocolo MIKEY-IBAKE. La reselección de destinatario o redireccionamiento es un escenario en el que uno o más elementos funcionales en el sistema de comunicaciones deciden redirigir la llamada a un destino diferente. Esta decisión de redireccionamiento de una sesión puede tomarse por diferentes razones por varios elementos funcionales diferentes y en diferentes puntos en el establecimiento de la sesión. Esto también se denomina desvío de llamada.

El ejemplo de la FIG. 3 muestra un servidor 302 de aplicaciones tomando la decisión de redireccionamiento. En el escenario de la ramificación, las etapas 310, 312, 314 y 316 del protocolo MIKEY-IBAKE son esencialmente iguales que las etapas 110, 112, 114 y 116 del protocolo MIKEY-IBAKE en el contexto general de la FIG. 1B, con las siguientes excepciones.

El dispositivo 102-I envía el primer mensaje en el protocolo en la etapa 310 con la intención de que vaya al dispositivo 102-R1 (estando cifrado el mensaje con la clave pública de R1). Sin embargo, el elemento funcional 302 adoptó la decisión de que el mensaje en 310 fuera redirigido al dispositivo (véase la etapa 310′). Con anterioridad a ello, o en unión con ello, se da por sentado que R2 recibió la clave privada de R1 en un mensaje enviado en la etapa 308 a través del elemento funcional. El mensaje enviado desde R1 a R2 se cifra usando la clave pública de R2. Así, el elemento funcional 302 no puede descifrar el mensaje en 308, pero R2 puede descifrar el mensaje en 310′ y responder al iniciador en la etapa 312. A partir de este punto, las etapas 312, 314 y 316 son idénticas a las etapas 212, 214 y 216 en el escenario de ramificación de la FIG. 2.

La FIG. 4A muestra una extensión de entrega diferida del protocolo MIKEY-IBAKE. Ha de entenderse que, dado que esta es una extensión del protocolo MIKEY-IBAKE descrito en lo que antecede, no se repiten, en aras de la simplicidad, todas las características del protocolo MIKEY-IBAKE. La entrega diferida es un tipo de servicio tal que el contenido de la sesión no pueda ser entregado al destino en el momento en que se envía (por ejemplo, el usuario destinatario no está conectado en ese momento). No obstante, el remitente espera que la red entregue el mensaje tan pronto como el destinatario esté disponible. Un ejemplo de entrega diferida es el correo de voz.

En la FIG. 4A, supongamos que A es el dispositivo 102-I, que B es 102-R, que el dispositivo 402 es un elemento funcional tal como un servidor de aplicaciones y que MB es un buzón 102-MB (más en general, un destino temporal) asociado con B.

En la etapa 401, A envía a B un primer mensaje que comprende un primer componente cifrado (xP) de clave aleatoria. El primer componente de clave aleatoria se calculó en A, y el primer mensaje fue cifrado usando una clave pública de B. El elemento funcional 402 determina que B no está disponible y desvía el primer mensaje a MB en la etapa 402.

En la etapa 403, MB envía a A un segundo mensaje que comprende un segundo componente cifrado (yP) de clave aleatoria que calculó MB. El mensaje en la etapa 403 fue cifrado en MB usando una clave pública de A. En la etapa 404, el elemento funcional 402 envía el mensaje a A.

A descifra el mensaje de MB usando la clave privada obtenida por A del servicio de claves para obtener el segundo componente de clave aleatoria. A identifica que el mensaje recibido en la etapa 404 provino de MB (debido a que la identidad de MB está incluida en el mensaje).

En la etapa 405, A envía a MB un tercer mensaje (a través del elemento funcional en la etapa 406) que incluye un par de componentes cifrados de clave aleatoria, habiéndose formado el par de componentes de clave aleatoria a partir del primer componente (xP) de clave aleatoria y del segundo componente (yP) de clave aleatoria y habiéndose cifrado en A usando la clave pública de MB. Este tercer mensaje también incluye una clave secreta (sK) aleatoria cifrada calculada en A y cifrada en A usando la clave pública de B. MB da a A acuse de recibo a través de las etapas 407 y 408. MB no puede descifrar esa última parte del mensaje (dado que está cifrado usando la clave pública de B y MB no tiene la clave privada de B) y, así, no puede averiguar sK.

MB proporciona a B la clave secreta (sK) aleatoria cifrada, por petición de B, tras una operación mutua de autenticación entre B y MB. Esto se muestra en las etapas 409 y 410. Esta clave secreta es usada entonces por B para obtener el contenido (por ejemplo, el mensaje de voz) dejado por A en el buzón de B.

En una variación de la entrega diferida de la FIG. 4A representada en la FIG. 4B, supongamos que no se lleva a cabo un protocolo autenticado de acuerdo de clave, sino que, más bien, en el primer mensaje, A envía una clave secreta (sK) aleatoria cifrada, calculada en A y cifrada en A usando una clave pública de B (etapa 411). El elemento funcional 402, habiendo determinado que B no está disponible, remite el primer mensaje a MB (etapa 412), el cual l confirma (etapas 413 y 414). Después, B puede recuperar la clave secreta de MB de la misma manera que se ha descrito en lo que antecede (etapas 415 y 416).

La FIG. 5 muestra otra extensión del protocolo MIKEY-IBAKE. De nuevo, ha de entenderse que, dado que esta es una extensión del protocolo MIKEY-IBAKE descrito en lo que antecede, no se repiten, en aras de la simplicidad, todas las características del protocolo MIKEY-IBAKE. La extensión de la FIG. 5 está relacionada con el concepto de la interceptación legal de mensajes intercambiados en el sistema multimedia de comunicaciones. El concepto de interceptación legal se basa en una situación en la que una autoridad de aplicación de la ley precisa poder “escuchar” las comunicaciones de uno o más partícipes.

En un enfoque, la autoridad de aplicación de la ley puede simplemente obtener las claves privadas de 102-I y 102-R a través de una orden de registro y desempeñar un papel de “intermediario” activo durante el protocolo de acuerdo de claves y luego acceder al tráfico.

En otro enfoque, mostrado en la FIG. 5, un servidor 502 de las fuerzas de aplicación de la ley (servidor de LI) funciona con el KMS del iniciador (KMS_I) y con el KMS del contestador (KMS_R) para interceptar legalmente mensajes enviados entre el dispositivo 102-I y el dispositivo 102-R. Aunque la FIG. 5 muestra servidores separados para el servidor de LI, el KMS_I y el KMS_R, ha de apreciarse que puede usarse un elemento funcional (por ejemplo, un servidor de interceptaciones) en el sistema multimedia de comunicaciones para llevar a cabo las funciones de KMS y de interceptación.

En consecuencia, se lleva a cabo el protocolo MIKEY-IBAKE según se ha descrito en lo que antecede en el contexto de las FIGURAS 1A y 1B. Sin embargo, el servidor de LI imita al iniciador para los mensajes enviados al contestador e imita al contestador para los mensajes enviados al iniciador.

Por ejemplo, consideremos el flujo de mensajes cuando el servidor de LI imita al contestador. Supongamos que 102-I envía un primer mensaje que incluye un primer componente cifrado de clave aleatoria para la recepción prevista por parte de 102-R. El primer mensaje es interceptado por el servidor de LI. El servidor de LI calcula entonces un segundo componente de clave aleatoria y envía a 102-I un segundo mensaje que incluye un par de componentes cifrados de clave aleatoria. El par de componentes de clave aleatoria se forma a partir del primer componente de clave aleatoria y del segundo componente de clave aleatoria calculado en el servidor de LI. El segundo mensaje se cifra en el servidor de LI usando la clave pública de 102-I.

El segundo mensaje es descifrado usando la clave privada obtenida por 102-I del servicio de claves para obtener el segundo componente de clave aleatoria. El dispositivo 102-I envía entonces un tercer mensaje que incluye el segundo componente de clave aleatoria para la recepción prevista por parte de 102-R, pero que es interceptado por el servidor de LI. Así, el servidor de LI es capaz de calcular la misma clave segura que calcula el dispositivo 102-I.

Ha de entenderse que el servidor de LI también imita al iniciador (102-I) en el envío y la recepción de mensajes durante la operación autenticada del acuerdo de claves, de modo que el contestador (102-R) establezca una clave segura con el servidor de LI que el contestador cree que fue objeto de acuerdo por parte del iniciador (pero que, de hecho, fue objeto de cuerdo con el servidor de LI).

Ha de apreciarse que una o más de las características del protocolo MIKEY-IBAKE descritas en lo que antecede pueden extenderse a un escenario de un sistema de conferencia. Tal extensión está representada en las FIGURAS 6A a 6C.

La suposición general es que el servidor de conferencia (más en general, el elemento de gestión de la conferencia) que retransmite la comunicación de múltiples partícipes (por ejemplo, un puente de conferencia) no conoce la clave de grupo, mientras que todos los usuarios tienen acceso a la misma clave de grupo. Hay una excepción a esta premisa, concretamente en la conferencia entre dispositivos del mismo nivel, cuando el dispositivo de cálculo que hace de puente de conferencia es también un partícipe que participa de forma sustantiva en la conferencia.

Según se muestra en la FIG. 6A, se da por sentado que una conferencia 600 de múltiples partícipes incluye un servidor de conferencia y usuarios (partícipes) 1 a N, asignándose el número de usuario en el orden en que el usuario intenta incorporarse a la conferencia, es decir, secuencialmente, 1, 2, 3, … N.

En la etapa 602, cada usuario ejecuta individualmente el protocolo IBAKE con el servidor de conferencia. Sea $Z_i = a_iP$ el valor enviado por el usuario "I" al servidor de conferencia durante la autenticación con el servidor. Recuérdese que a_iP es el componente de clave aleatoria calculado por el partícipe según IBAKE.

Tras el éxito de la autenticación, en la etapa 604, el servidor de conferencia envía el conjunto $\{a_iP\}$ a todos los usuarios (ya sea por difusión o unidifusión individual). El conjunto $\{a_iP\}$ es, así, un conjunto que incluye los componentes de clave aleatoria calculados por cada uno de los partícipes.

En la etapa 606, cada usuario individualmente devuelve $X_i = a_i\{a_{i+1}P - a_{i-1}P\}$ al servidor de conferencia. Obsérvese que $a_i\{a_{i+1}P - a_{i-1}P\}$ es un componente de clave aleatoria de grupo, siendo calculado el componente de clave aleatoria de grupo por cada partícipe mediante un cálculo basado en el número aleatorio usado por el partícipe durante la operación de autenticación de claves y los componentes de clave aleatoria calculados por un subconjunto de otros partícipes de los dos o más partícipes que buscan participar en la conferencia. En esta realización, el componente de clave aleatoria de grupo para un partícipe dado $a_i\{a_{i+1}P - a_{i-1}P\}$ se calcula de tal modo que a_i sea el número aleatorio seleccionado por el partícipe dado, $a_{i+1}P$ sea el componente de clave aleatoria enviado al servidor por el partícipe que sigue inmediatamente al partícipe dado en la ordenación de la conferencia, $a_{i-1}P$ sea el componente de clave aleatoria enviado por el partícipe que precede inmediatamente al partícipe dado en la ordenación de la conferencia y P sea un punto seleccionado de un grupo asociado con la operación de autenticación de claves basada en el cifrado de identidades (por ejemplo, un punto seleccionado de una curva elíptica, según se ha descrito en lo que antecede).

En la etapa 608, el servidor de conferencia comparte entonces con todos el conjunto $\{X_i\}$ (ya sea por difusión o unidifusión individual). Es decir, el conjunto $\{X_i\}$ es un conjunto que incluye los componentes de clave aleatoria de grupo calculados por los partícipes.

En la etapa 610, cada partícipe puede calcular la misma clave de grupo para su uso en la comunicación con cada uno de los demás partícipes a través del servidor de conferencia. La clave de grupo se calcula como sigue: $Na_i(Z_{i-1}) + (N-1)X_i + (N-2)X_{i+1} + \ldots + X_{i-2}$, representando N el número total de partícipes que buscan participar en la conferencia, representando a_i el número aleatorio seleccionado por el partícipe dado, representando Z_i el componente de clave aleatoria calculado por el partícipe dado, representando X_i el componente de clave aleatoria de grupo calculado por el partícipe dado, y representando i un número de ordenación de la conferencia para el partícipe dado en la conferencia de N partícipes, siendo i-1=N cuando i=1 e i+1=1 cuando i=N.

Según se ha mencionado en lo que antecede, el servidor de conferencia no es un partícipe participante y, por ello, es incapaz de calcular la clave de grupo. Sin embargo, en un escenario de dispositivos del mismo nivel, el servidor de conferencia es un partícipe participante en la llamada de conferencia y, por ello, precisa ser capaz de calcular la clave de grupo.

Se entiende que el servidor de conferencia lleva a cabo una operación de autenticación mutua con cada partícipe que busca participar en la conferencia. Además, el servidor de conferencia solo admite a un partícipe dado en la conferencia cuando se satisfacen al menos dos condiciones: (i) el partícipe dado es autenticado por el elemento de gestión de la conferencia; y (ii) se confirma que el partícipe dado pertenece a una lista de autorización de la conferencia. Además, según el anterior protocolo MIKEY-IBAKE, los partícipes que buscan participar en la conferencia y el servidor de conferencia obtienen respectivas claves privadas de uno o más servicios de gestión de claves (KMS).

La FIG. 6B ilustra cómo se suma un nuevo participante en la conferencia (usuario N+1) a una conferencia en curso, resultando así en una conferencia modificada 600′.

En la etapa 612, el usuario N+1 ejecuta un IBAKE con el servidor de conferencia. Sea $Z_{N+1} = a_{N+1}P$ el valor enviado por el usuario "N+1" al servidor durante la autenticación con el servidor. Una vez que tiene éxito la autenticación del usuario N+1, en la etapa 614, el servidor de conferencia anuncia la admisión del nuevo usuario N+1 y envía a todos el conjunto $\{a_iP\}$ (ya sea por difusión o unidifusión individual), incluyendo a Z_{N+1}.

En la etapa 616, los usuarios 1, N, N+1 devuelven $X_i = a_i(a_{i+1}P - a_{i-1}P\}$ al servidor; alternativamente, todos ellos podrían ejecutar esta etapa. En la etapa 618, el servidor de conferencia comparte entonces con todos el conjunto $\{X_i\}$ (ya sea por difusión o unidifusión individual), incluyendo a X_{N+1}. Entonces vuelve a calcularse la clave de grupo

$(N+1)a_i(Z_{i-1}) + (N)X_i + (N-1)X_{i+1} + \ldots + X_{i-2}$ en la etapa 620. Obsérvese que la clave de grupo cambia después de que se admite al nuevo usuario

La FIG. 6C ilustra cómo sale de una conferencia en curso un participante, resultando así en una conferencia modificada 600″.

Supongamos que el usuario 3 abandona la llamada (ha de entenderse que la elección del usuario 3 es solo un ejemplo). En la etapa 622, el servidor de conferencia anuncia (ya sea por difusión o unidifusión individual) qué usuario abandonó la llamada. La ordenación de los usuarios cambia en la etapa 624. Los usuarios 1 y 2 siguen igual. El usuario i se convierte en el usuario i-1 para todas las i mayores o iguales que 4. En la etapa 626, el usuario 4 (que ahora es el usuario 3) recalcula X_i y comparte esta aportación con el servidor de conferencia. En la etapa 628, el servidor de conferencia comparte el conjunto $\{X_i\}$ con todos los participantes. En la etapa 630, los participantes recalculan la clave de grupo $(N-1)a_i(Z_{i-1}) + (N-2)X_i + (N-3)X_{i+1} + \ldots + X_{i-2}$. Obsérvese, de nuevo, que la clave de grupo cambia después de que un participante abandona la llamada.

Los principios de la invención también proporcionan una extensión a las técnicas de gestión de conferencia descritas en lo que antecede. La extensión implica la interceptación legal de mensajes de conferencia.

Supongamos que hay N participantes en el sistema de conferencia. Supongamos que el participante N es “sospechoso” y que las autoridades de aplicación de la ley han obtenido una orden de registro para acceder a las llamadas destinadas al participante N y procedentes del mismo. La elección de declarar sospechoso de delitos al participante N es solo para ilustrar y hace la descripción más fácil de seguir, y la solución de ninguna manera está limitada a declarar el usuario enésimo usuario sospechoso de delitos.

Antes de la llamada de conferencia, el servidor de LI (recuérdese la FIG. 5) se dirige al KMS correspondiente al participante N y obtiene la clave privada del participante N. Esto permitirá que el servidor de LI se haga pasar por el participante N durante el procedimiento de intercambio de la clave de grupo y ejecute todas las etapas de la FIG. 6A, salvo que las aportaciones del participante N son sustituidas con aportaciones del servidor de LI. En particular, el servidor de LI sustituirá Z_N y X_N con Z_{LI} y X_{LI}. El resto de los participantes de se percatará de la diferencia y calculará una clave de grupo, llamémosla GK′.

A continuación, el servidor de LI trabaja con el servidor de conferencia y sustituye Z_1 y X_1 con Z_{LI} y X_{LI} en todas las comunicaciones con el participante N. Esto implicará que el participante N calcule una clave de grupo diferente de GK′. Llamemos a esta nueva clave GK″.

Obsérvese que, en la etapa anterior, el servidor de LI podría haber sustituido Z_i y X_i con Z_{LI} y X_{LI} para cualquier participante, y la elección de i=1 es solo para la ilustración.

Después de que se establece la llamada, cualquier comunicación procedente de los participante 1 a N-1 será cifrada usando GK′. Dado que el servidor de LI conoce GK′, puede interceptar entonces la comunicación, descifrarla, tras lo cual volverá a cifrarla con GK″ y enviarla al participante N. Por su parte, cualquier comunicación procedente del participante N será cifrada usando GK″, la cual será interceptada por el servidor de LI server, luego descifrada usando GK″, cifrada nuevamente usando GK′ y enviada a los participantes 1 a N-1.

III. Realizaciones IMS

En la sección siguiente, se aplican los anteriores principios generales de MIKEY_IBAKE y sus extensiones a un entorno de un subsistema multimedia IP (IMS). Es decir, se considera que el sistema multimedia de comunicaciones de esta sección es una red IMS. Los estándares IMS se describen, por ejemplo, en las memorias técnicas TS 23.218, TS 23.228, TS 24.228, TS 24.229 y TS 24.930 de 3GPP, cuyas divulgaciones se incorporan por referencia al presente documento.

Describimos en primer lugar un marco arquitectónico para la seguridad del plano de medios IMS, específicamente la gestión de claves, basado en el cual pueden derivarse diversos casos de uso y diversas características.

En el centro de la solución se encuentra el concepto de cifrado basado en identidades (IBE), similar a las RFC 5091, RFC 5408 Y RFC 5409, cuyas divulgaciones se incorporan por referencia al presente documento.

Sin embargo, estas RFC no proporcionan autenticación y adolecen de un problema inherente de depósito de claves. Abordamos estos problemas extendiendo el IBE básico para que incluya el protocolo de intercambio autenticado de claves basado en identidades (IBAKE) que proporciona autenticación mutua, elimina el depósito pasivo de claves y proporciona perfecta confidencialidad de claves. Aunque IBAKE es la estructura básica de protocolo, se usa MIKEY como contenedor de protocolo para la entrega de claves.

Una idea clave sobre el marco de la solución IMS de la invención es que se reutiliza la arquitectura propuesta que incluye un KMS, pero, notablemente, no se requiere que estos servidores KMS estén siempre conectados. En otras palabras, en el marco propuesto, los KMS son servidores desconectados que se comunican periódicamente (por ejemplo, una vez al mes) con clientes usuarios finales para crear un marco seguro de cifrado basado en identidades,

mientras que las transacciones en línea entre los clientes usuarios finales (para la seguridad del plano de medios) se basan en un marco IBAKE que permite que los clientes participantes intercambien componentes de claves en un marco de cifrado asimétrico basado en identidades. Este marco, además de eliminar el depósito pasivo, permite que los clientes usuarios finales se autentiquen mutuamente (en la capa del plano de medios IMS) y proporciona perfecta confidencialidad en la ida y en la vuelta.

Obsérvese que el intercambio del KMS hacia los clientes se usa con moderación (por ejemplo, una vez al mes); de aquí que ya no hace falta que el KMS sea un servidor de alta disponibilidad y, en particular, diferentes KMS no tienen que comunicarse entre sí (cruzando límites de operadores). Además, dado que se usa un marco de cifrado asimétrico basado en identidades, se elimina la necesidad de una costosa infraestructura de claves públicas (PKI) y todos los costes operativos de la gestión y la revocación de certificados. Además, se da soporte de forma segura a diversas características del plano de medios IMS; esto incluye la ramificación segura, la reselección de destinatarios, la entrega diferida, el contenido codificado de antemano, el recorte multimedia y la anonimidad.

Las extensiones de la solución permiten aplicaciones seguras de conferencia en las que la aplicación de conferencia IMS autentica a los usuarios que se incorporan a una llamada, pero todos los participan de la llamada deciden una clave de grupo (con aportaciones de todos) mientras que el propio servidor de conferencia no averigua la clave de grupo. Además, la clave de grupo puede modificarse para dar cuenta de nuevos participantes y de participantes que abandonan una llamada. Una característica adicional del marco de gestión de claves basado en IMS es que, a pesar de la eliminación del depósito pasivo de claves, soporta compartir legalmente credenciales de seguridad con las fuerzas de seguridad usando el concepto de depósito activo.

La FIG. 7 proporciona un esquema de la arquitectura junto con las entidades implicadas en un ejemplo de protocolo de intercambio de claves entre extremos en el plano de medios IMS. Se entiende que, dado que la arquitectura IMS es bien conocida, no se describen con detalle los componentes funcionales representados en la FIG. 7. Puede hacerse referencia a los estándares de IMS para una explicación detallada de sus funciones. Obsérvese que, según se conoce, CSCF se refiere a una función de control de la sesión de la llamada, por lo que P-CSCF es una CSCF delegada y S-CSCF es una CSCF servidora. NAF se refiere a una función de aplicación de red.

En el escenario ilustrado, dos teléfonos de usuario final con prestaciones IMS están inmersos en un intercambio de claves entre extremos (e2e) para proteger las comunicaciones en la capa de aplicación. Obsérvese que la ilustración incluye transacciones autónomas entre un UE (equipo de usuario) y un KMS, así como transacciones en línea entre los UE a través del IMS.

Obsérvese que los UE y el KMS comparten una asociación de seguridad configurada de antemano en la que los usuarios pueden establecer comunicaciones seguras con el servidor de gestión de claves y en la que se proporciona autenticación mutua. Un ejemplo natural en el contexto de los sistemas 3GPP es el uso de la arquitectura genérica de arranque (véase, por ejemplo, la TS 33.220 de 3GPP, cuya divulgación se incorpora por referencia al presente documento). En la FIG. 7, las transacciones entre el KMS y un UE están habilitadas por medio de una BSF (función servidora de arranque), y recuérdese que esta transacción se lleva a cabo de forma moderada (por ejemplo, una vez al mes). Obsérvese que si la GBA no está disponible, pueden usarse otros tipos de credenciales, tal como IKEv2 con claves o certificados compartidos de antemano (véase, por ejemplo, IETF RFC 4306, cuya divulgación se incorpora por referencia al presente documento) para establecer esta autenticación mutua entre el usuario y el KMS.

Durante esta transacción, el UE presenta sus credenciales de abono, tras lo cual el KMS genera un conjunto de claves privadas (usadas en IBAKE). Si esta transacción se lleva a cabo una vez al mes, el KMS puede elegir generar una clave para cada día. El número de claves y la frecuencia de este intercambio son cuestión de directrices y pueden estar ligados al abono. Esta flexibilidad resulta especialmente útil para clientes de prepago.

Obsérvese que, en vez de un solo KMS, puede haber implicados dos KMS diferentes; uno para el usuario A, o sea, KMS_A, y uno para el usuario B, o sea, KMS_B. Sin embargo, KMS_A y KMS_B no tienen que comunicarse entre sí. Este escenario es especialmente aplicable en escenarios entre operadores.

Los inventores dan ahora un breve resumen de los intercambios implicados en MIKEY-IBAKE en el contexto del IMS.

Supongamos que A, B son los dos usuarios que intentan autenticarse y acordar una clave. A la vez, A y B representan sus correspondientes identidades, que, por definición, también representan sus claves públicas. Sean $H_1(A)=Q_A$ y $H_1(B)=Q_B$ los respectivos puntos de la curva elíptica correspondientes a las claves públicas. De hecho, también podríamos referirnos a Q_A y Q_B como claves públicas, dado que existe una correspondencia biunívoca entre las identidades y los puntos de la curva obtenidos aplicando H_1. Sea x un número aleatorio escogido por A, y sea y un número aleatorio escogido por B. El cifrado que sigue se refiere a un cifrado basado en identidades descrito en lo que antecede en la sección I.

El intercambio del protocolo MIKEY-IBAKE basado en IMS incluye las siguientes etapas (con referencia a componentes mostrados en la FIG. 7):

1. El UE IMS perteneciente al usuario A arranca con la BSF para poder establecer una conexión segura con el KMS, que actúa como una NAF. Esto permite que la BSF autentique al usuario y que el usuario autentique indirectamente al KMS. Si no puede usarse GBA, el UE IMS se conecta con el KMS y lo autentica y establece una clave compartida en función de una asociación de seguridad establecida de antemano.
2. El UE IMS entabla un intercambio MIKEY con el KMS y solicita una clave secreta (o múltiples claves secretas; por ejemplo, una para cada día).
3. El KMS genera la o las claves secretas multimedia para el UE IMS del usuario A y las envía al usuario A.
4. El UE IMS del usuario A calcula xP (es decir, P sumada consigo misma x veces como un punto en E, usando la ley aditiva en E) lo cifra usando la clave pública de B y lo transmite al UE IMS del usuario B.
5. El núcleo del IMS detecta la INVITACIÓN y la gestiona de tal forma que una función de red, si está autorizada, pueda obtener acceso a la clave de sesión. Esta etapa en particular es aplicable únicamente para soportar la característica de depósito activo necesaria para satisfacer cualquier requisito de interceptación legal.
6. El UE IMS del usuario B recibe la INVITACIÓN, que incluye el xP cifrado. El UE IMS del usuario B descifra el mensaje y obtiene xP. Subsiguientemente, B calcula yP y cifra el par {xP, yP} usando la clave pública del UE IMS del usuario A y luego lo transmite en un mensaje de respuesta a A.
7. Tras la recepción de este mensaje, el UE IMS del usuario A descifra el mensaje y obtiene yP. Subsiguientemente, el UE IMS del usuario A cifra yP usando la clave pública de B y lo devuelve en un mensaje de confirmación de respuesta a B. Tras esto, tanto A como B calculan xyP como la clave de sesión.
8. En este punto, el UE IMS del usuario B acepta la invitación y el uso de la seguridad multimedia.

Obsérvese que A escogió x al azar y que recibió yP en la segunda etapa del intercambio de protocolo. Esto permite que A calcule xyP sumando yP consigo mismo x veces. Por su parte, B escogió y al azar y recibió xP en la primera etapa del intercambio de protocolo. Esto permite que B calcule xyP sumando xP consigo mismo y veces.

Algunas propiedades ventajosas que se derivan del protocolo MIKEY-IBAKE son las siguientes:

Autenticación mutua. Obsérvese que el contenido de la carga útil en las etapas 4 y 7 se cifra usando la clave pública de B. De aquí que B, y solo B, pueda descifrar estos mensajes. Asimismo, el contenido del mensaje en la etapa 6 puede ser descifrado por A, y solo por A. Obsérvese también que las etapas 6 y 7 permiten que B y A se autentiquen mutuamente (demostrando que el mensaje fue descifrado correctamente). Esta característica novedosa permite que A y B se autentiquen mutuamente sin ayuda de ningún servidor en línea ni de ninguna autoridad de certificación.

Perfecta confidencialidad. Obsérvese que x e y son aleatorios. De aquí que la clave de sesión xyP sea nueva y no tenga ninguna relación con ninguna transacción pasada ni futura.

Eliminación del depósito pasivo. Obsérvese que, aunque el KMS (o un par de KMS) puede descifrar los mensajes del intercambio, es difícil determinar xyP dados xP e yP. La premisa de la dificultad se vale del problema de Diffie-Hellman en curvas elípticas. Obsérvese, además, que las curvas usadas para el IBE son específicas al KMS y, además, no es preciso que sean iguales que la curva usada para generar la clave de sesión. Esta flexibilidad ofrece un amplio número de opciones y también elimina cualquier coordinación necesaria entre KMS.

Gestión de identidades. Según se ha descrito en lo que antecede, para cifrar un mensaje un usuario usa la clave pública del destinatario usando la identidad (o una de las identidades) del destinatario. La identidad del destinatario puede estar en el formato que especifique un usuario específico, un grupo de usuarios o cualquier usuario. La denominación de los usuarios y de los grupos de usuarios puede seguir las convenciones normales del IMS y puede extenderse con el uso de comodines. En ciertos escenarios que implican aplicaciones de grupo, puede ser natural contar con normas que permitan que todos los destinatarios del grupo usen la clave secreta correspondiente a la identidad de ese grupo particular de usuarios. Por ejemplo, para usuarios empresariales, puede ser natural hacer que, por defecto, las claves secretas que correspondan a la identidad de la empresa se distribuyan a todos los usuarios de la empresa. Obsérvese que, debido a las propiedades del cifrado basado en identidades, aunque todos los usuarios pertenecientes a un grupo posiblemente posean la clave secreta de ese grupo, no todos los usuarios pueden obtener, no obstante, la clave de sesión establecida entre un remitente y algún otro usuario perteneciente a ese mismo grupo. Para garantizar que se imponen las normas, también es necesario que una identidad pública del usuario pueda vincularse de manera segura con un UE IMS. En otras palabras, es importante para la identidad usada por el usuario para autenticarse en el KMS con respecto a una identidad pública o un conjunto de identidades públicas.

Ahora los inventores exponen las extensiones del protocolo MIKEY-IBAKE con respecto a diversos escenarios de casuística de uso basada en IMS. Obsérvese que estas extensiones fueron descritas en general en lo que antecede en la sección II. La descripción que sigue está en el contexto de un entorno IMS.

A. Interceptación legal (LI) a través de depósito activo

Para poder proporcionar una copia en claro de la comunicación interceptada, tienen que cumplirse las condiciones siguientes:

1. Debe ser posible interceptar el tráfico (tanto la señalización como los medios).
2. Tienen que estar disponibles las claves de sesión usadas para la protección real del tráfico. Para hacer disponibles las claves de sesión se requieren funciones/servicios de KMS.

Según se ha mencionado en lo que antecede, las claves reales de sesión usadas para la protección del tráfico son generadas entre el remitente y el destinatario; así, no son conocidas por el KMS. Por lo tanto, se precisa una solución de depósito activo. En este escenario, para que el KMS obtenga una clave de sesión entre los usuarios A y B, precisa establecer una clave de sesión activa entre sí mismo y el usuario A y otra sesión activa simultánea entre sí mismo y el usuario B. El KMS se hace pasar por B ante A, y viceversa. Este papel de "intermediario" desempeñado por el KMS se denomina depósito activo y es similar a los procedimientos usados en un entorno de PKI, en el que una autoridad de certificación genera "certificados falsos" y se sitúa en medio del intercambio. La diferencia entre la técnica usada en las autoridades convencionales de certificación y el presente enfoque del depósito activo es que el KMS no tiene que generar claves falsas.

Con el encaminamiento del tráfico de señalización a través de la red de origen, la interceptación del tráfico de señalización en la red de origen puede realizarse en el servidor o los servidores SIP (protocolo de inicio de sesiones). Este tráfico de señalización precisa entonces ser encaminado hacia el KMS apropiado para que este KMS establezca las necesarias claves de sesión con los correspondientes usuarios. En situaciones de itinerancia, dado que el tráfico de señalización SIP está protegido confidencialmente entre el UE IMS y la P-CSCF, y considerando que en los despliegues actuales la P-CSCF está situada en la red de origen, la señalización SIP solo está disponible en formato cifrado a nivel de portador en la red visitada.

Para escenarios de itinerancia, aunque la señalización y el contenido SIP cifrados siempre estén disponibles, para interceptar la señalización SIP y descifrar el contenido de la comunicación, tiene que haber un acuerdo interoperativo entre la red visitada y la entidad que gestiona el KMS. Normalmente, el KMS residirá en la red de origen, de modo que, para la LI llevada a cabo por la red visitada, se precisa la cooperación con la red de origen.

En línea con los estándares de LI, cuando la VPLMN (red pública móvil terrestre visitada) no está implicada en el cifrado, en la VPLMN solo estaría disponible para la LI el contenido cifrado.

B. Usuarios en diferentes dominios KMS

Los usuarios de diferentes dominios KMS tendrán claves secretas generadas por KMS diferentes. En consecuencia, puede usarse un conjunto diferente de parámetros públicos (por ejemplo, material criptográfico) para generar claves públicas y secretas para usuarios en diferentes dominios KMS. Para garantizar el debido cifrado/descifrado, un remitente y un destinatario precisan conocer los parámetros públicos exactos usados por cada lado. No obstante, si un usuario en un dominio KMS precisa establecer una llamada segura con un usuario de otro dominio KMS, no es preciso que los KMS implicados cooperen. Como en cualquier protocolo criptográfico basado en identidades, o, si a eso se va, cualquier protocolo de claves públicas, se puede dar por sentado con certeza que los parámetros públicos necesarios para el intercambio están disponibles o se intercambian públicamente.

C. Escenarios de extremo a intermediario

En los escenarios de extremo a intermediario, la protección multimedia es entre un UE IMS y una entidad de red. En un escenario en el que la llamada se inicia desde un UE IMS, el establecimiento de la llamada seguiría los mismos principios que para una llamada protegida entre extremos. El UE IMS iniciante usa la identidad de la entidad de red (por ejemplo, el MGWC: control de pasarela multimedia) para cifrar xP, según se ha descrito en lo que antecede, y lo envía junto con la INVITACIÓN. El MGWC intercepta el mensaje y genera yP de la misma manera que habría hecho un UE IMS receptor. El MGWC configura entonces la MGW para que tenga seguridad multimedia hacia el UE IMS. El tráfico multimedia se remite en claro por la PSTN (red fónica pública conmutada).

Para las llamadas entrantes a los UE IMS, el MGWC verifica que al menos un terminal dado de alta para el destinatario previsto haya hecho constar prestaciones y preferencias de seguridad multimedia. Si no hay ningún terminal con prestaciones de protección multimedia, la llamada se remite en claro. Si lo hay, el MGWC escoge y, y genera yP. El MGWC inserta entonces el yP cifrado (usando la identidad de los UE IMS) en la INVITACIÓN e inicia el uso de la seguridad multimedia en la MGW en el tráfico multimedia entre la MGW y el terminal IMS.

D. Ramificación de claves

En esta sección se presenta la ramificación para el caso de un MIKEY-IBAKE basado en IMS. Recuérdese que la ramificación se describe en general en lo que antecede en el contexto de la FIG. 2. La ramificación es la entrega de una petición (por ejemplo, un mensaje INVITACIÓN) a múltiples ubicaciones. Esto ocurre cuando una único usuario del IMS está dado de alta más de una vez. Un ejemplo de ramificación es cuando un usuario tiene un teléfono de sobremesa, un cliente de PC y un terminal móvil, todos dados de alta con la misma identidad pública.

En el ejemplo representado en lo que sigue y mostrado en el contexto de las etapas 1 a 8 de la FIG. 8, supongamos que el UE IMS del usuario B tiene múltiples direcciones de contacto dadas de alta con una única identidad pública B

de usuario. En otras palabras, tanto B1 como B2 obtienen una clave secreta correspondiente a una identidad pública B. En este caso, si el UE IMS del usuario A quiere ponerse en contacto con el UE IMS del usuario B, la petición será entregada tanto a B1 como a B2. Suponiendo que B2 responda a una llamada, B2 descifra primera el mensaje recibido usando la clave secreta asociada con la identidad B. B2 elige entonces una y aleatoria y envía a A un mensaje que incluye yP y su identidad B2 cifrada usando la identidad pública de A. Tras la recepción de este mensaje, el usuario A lo descifra, se percata de que está comunicándose con el usuario B2 y envía un mensaje de confirmación de respuesta que incluye el yP recibido cifrado usando la identidad pública de B2.

Obsérvese que B1 es capaz de descifrar el mensaje recibido del usuario A cifrado usando la identidad pública de B; por lo tanto, es capaz de obtener xP. Sin embargo, no es capaz de descifrar el mensaje enviado desde B2, ya que está cifrado usando la identidad de A. Así, el usuario B1 no es capaz de obtener yP. Obsérvese, además, que aunque B1 sea capaz de obtener yP, seguiría siendo incapaz de calcular xyP. Obsérvese que, en la FIG. 7, (M)_X denota que el mensaje M está cifrado usando la identidad de X.

E. Redireccionamiento

En esta sección se presenta el redireccionamiento (reselección de destinatario) para el caso de un MIKEY-IBAKE basado en IMS. Recuérdese que el redireccionamiento se describe en general en lo que antecede en el contexto de la FIG. 3. El redireccionamiento de la sesión es un escenario en el que un elemento funcional decide redirigir la llamada a un destino diferente. El redireccionamiento de la sesión permite los típicos servicios de “desvío de sesión incondicional”, “desvío de sesión ocupado”, “desvío de sesión variable”, “desvío de sesión selectivo” y “desvío de sesión sin respuesta”.

Hay dos escenarios básicos de redireccionamiento de sesiones. En el primer escenario, un elemento funcional (por ejemplo, la S-CSCF) decide redirigir la sesión usando el procedimiento REDIRECCIONAMIENTO SIP. En otras palabras, el elemento funcional pasa al originador la nueva información de destino. En consecuencia, el originador inicia una nueva sesión con el destino redirigido proporcionado por el elemento funcional. Para el caso de un MIKEY-IBAKE, esto quiere decir que el originador iniciará una nueva sesión con la identidad del destino redirigido.

En el segundo escenario, un elemento funcional decide redirigir la sesión sin informar al originador. Un escenario común es uno en el que la S-CSCF del usuario de destino determina que la sesión ha de ser redirigida. La información del perfil del usuario obtenida del HSS (servidor de abonados en origen) mediante la “atracción de Cx” durante el alta puede contener lógica y desencadenantes complejos que causen el redireccionamiento de la sesión.

En el ejemplo representado en las etapas 1 a 8 de la FIG. 9, sin pérdida de la generalidad, se da por sentado que el usuario B estableció el desvío de la sesión con el usuario C. En este caso, el usuario B incluye en su perfil de usuario su clave secreta SK_B cifrada usando la identidad de C. Por lo tanto, una vez que la S-CSCF recibe el mensaje del usuario A y decide que el mensaje precisa ser redirigido, incluye la clave cifrada de B en el mensaje redirigido al usuario C. Tras recibir el mensaje, el usuario C cifra la clave secreta y, a su vez, el mensaje procedente de A. El usuario C escoge entonces la y aleatoria y envía a A un mensaje que incluye yP y su identidad C cifrada usando la identidad pública de A. Tras recibir este mensaje, el usuario A lo descifra, se percata de que está comunicándose con el usuario C y envía un mensaje de confirmación de respuesta que incluye el yP recibido cifrado usando la identidad pública de C. En la FIG. 9, (M)_X denota que el mensaje M está cifrado usando la identidad de X.

F. Entrega diferida

En esta sección se presenta la entrega diferida para el caso de un MIKEY-IBAKE basado en IMS. Recuérdese de la sección II que la entrega diferida es un tipo de servicio tal que el contenido de la sesión no pueda ser entregado al destino en el momento en que se envía (por ejemplo, el usuario de destino no está conectado en ese momento o decide no contestar la llamada). No obstante, el remitente espera que la red entregue el mensaje tan pronto como el destinatario esté disponible. Un ejemplo típico de entrega diferida es el correo de voz.

En lo que sigue se presentan dos escenarios básicos de entrega diferida para el caso de un MIKEY-IBAKE basado en IMS. Puede volver a hacerse referencia a la FIG. 4A para el primer escenario y a la FIG. 4B para el segundo escenario.

En el primer escenario, el usuario A y el buzón de B llevan a cabo una autenticación mutua antes de acordar la clave que ha de usarse para descifrar el contenido del mensaje previsto para una entrega diferida, mientras que en el segundo escenario no se lleva a cabo una autenticación mutua.

En el primer escenario (de nuevo, puede volver a hacerse referencia a la FIG. 4A, en la que el elemento funcional 402 es un servidor IMS), se da por sentado que el usuario A está intentando ponerse en contacto con el usuario B, que no está disponible en ese momento; por lo tanto, la llamada se desvía al “correo de voz” de B (más en general, un servidor de entrega diferida). Siguiendo el protocolo MIKEY-IBAKE, el mensaje recibido por el buzón de B se cifra usando la identidad de B; por lo tanto, el buzón de B no podrá descifrarlo. El buzón de B escoge una y aleatoria y calcula yP y envía su identidad e yP, cifrados por IBE, al usuario A. El usuario A reconoce que B no recibió el

mensaje y que el destinatario real no pudo descifrar el mensaje enviado en la primer etapa por la falta de su identidad y de xP. Por lo tanto, el usuario envía un nuevo mensaje que contiene la identidad de A, la identidad del buzón de B, xP e yP, todos cifrados por IBE usando la identidad del buzón de B. Tras la recepción de este mensaje, el buzón de B acepta "sK" como clave de sesión para el mensaje previsto para B y devuelve la identidad de A y xP al usuario A para completar la autenticación.

Obsérvese que sK se cifra usando la clave pública de B; de aquí que el buzón B no pueda descifrar este mensaje ni obtener "sK". Subsiguientemente, cuando B esté conectado y compruebe el "correo de voz" (haga una verificación con el servidor de entrega diferida), B podrá obtener del servidor del buzón el valor cifrado de sK. Obsérvese que B puede tener que autenticarse en el buzón para obtener la clave; esto podría basarse en mecanismos existentes de autenticación ya implementados.

En el segundo escenario (de nuevo, puede volver a hacerse referencia a la FIG. 4B, en la que el elemento funcional 402 es un servidor IMS), vale la misma premisa: el usuario A está intentando ponerse en contacto con el usuario B, que no está disponible en ese momento; por lo tanto, la llamada se desvía al correo de voz de B. Sin embargo, en este caso el buzón de B y el usuario A no llevan a cabo la autenticación. En vez de ello, el buzón de B simplemente acepta sK como clave de sesión y devuelve un mensaje de OK al usuario A para confirmarlo.

G. Llamadas de grupo y conferencia

En esta sección, el protocolo de gestión de claves de MIKEY-IBAKE se extiende a llamadas de grupo y conferencia. Obsérvese que las propiedades ventajosas que se derivan del protocolo MIKEY-IBAKE se realizan, por lo tanto, en un entorno de conferencia. Recuérdese que la conferencia fue descrita en general en lo que antecede en el contexto de las FIGURAS 6A a 6C. Obsérvese que el ejemplo de IMS de la FIG. 10 es para N=3.

En el escenario basado en IMS representado en las etapas 1 a 18 de la FIG. 10, se da por sentado que hay un servidor de conferencia (AS/MRFC: servidor de aplicaciones/controlador de funciones de recursos multimedia) que invita a los usuarios a la llamada de conferencia. Esto podría ser resultado, por ejemplo, de una petición de REFERENCIA recibida anteriormente de otro usuario. Un enfoque alternativo sería delegar esta función a uno de los usuarios (por ejemplo, a quien presida la conferencia). Aunque la FIG. 10 no muestra esta alternativa, el enfoque sería similar y el cálculo de la clave de grupo sería el mismo.

En la descripción que sigue, se da por sentado que todos los mensajes están cifrados por IBE (por ejemplo, si un usuario Y está enviando un mensaje M a un usuario X, el mensaje M está cifrado usando la identidad de X) usando la identidad apropiada. En la FIG. 10, esto se denota como (M)_X, que significa que el mensaje M está cifrado por IBE usando la identidad de X.

En el primer conjunto de intercambios con el servidor de conferencia, los usuarios A_1, A_2, y A_3 escogen a_1, a_2, y a_3 aleatorias, respectivamente, y cada usuario A_i envía $w_i = a_iP$ al servidor de conferencia. En el segundo conjunto de intercambios el servidor de conferencia envía todos los a_iP a todos los usuarios, mientras que cada usuario envía $z_i = a_i(a_{i+1}P - a_{i-1}P)$. En el intercambio final, el servidor de conferencia envía todos los z_i a cada usuario. Tras esto, todos los participantes de la conferencia pueden calcular la clave de grupo como sigue: $K_i = 3a_iw_{i-1} + 2z_i + z_{i+1}$.

Obsérvese que $K_1=K_2=K_3$. Obsérvese también que, aunque los usuarios A_1, A_2, y A_3 son capaces de generar la clave de grupo, el servidor de conferencia no lo es, dado que, aunque conoce los z_i y los w_i, solo los usuarios individuales conocen sus a_i escogidas al azar.

En aras de la simplicidad, la exposición anterior se centra en tres participantes de la llamada de conferencia. Sin embargo, los anteriores procedimientos pueden generalizarse a n participantes. En el caso de n participantes, la clave de grupo se genera como $K_i = na_iw_{i-1} + (n\text{-}1)z_i + (n\text{-}2)z_{i-1} + \ldots + z_{i-2}$, siendo w_i y z_i según se define en lo que antecede.

Una de las características importantes del protocolo es que la clave de grupo cambia cada vez que se admite a un nuevo usuario o que un usuario existente abandona la llamada. Esto garantiza que los nuevos usuarios no averigüen la clave de grupo antes de sumarse a la llamada y que los usuarios que abandonan la llamada prematuramente no logren acceso a las conversaciones tras la llamada.

Obsérvese que cuando se suma un nuevo usuario y ya hay N usuarios en el sistema, habrá un total de N+1 usuarios en el sistema. Cuando estos usuarios son puestos en un círculo, el usuario próximo al usuario enésimo será ahora el usuario (N+1)-ésimo (y no el 1er usuario, como ocurría ante de admitir al usuario (N+1)-ésimo). El protocolo para admitir a un nuevo usuario funciona como sigue:

El nuevo usuario se autentica con el servidor de conferencia usando IBAKE, de forma similar a todos los usuarios. Esto permite que el usuario sea admitido (y autorizado en la llamada) y se garantiza al nuevo usuario que se incorpora a la conferencia correcta (mediante la autenticación del servidor de conferencia).

Sea $z_{N+1} = a_{N+1}P$ el valor escogido por el nuevo usuario durante la autenticación

El servidor de conferencia envía entonces el conjunto {z_i} para todo i=1 a N+1 a todos los usuarios, ya sea por difusión o unidifusión. Esto permite que todos los usuarios sepan del nuevo usuario y que determinen sus nuevos vecinos. Obsérvese que la lista de vecinos cambia solo para los usuarios 1, N, y N+1.

Los usuarios 1, N, y N+1 calculan entonces su correspondiente valor de w, y lo devuelven (individualmente) al servidor de conferencia.

El servidor envía entonces una lista actualizada de {w_i} a todos los usuarios.

Todos los participantes recalculan entonces la clave de grupo usando la misma relación que en lo que antecede, salvo que N es sustituida por N+1 y los nuevos valores de z_i y w_i.

Cuando un usuario abandona la llamada de conferencia, no tiene que ejecutarse ningún procedimiento nuevo de autenticación, pero la clave de grupo cambia. El procedimiento funciona como sigue:

El servidor de conferencia se percata de que el usuario abandona la llamada de conferencia.

Subsiguientemente, el servidor de conferencia informa a todos de esta circunstancia y de información pertinente a qué usuario (no solo su identidad, sino que también incluye el orden) abandonó la llamada. Para simplificar las cosas, el servidor de conferencia puede volver a enviar la nueva lista {z_i}.

Esto permite que todos los usuarios redescubran a sus vecinos y que recalculen w_i, si es necesario.

Todos los participantes que permanecen en la llamada, para los cuales w_i cambió, informarán al servidor de conferencia de su nuevo valor.

El servidor de conferencia envía entonces la lista actualizada {w_i}.

Todos los participantes recalculan entonces la clave de grupo usando la misma relación que en lo que antecede, salvo que N es sustituida por N-1 y se usan los nuevos valores de w_i.

IV. Sistema de cálculo ilustrativo

La FIG. 11 ilustra una arquitectura genérica 1100 de soporte físico de un entorno de red y dispositivos de comunicaciones en forma de dispositivos de cálculo adecuados para implementar un protocolo seguro de gestión de claves entre dos entidades según la presente invención. Aunque la FIG. 11 muestra solo dos entidades, ha de entenderse que otras entidades pueden tener la misma configuración. Así, en términos de los protocolos seguros de gestión de claves descritos en lo que antecede, las dos entidades pueden ser el iniciador 102-I (un primer partícipe o A) y el contestador 102-R (un segundo partícipe o B). Sin embargo, pueden implementarse varios KMS, servidores de conferencia, servidores de LI, elementos funcionales, dispositivos cliente (partícipes) adicionales y servidores adicionales con la misma arquitectura que la mostrada en un dispositivo de cálculo de la FIG. 11. Así, en aras de la simplicidad, en la FIG. 11 no se muestran todos los dispositivos de cálculo (dispositivos de comunicaciones) que puedan participar en los protocolos de la invención.

Según se muestra, el dispositivo de cálculo de A, designado 1102 y el dispositivo de cálculo de B, designado 1104, están acoplados por medio de una red 1106. La red puede ser cualquier red en la que los dispositivos sean capaces de comunicarse; por ejemplo, como en las realizaciones descritas en lo que antecede, la red 1106 podría incluir una red de comunicaciones de área amplia de acceso público, tal como una red de comunicaciones celulares explotada por una empresa explotadora de la red (por ejemplo, Verizon, AT&T, Sprint). Sin embargo, la invención no está limitada a un tipo particular de red. Normalmente, los dispositivos podrían ser máquinas clientes. Ejemplos de dispositivos clientes que pueden emplearse por los partícipes para participar en los protocolos descritos en el presente documento pueden incluir, sin limitaciones, teléfonos celulares, teléfonos inteligentes, teléfonos de sobremesa, agendas electrónicas, ordenadores portátiles, ordenadores personales, etc. Sin embargo, uno o más de los dispositivos podrían ser servidores. Así, ha de entenderse que el protocolo de comunicaciones de la presente invención no está limitado al caso en que los sistemas de cálculo sean cliente y servidor, respectivamente, sino que, en vez de ello, es aplicable a cualesquiera dispositivos de cálculo que comprendan los dos elementos de red.

Tal como será fácilmente evidente a una persona con un dominio de la técnica, los servidores y los clientes pueden implementarse como ordenadores programados que operen bajo el control de código de programas de ordenador. El código de programas de ordenador estaría almacenado en un medio de almacenamiento legible por ordenador (por ejemplo, una memoria) y el código sería ejecutado por un procesador del ordenador. Dada esta divulgación de la invención, un experto en la técnica podría producir fácilmente código apropiado de programas de ordenador para implementar los protocolos descritos en el presente documento.

No obstante, la FIG. 11 ilustra en general una arquitectura ejemplar para cada sistema de ordenador que se comunica por la red. Según se muestra, el dispositivo 1102 comprende dispositivos de E/S 1108-A, el procesador 1110-A y la memoria 1112-A. El dispositivo 1104 comprende dispositivos de E/S 1108-B, el procesador 1110-B y la memoria 1112-B. Debería entenderse que, según se usa en el presente documento, se pretende que el término "procesador" incluya uno o más dispositivos de proceso, incluyendo una unidad central de proceso (CPU) u otra circuitería de proceso, incluyendo, sin limitación, uno o más procesadores de señales, uno o más circuitos integrados y similares. Además, según se usa en el presente documento, se pretende que el término "memoria" incluya memoria asociada con un procesador o una CPU, tal como RAM, ROM, un dispositivo fijo de memoria (por ejemplo, un disco duro) o un dispositivo extraíble de memoria (por ejemplo, un disquete o un CDROM). Además, según se usa en el presente documento, se pretende que la expresión "dispositivos de E/S" incluya uno o más dispositivos de entrada (por ejemplo, teclado, ratón) para introducir datos en la unidad de proceso, así como uno o más dispositivos de salida (por ejemplo, una pantalla de rayos catódicos) para proporcionar resultados asociados con la unidad de proceso.

En consecuencia, las instrucciones o el código de soporte lógico para llevar a cabo las metodologías de la invención, descritas en el presente documento, pueden almacenarse en uno o más de los dispositivos de memoria asociados, por ejemplo ROM, memoria fija o extraíble, y, cuando estén listos para ser utilizados, ser cargados en la RAM y ejecutados por la CPU.

Aunque en el presente documento se han descrito realizaciones ilustrativas de la presente invención con referencia a los dibujos adjuntos, ha de entenderse que la invención no está limitada a esas realizaciones precisas y que un experto en la técnica puede realizar diversos cambios y modificaciones adicionales sin apartarse del ámbito de la invención.

REIVINDICACIONES

1. Un procedimiento de gestión de una conferencia entre dos o más partícipes en un sistema de comunicaciones, comprendiendo el procedimiento las etapas de:

llevar a cabo una operación de intercambio autenticado de claves basado en identidades entre un elemento de gestión de la conferencia del sistema de comunicaciones y cada uno de los dos o más partícipes que buscan participar en la conferencia, estando cifrados los mensajes intercambiados entre el elemento de gestión de la conferencia y los dos o más partícipes en función de las respectivas identidades de los destinatarios de los mensajes, y recibiendo, además, el elemento de gestión de la conferencia, procedente de cada partícipe, durante la operación de autenticación de claves, un componente de clave aleatoria que es calculado en función de un número aleatorio seleccionado por el interlocutor;
enviar a cada partícipe, desde el elemento de gestión de la conferencia, un conjunto que comprende los componentes de clave aleatoria calculados por los partícipes;
recibir en el elemento de gestión de la conferencia, procedente de cada partícipe, un componente de clave aleatoria de grupo, siendo calculado el componente de clave aleatoria de grupo por cada partícipe mediante un cálculo en función del número aleatorio usado por el partícipe durante la operación de autenticación de claves y los componentes de clave aleatoria calculados por un subconjunto de otros partícipes de los dos o más partícipes que buscan participar en la conferencia; y
enviar a cada partícipe, desde el elemento de gestión de la conferencia, un conjunto que comprende los componentes de clave aleatoria de grupo calculados por los partícipes de tal modo que cada partícipe pueda calcular la misma clave de grupo para su uso en la comunicación con cada uno de los demás partícipes por medio del elemento de gestión de la conferencia.

2. El procedimiento de la reivindicación 1 en el que la clave de grupo calculada por cada partícipe se representa como $Na_i(Z_{i-1}) + (N-1)X_i + (N-2)X_{i+1} + \ldots + X_{i-2}$, representando N el número total de partícipes que buscan participar en la conferencia, representando a_i el número aleatorio seleccionado por el partícipe dado, representando Z_i el componente de clave aleatoria calculado por el partícipe dado, representando X_i el componente de clave aleatoria de grupo calculado por el partícipe dado, y representando i un número de ordenación de la conferencia para el partícipe dado en la conferencia de N partícipes, siendo i-1=N cuando i=1 e i+1=1 cuando i=N.

3. El procedimiento de la reivindicación 2 en el que el componente de clave aleatoria para un partícipe dado es calculado mediante un cálculo representado como a_iP, siendo a_i el número aleatorio seleccionado por el partícipe dado y siendo P un punto seleccionado de un grupo asociado con la operación de autenticación de claves basada en el cifrado de identidad.

4. El procedimiento de la reivindicación 2 en el que el componente de clave aleatoria de grupo para un partícipe dado se calcula mediante un cálculo representado como $a_i(a_{i+1}P - a_{i-1}P)$, siendo a_i el número aleatorio seleccionado por el partícipe dado, siendo $a_{i+1}P$ el componente de clave aleatoria enviado al elemento de gestión de la conferencia por el partícipe que sigue inmediatamente al partícipe dado en la ordenación de la conferencia, siendo $a_{i-1}P$ el componente de clave aleatoria enviado al elemento de gestión de la conferencia por el partícipe que precede inmediatamente al partícipe dado en la ordenación de la conferencia y siendo P un punto seleccionado de un grupo asociado con un protocolo de intercambio de claves criptográficas.

5. El procedimiento de la reivindicación 1 en el que los dos o más partícipes que buscan participar en la conferencia obtienen claves privadas respectivas de uno o más servicios de gestión de claves.

6. El procedimiento de la reivindicación 1 en el que la clave de grupo cambia siempre que un nuevo partícipe se suma a la conferencia o un partícipe participante abandona la conferencia.

7. El procedimiento de la reivindicación 1 en el que el elemento funcional imita a un partícipe sospechoso de delitos que busca participar en la conferencia, de modo que el elemento funcional puede interceptar mensajes de conferencia destinados al partícipe sospechoso de delitos y procedentes del mismo.

8. Un aparato de gestión de una conferencia entre dos o más partícipes en un sistema de comunicaciones, comprendiendo el aparato:

una memoria; y
al menos un procesador acoplado a la memoria y configurado para:

llevar a cabo una operación de intercambio autenticado de claves basado en identidades entre un elemento de gestión de la conferencia del sistema de comunicaciones y cada uno de los dos o más partícipes que buscan participar en la conferencia, estando cifrados los mensajes intercambiados entre el elemento de gestión de la conferencia y los dos o más partícipes en función de las respectivas identidades de los destinatarios de los mensajes, y recibiendo, además, el elemento de gestión de la conferencia, procedente de cada partícipe, durante la operación de autenticación de claves, un

componente de clave aleatoria que se calcula en función de un número aleatorio seleccionado por el interlocutor;
enviar a cada partícipe, desde el elemento de gestión de la conferencia, un conjunto que comprende los componentes de clave aleatoria calculados por los partícipes;
recibir en el elemento de gestión de la conferencia, procedente de cada partícipe, un componente de clave aleatoria de grupo, siendo calculado el componente de clave aleatoria de grupo por cada partícipe mediante un cálculo en función del número aleatorio usado por el partícipe durante la operación de autenticación de claves y los componentes de clave aleatoria calculados por un subconjunto de otros partícipes de los dos o más partícipes que buscan participar en la conferencia; y
enviar a cada partícipe, desde el elemento de gestión de la conferencia, un conjunto que comprende los componentes de clave aleatoria de grupo calculados por los partícipes de tal modo que cada partícipe pueda calcular la misma clave de grupo para su uso en la comunicación con cada uno de los demás partícipes por medio del elemento de gestión de la conferencia, pero siendo incapaz el elemento de gestión de la conferencia de calcular la clave de grupo.

9. Un procedimiento para su uso en la participación en una conferencia entre partícipes en un sistema de comunicaciones, comprendiendo el procedimiento, en un partícipe dado, las etapas de:

llevar a cabo una operación de intercambio autenticado de claves basado en identidades entre un elemento de gestión de la conferencia del sistema de comunicaciones y el partícipe dado, llevando a cabo también el elemento de gestión de la conferencia la operación de intercambio de claves autenticado basado en identidades con los otros partícipes que buscan participar en la conferencia, estando cifrados los mensajes intercambiados entre el elemento de gestión de la conferencia y los partícipes en función de las respectivas identidades de los destinatarios de los mensajes, y recibiendo, además, el elemento de gestión de la conferencia, procedente de cada partícipe, durante la operación de autenticación de claves, un componente de clave aleatoria que se calcula en función de un número aleatorio seleccionado por el interlocutor;
recibir, en el partícipe dado, procedente del elemento de gestión de la conferencia, un conjunto que comprende los componentes de clave aleatoria calculados por los partícipes;
enviar desde el partícipe dado al elemento de gestión de la conferencia, un componente de clave aleatoria de grupo, recibiendo también el elemento de gestión de la conferencia un componente de clave aleatoria de grupo procedente de cada uno de los demás partícipes, siendo calculado el componente de clave aleatoria de grupo por cada partícipe mediante un cálculo en función del número aleatorio usado por el partícipe durante la operación de autenticación de claves y los componentes de clave aleatoria calculados por un subconjunto de otros partícipes de los partícipes que buscan participar en la conferencia;
recibir, en el partícipe dado, procedente del elemento de gestión de la conferencia, un conjunto que comprende los componentes de clave aleatoria de grupo calculados por los partícipes; y
calcular, en el partícipe dado, una clave de grupo que sea la misma clave de grupo calculada por los demás partícipes para su uso en la comunicación con cada uno de los demás partícipes por medio del elemento de gestión de la conferencia.

10. Un aparato para su uso al participar en una conferencia entre partícipes en un sistema de comunicaciones, comprendiendo el aparato, en un partícipe dado:

una memoria; y
al menos un procesador acoplado a la memoria y configurado para:

llevar a cabo una operación de intercambio autenticado de claves basado en identidades entre un elemento de gestión de la conferencia del sistema de comunicaciones y el partícipe dado, llevando a cabo también el elemento de gestión de la conferencia la operación de intercambio de claves autenticado basado en identidades con los otros partícipes que buscan participar en la conferencia, estando cifrados los mensajes intercambiados entre el elemento de gestión de la conferencia y los partícipes en función de las respectivas identidades de los destinatarios de los mensajes, y recibiendo, además, el elemento de gestión de la conferencia, procedente de cada partícipe, durante la operación de autenticación de claves, un componente de clave aleatoria que se calcula en función de un número aleatorio seleccionado por el interlocutor;
recibir, en el partícipe dado, procedente del elemento de gestión de la conferencia, un conjunto que comprende los componentes de clave aleatoria calculados por los partícipes;
enviar desde el partícipe dado al elemento de gestión de la conferencia, un componente de clave aleatoria de grupo, recibiendo también el elemento de gestión de la conferencia un componente de clave aleatoria de grupo procedente de cada uno de los demás partícipes, siendo calculado el componente de clave aleatoria de grupo por cada partícipe mediante un cálculo en función del número aleatorio usado por el partícipe durante la operación de autenticación de claves y los componentes de clave aleatoria calculados por un subconjunto de otros partícipes de los partícipes que buscan participar en la conferencia;
recibir, en el partícipe dado, procedente del elemento de gestión de la conferencia, un conjunto que comprende los componentes de clave aleatoria de grupo calculados por los partícipes; y

calcular, en el partícipe dado, una clave de grupo que sea la misma clave de grupo calculada por los demás partícipes para su uso en la comunicación con cada uno de los demás partícipes por medio del elemento de gestión de la conferencia.

FIG. 1A

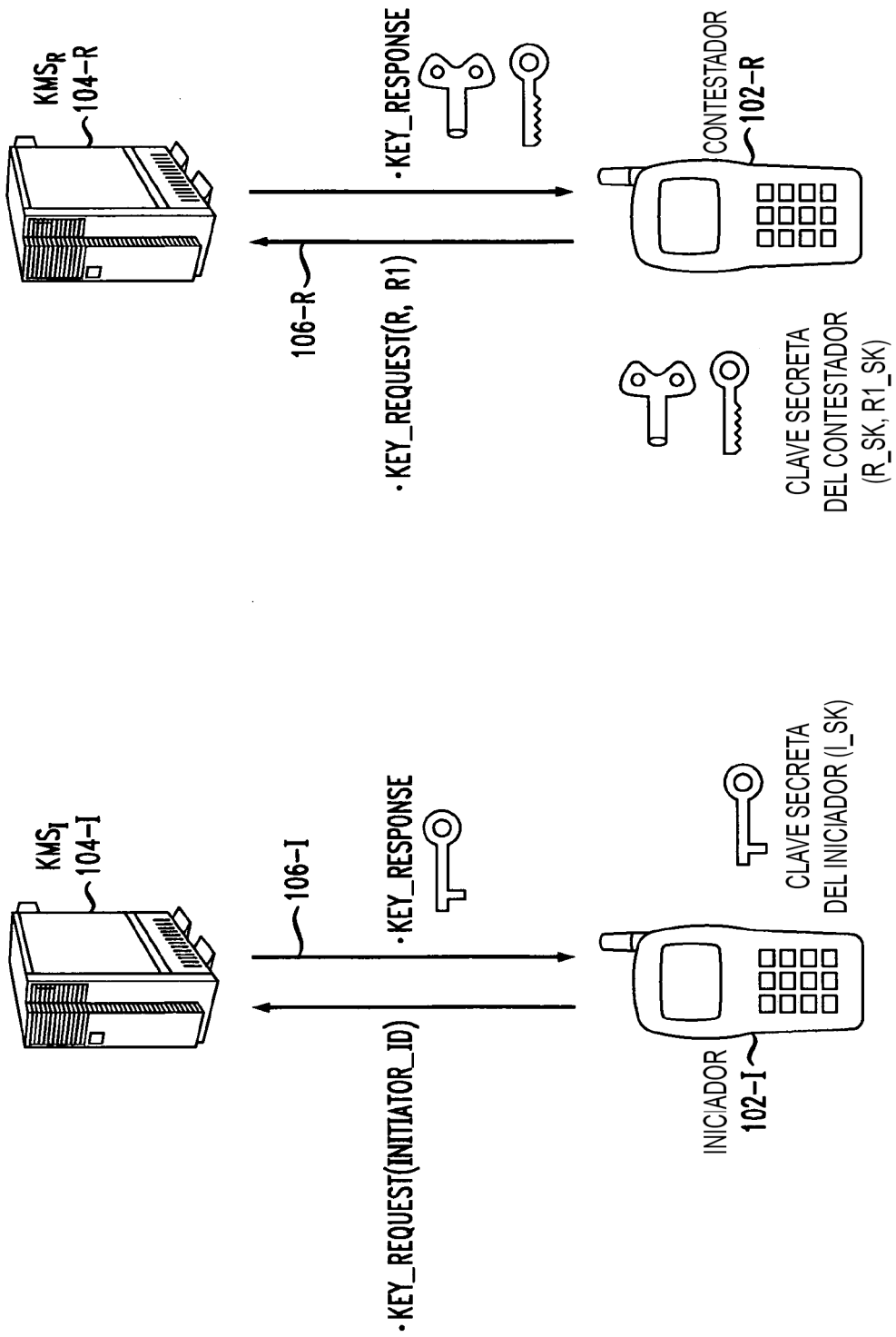

KMS_R
104-R
·KEY_RESPONSE
CONTESTADOR
102-R
106-R
·KEY_REQUEST(R, R1)
CLAVE SECRETA
DEL CONTESTADOR
(R_SK, R1_SK)
KMS_I
104-I
106-I
·KEY_RESPONSE
CLAVE SECRETA
DEL INICIADOR (I_SK)
·KEY_REQUEST(INITIATOR_ID)
INICIADOR
102-I

FIG. 1B

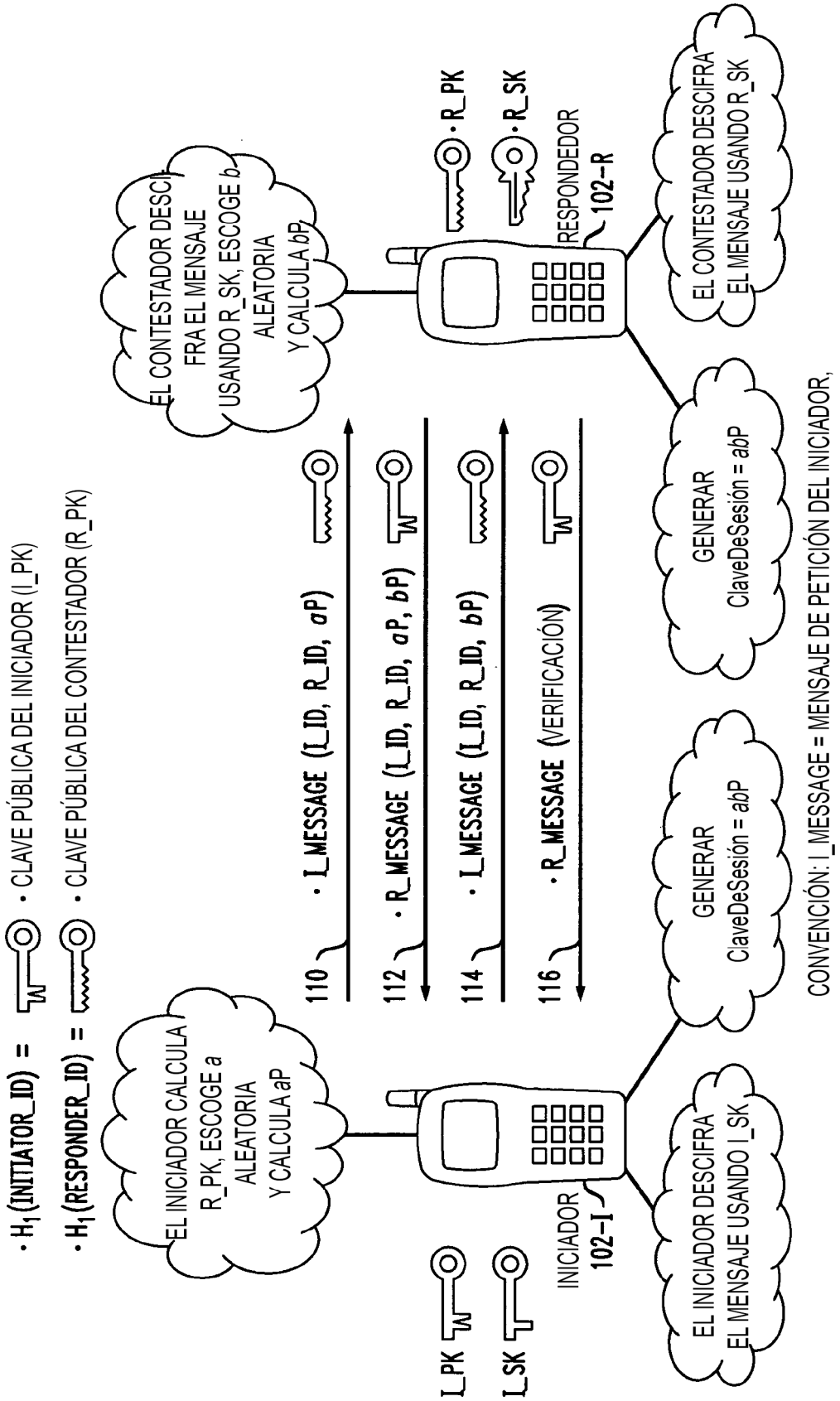
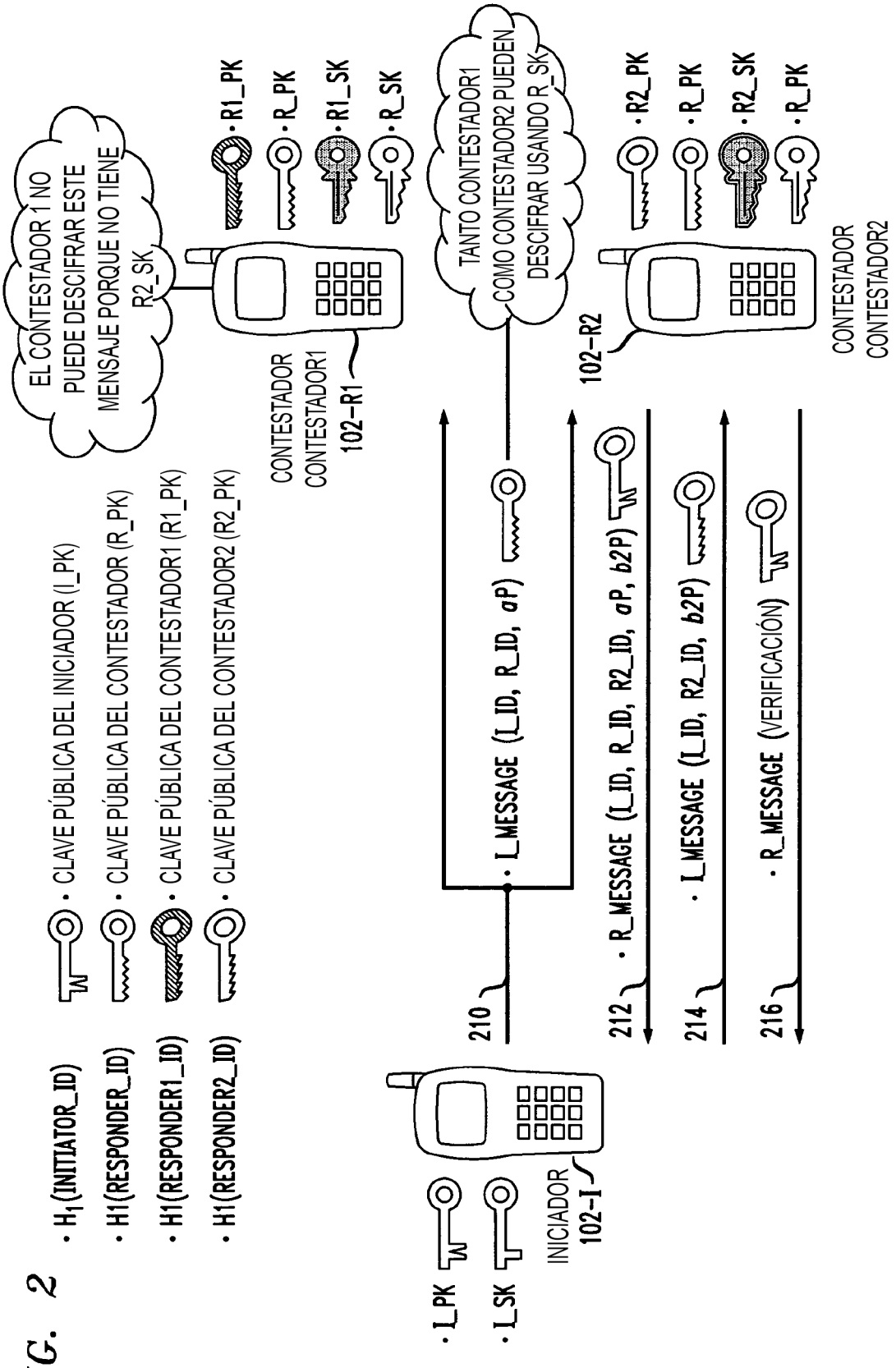

• H_1(INITIATOR_ID) = • CLAVE PÚBLICA DEL INICIADOR (I_PK)
• H_1(RESPONDER_ID) = • CLAVE PÚBLICA DEL CONTESTADOR (R_PK)
EL INICIADOR CALCULA R_PK, ESCOGE a ALEATORIA Y CALCULA aP
EL CONTESTADOR DESCIFRA EL MENSAJE USANDO R_SK, ESCOGE b ALEATORIA Y CALCULA bP
110 • I_MESSAGE (I_ID, R_ID, aP)
112 • R_MESSAGE (I_ID, R_ID, aP, bP)
114 • I_MESSAGE (I_ID, R_ID, bP)
116 • R_MESSAGE (VERIFICACIÓN)
• I_PK
• I_SK
INICIADOR 102-I
• R_PK
• R_SK
RESPONDEDOR 102-R
GENERAR ClaveDeSesión = abP
GENERAR ClaveDeSesión = abP
EL INICIADOR DESCIFRA EL MENSAJE USANDO I_SK
EL CONTESTADOR DESCIFRA EL MENSAJE USANDO R_SK
CONVENCIÓN: I_MESSAGE = MENSAJE DE PETICIÓN DEL INICIADOR,
R_MESSAGE = MENSAJE DE RESPUESTA DEL DESTINATARIO

FIG. 2


• H_1(INITIATOR_ID)
• H1(RESPONDER_ID)
• H1(RESPONDER1_ID)
• H1(RESPONDER2_ID)
• CLAVE PÚBLICA DEL INICIADOR (I_PK)
• CLAVE PÚBLICA DEL CONTESTADOR (R_PK)
• CLAVE PÚBLICA DEL CONTESTADOR1 (R1_PK)
• CLAVE PÚBLICA DEL CONTESTADOR2 (R2_PK)
EL CONTESTADOR 1 NO PUEDE DESCIFRAR ESTE MENSAJE PORQUE NO TIENE R2_SK
• R1_PK
• R_PK
• R1_SK
• R_SK
CONTESTADOR CONTESTADOR1
102-R1
TANTO CONTESTADOR1 COMO CONTESTADOR2 PUEDEN DESCIFRAR USANDO R_SK
• R2_PK
• R_PK
• R2_SK
• R_PK
102-R2
CONTESTADOR CONTESTADOR2
• I_PK
• I_SK
INICIADOR
102-I
210
• I_MESSAGE (I_ID, R_ID, aP)
212
• R_MESSAGE (I_ID, R_ID, R2_ID, aP, b2P)
214
• I_MESSAGE (I_ID, R2_ID, b2P)
216
• R_MESSAGE (VERIFICACIÓN)

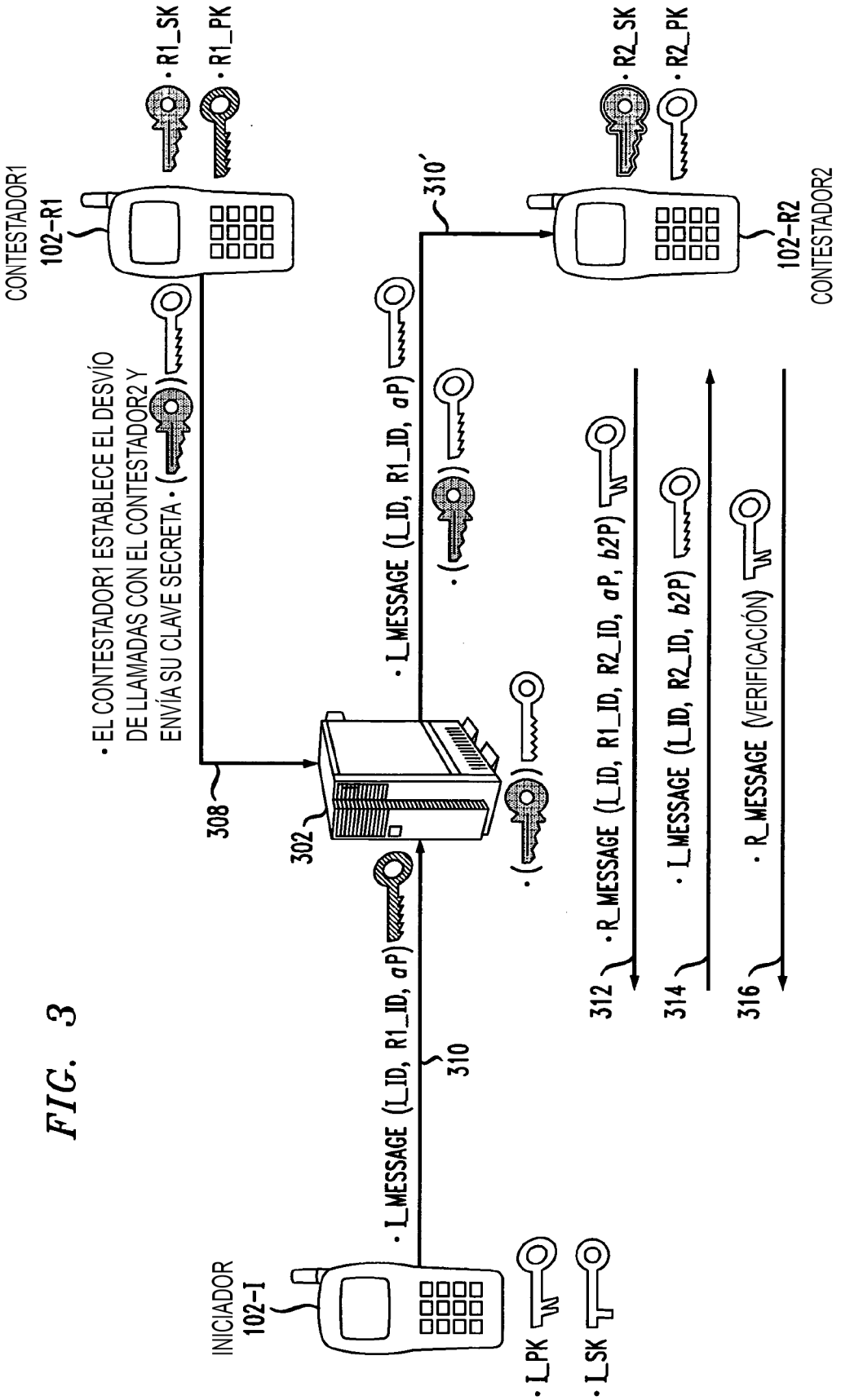

CONTESTADOR1
102-R1
• R1_SK
• R1_PK
• EL CONTESTADOR1 ESTABLECE EL DESVÍO DE LLAMADAS CON EL CONTESTADOR2 Y ENVÍA SU CLAVE SECRETA • (
308
302
• L_MESSAGE (L_ID, R1_ID, aP)
310'
• (
• (
• L_MESSAGE (L_ID, R1_ID, aP)
310
INICIADOR
102-I
• L_PK
• L_SK
• R_MESSAGE (L_ID, R1_ID, R2_ID, aP, b2P)
312
• L_MESSAGE (L_ID, R2_ID, b2P)
314
• R_MESSAGE (VERIFICACIÓN)
316
• R2_SK
• R2_PK
102-R2
CONTESTADOR2

FIG. 3

FIG. 4A

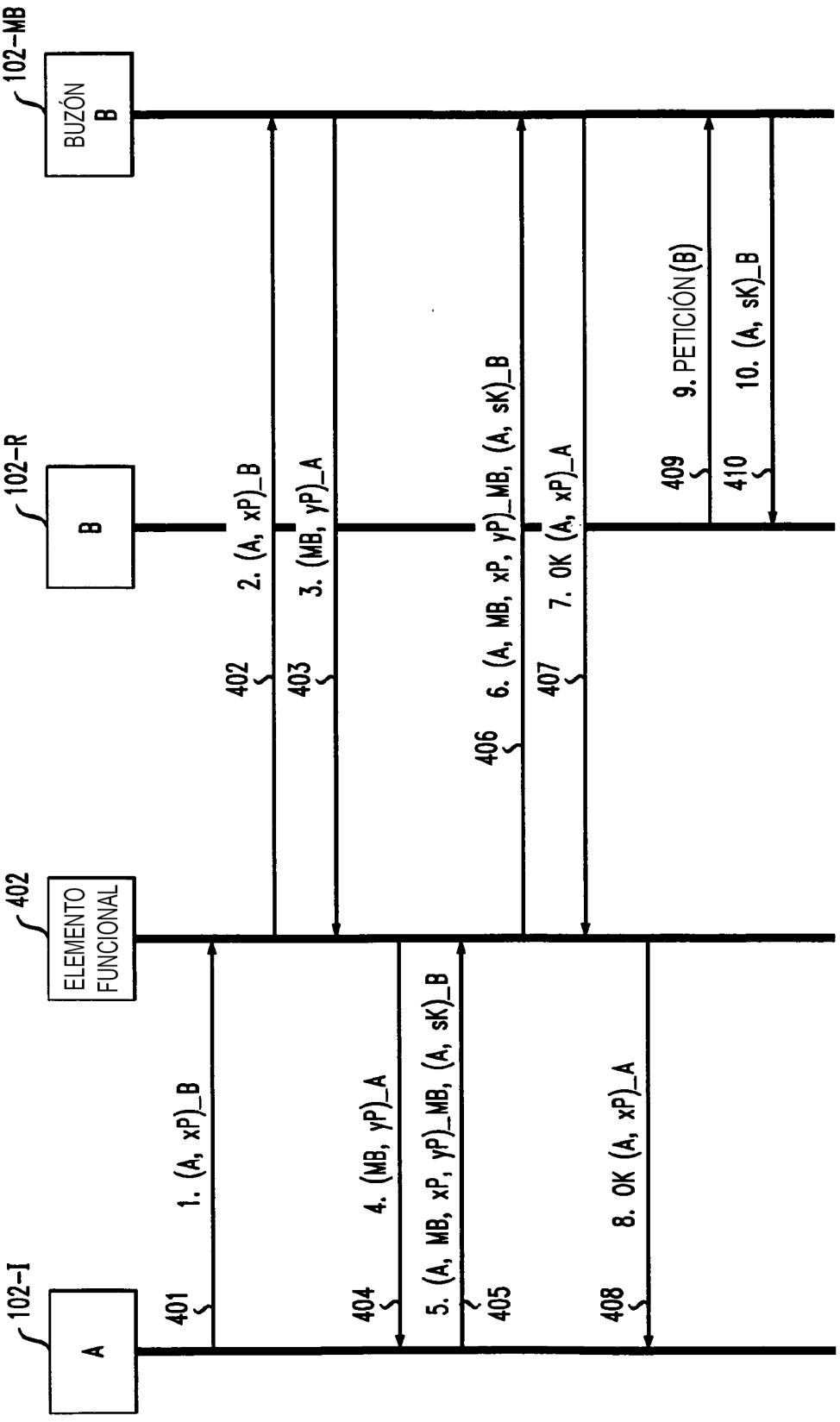

102-I
A
102-R
B
102-MB
BUZÓN B
402
ELEMENTO FUNCIONAL
401
1. (A, xP)_B
402
2. (A, xP)_B
403
3. (MB, yP)_A
404
4. (MB, yP)_A
405
5. (A, MB, xP, yP)_MB, (A, sK)_B
406
6. (A, MB, xP, yP)_MB, (A, sK)_B
407
7. OK (A, xP)_A
408
8. OK (A, xP)_A
409
9. PETICIÓN(B)
410
10. (A, sK)_B

FIG. 4B

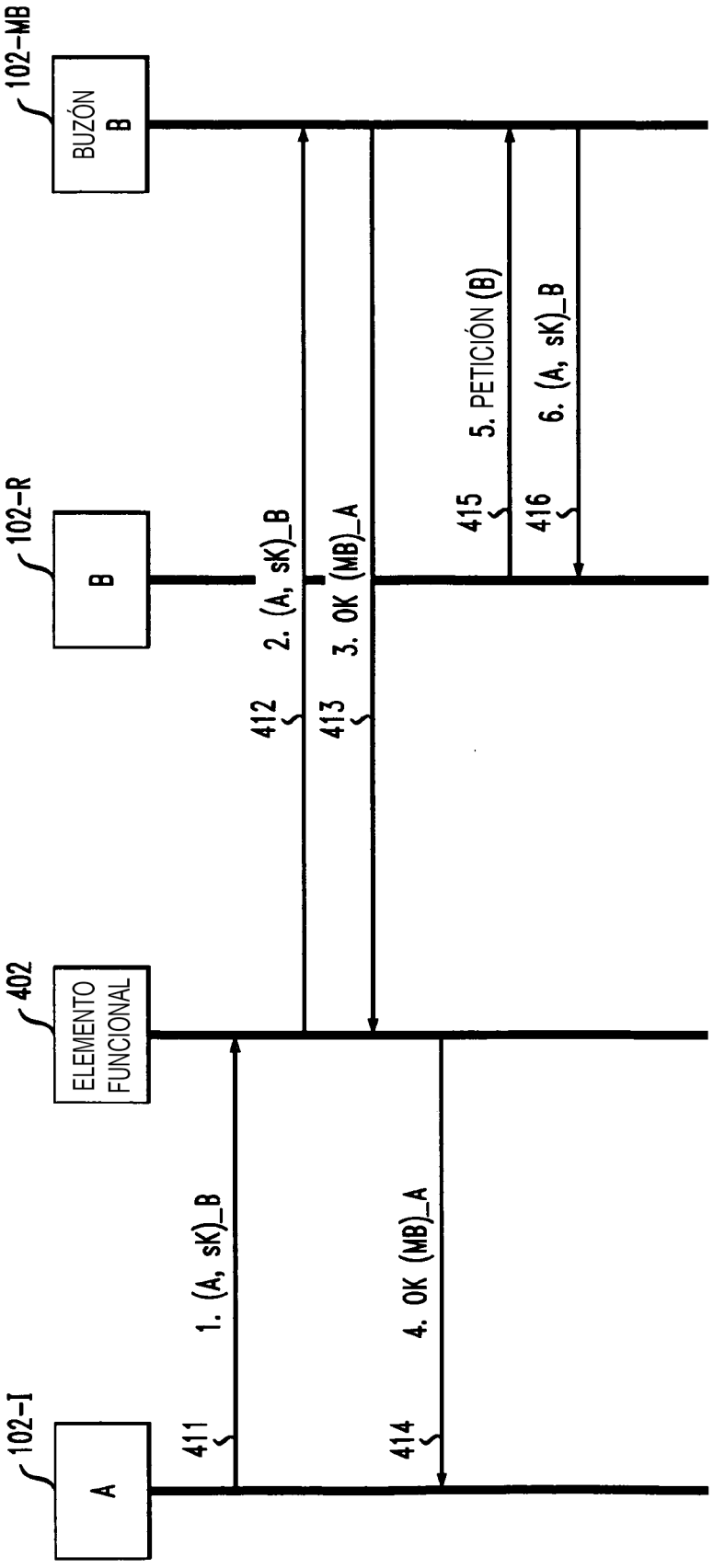

102-MB
BUZÓN B
102-R
B
402
ELEMENTO FUNCIONAL
102-I
A
411
1. (A, sK)_B
412
2. (A, sK)_B
413
3. OK (MB)_A
414
4. OK (MB)_A
415
5. PETICIÓN (B)
416
6. (A, sK)_B

FIG. 5

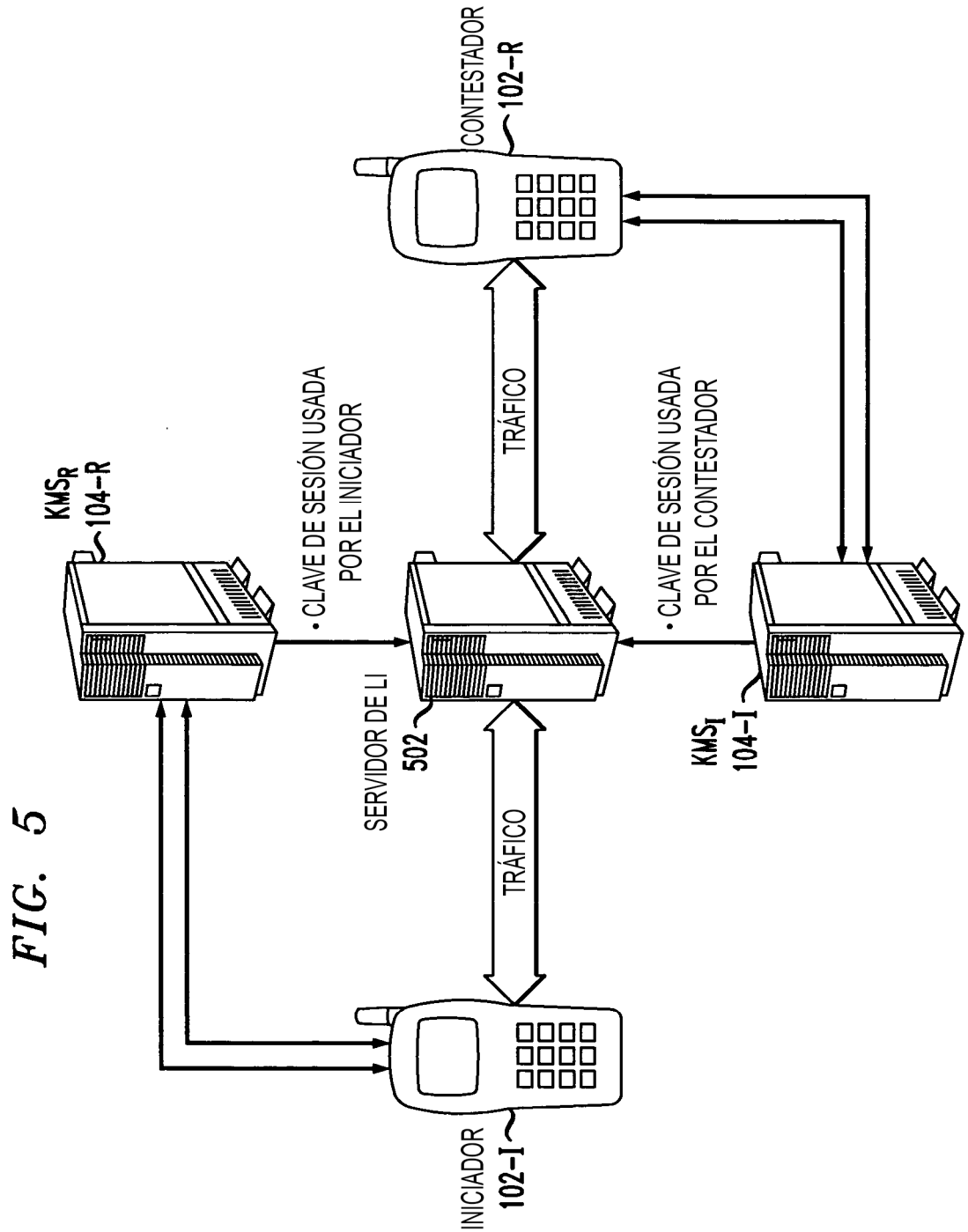

CONTESTADOR
102-R
TRÁFICO
• CLAVE DE SESIÓN USADA POR EL INICIADOR
• CLAVE DE SESIÓN USADA POR EL CONTESTADOR
KMS_R
104-R
SERVIDOR DE LI
502
KMS_I
104-I
TRÁFICO
INICIADOR
102-I

FIG. 6A

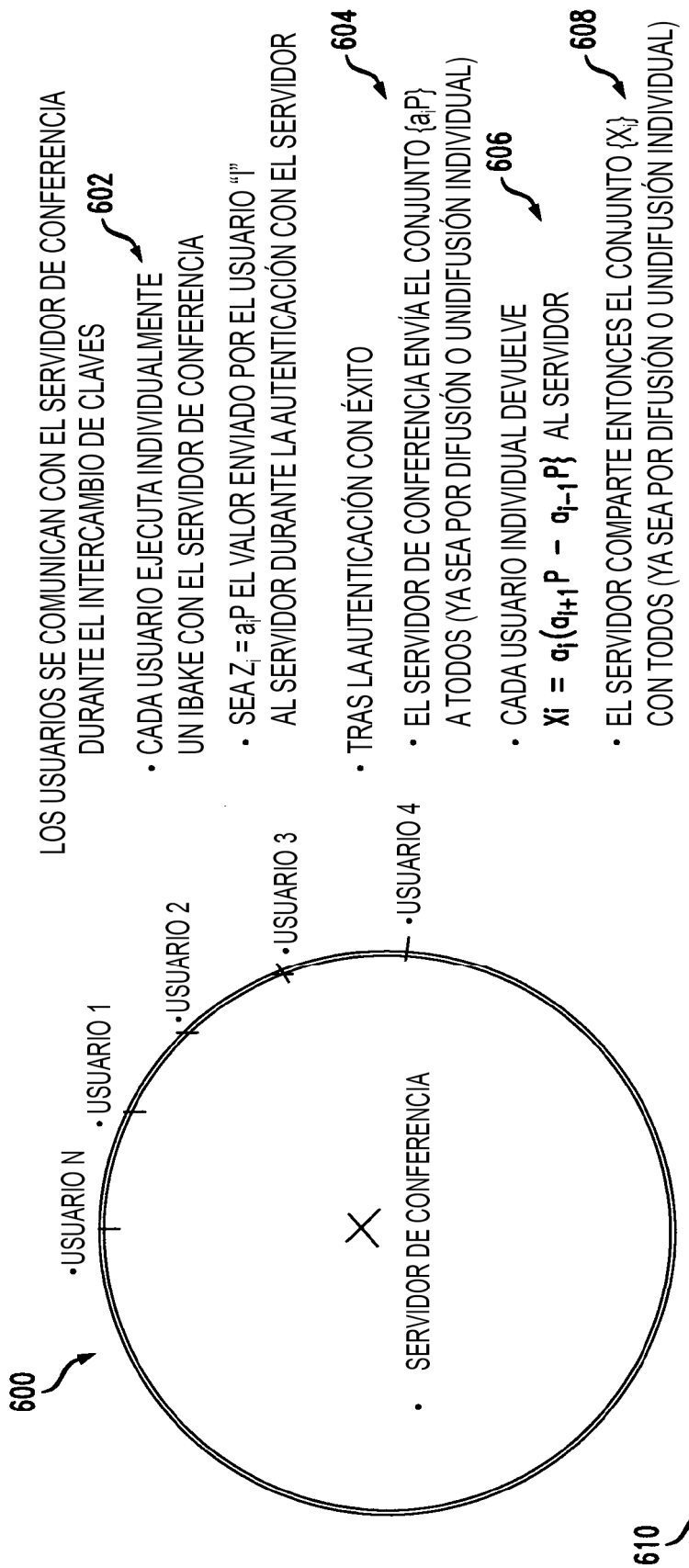
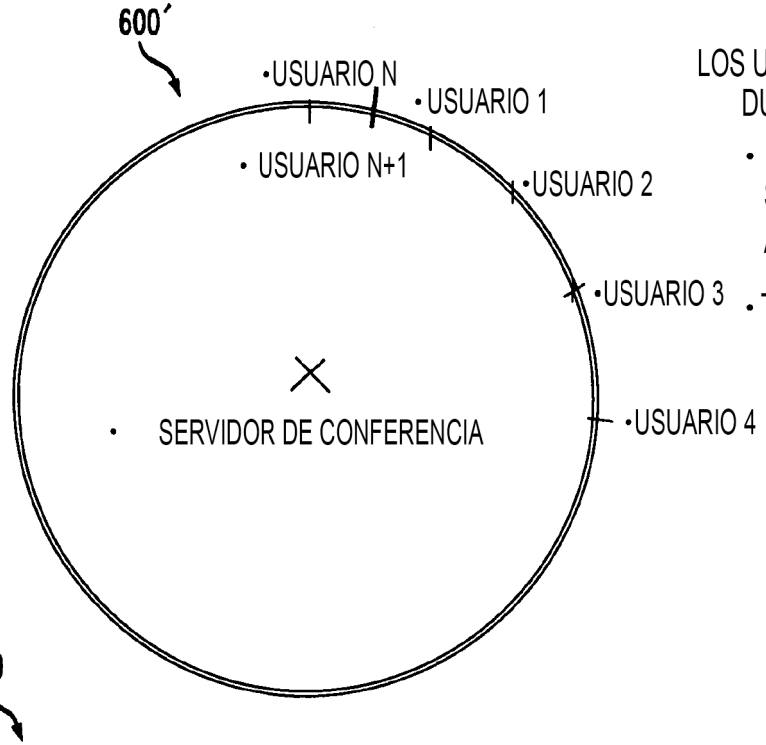

600
LOS USUARIOS SE COMUNICAN CON EL SERVIDOR DE CONFERENCIA DURANTE EL INTERCAMBIO DE CLAVES
602
• CADA USUARIO EJECUTA INDIVIDUALMENTE UN IBAKE CON EL SERVIDOR DE CONFERENCIA
• SEA $Z_i = a_iP$ EL VALOR ENVIADO POR EL USUARIO "i" AL SERVIDOR DURANTE LA AUTENTICACIÓN CON EL SERVIDOR
604
• TRAS LA AUTENTICACIÓN CON ÉXITO
• EL SERVIDOR DE CONFERENCIA ENVÍA EL CONJUNTO {a_iP} A TODOS (YA SEA POR DIFUSIÓN O UNIDIFUSIÓN INDIVIDUAL)
606
• CADA USUARIO INDIVIDUAL DEVUELVE $X_i = a_i(a_{i+1}P - a_{i-1}P)$ AL SERVIDOR
608
• EL SERVIDOR COMPARTE ENTONCES EL CONJUNTO {X_i} CON TODOS (YA SEA POR DIFUSIÓN O UNIDIFUSIÓN INDIVIDUAL)
610
• CLAVE DE GRUPO = $Na_i(Z_{i-1}) + (N-1)X_i+(N-2)X_{i+1}+....+X_{i-2}$
•USUARIO N
•USUARIO 1
•USUARIO 2
•USUARIO 3
•USUARIO 4
• SERVIDOR DE CONFERENCIA

FIG. 6B



LOS USUARIOS SE COMUNICAN CON EL SERVIDOR DE CONFERENCIA DURANTE EL INTERCAMBIO DE CLAVES

612

- EL USUARIO N+1 EJECUTA UN IBAKE CON EL SERVIDOR DE CONFERENCIA SEA $Z_{N+1} = a_{N+1}P$ EL VALOR ENVIADO POR EL USUARIO "N+1" AL SERVIDOR DURANTE LA AUTENTICACIÓN CON EL SERVIDOR
- TRAS LA AUTENTICACIÓN CON ÉXITO

614

- EL SERVIDOR DE CONFERENCIA ANUNCIA LA ADMISIÓN DEL NUEVO USUARIO N+1 Y ENVÍA EL CONJUNTO $\{a_iP\}$ A TODOS (YA SEA POR DIFUSIÓN O UNIDIFUSIÓN INDIVIDUAL), INCLUYENDO A Z_{N+1}

616

- LOS USUARIOS 1, N, N+1 DEVUELVEN $Xi = a_i(a_{j+1}P - a_{i-1}P\}$ AL SERVIDOR; ALTERNATIVAMENTE, TODOS PODRÍAN EJECUTAR ESTA ETAPA

618

- EL SERVIDOR COMPARTE ENTONCES EL CONJUNTO $\{X_i\}$ CON TODOS (YA SEA POR DIFUSIÓN O UNIDIFUSIÓN INDIVIDUAL), INCLUYENDO A X_{N+1}

- CLAVE DE GRUPO = $(N+1)a_i(Z_{i-1}) + (N)X_i+(N-1)X_{i+1}+....+X_{i-2}$
  - OBSÉRVESE QUE LA CLAVE DE GRUPO CAMBIA DESPUÉS DE QUE SE ADMITE UN NUEVO USUARIO

FIG. 6C

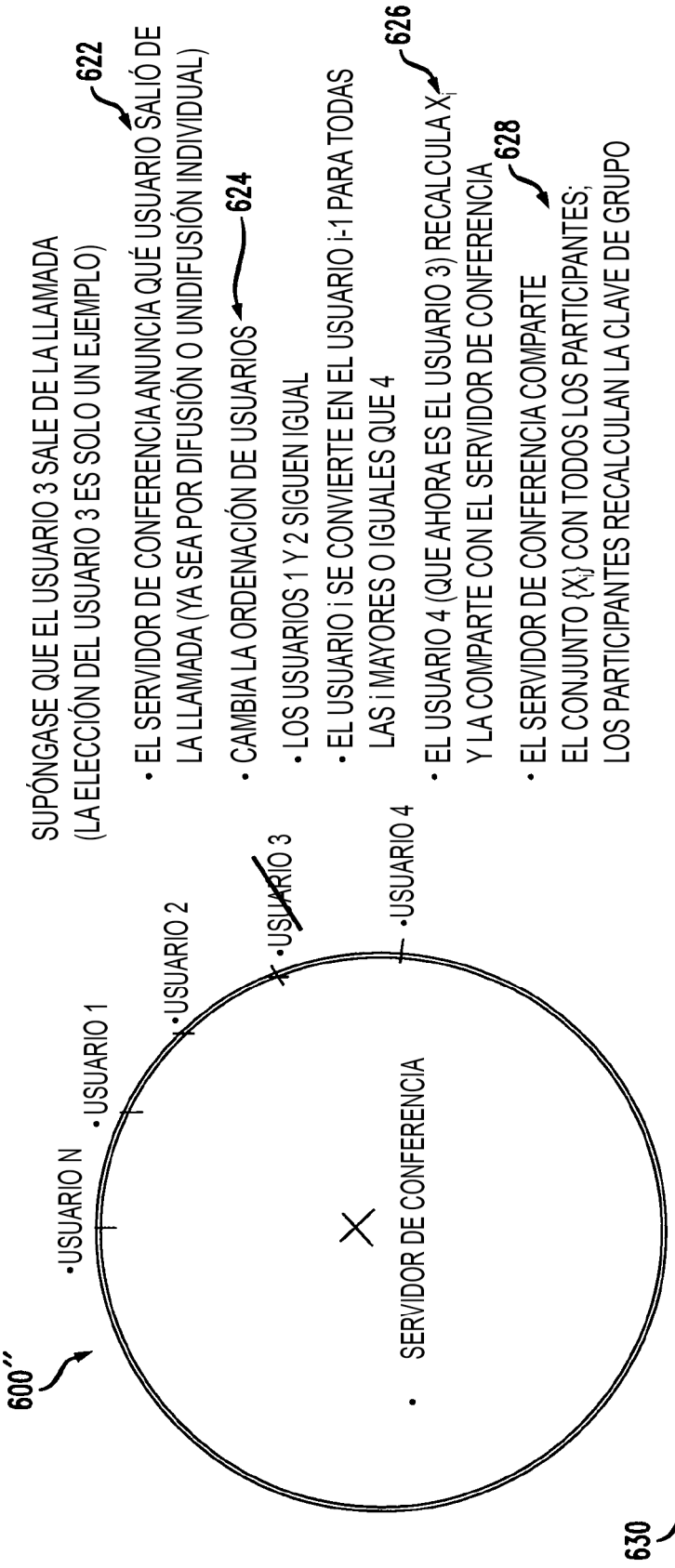

600''
SUPÓNGASE QUE EL USUARIO 3 SALE DE LA LLAMADA
(LA ELECCIÓN DEL USUARIO 3 ES SOLO UN EJEMPLO)
• EL SERVIDOR DE CONFERENCIA ANUNCIA QUÉ USUARIO SALIÓ DE LA LLAMADA (YA SEA POR DIFUSIÓN O UNIDIFUSIÓN INDIVIDUAL)
622
• CAMBIA LA ORDENACIÓN DE USUARIOS
624
• LOS USUARIOS 1 Y 2 SIGUEN IGUAL
• EL USUARIO i SE CONVIERTE EN EL USUARIO i-1 PARA TODAS LAS i MAYORES O IGUALES QUE 4
• EL USUARIO 4 (QUE AHORA ES EL USUARIO 3) RECALCULA X_i Y LA COMPARTE CON EL SERVIDOR DE CONFERENCIA
626
• EL SERVIDOR DE CONFERENCIA COMPARTE EL CONJUNTO {X_i} CON TODOS LOS PARTICIPANTES; LOS PARTICIPANTES RECALCULAN LA CLAVE DE GRUPO
628
• USUARIO N
• USUARIO 1
• USUARIO 2
• USUARIO 3
• USUARIO 4
• SERVIDOR DE CONFERENCIA
630
• CLAVE DE GRUPO = $(N-1)\alpha_1(Z_{i-1}) + (N-2)X_i+(N-3)X_{i+1}+....+X_{i-2}$
• OBSÉRVESE QUE LA CLAVE DE GRUPO CAMBIA DESPUÉS DE QUE UN PARTICIPANTE SALE DE LA LLAMADA

FIG. 7

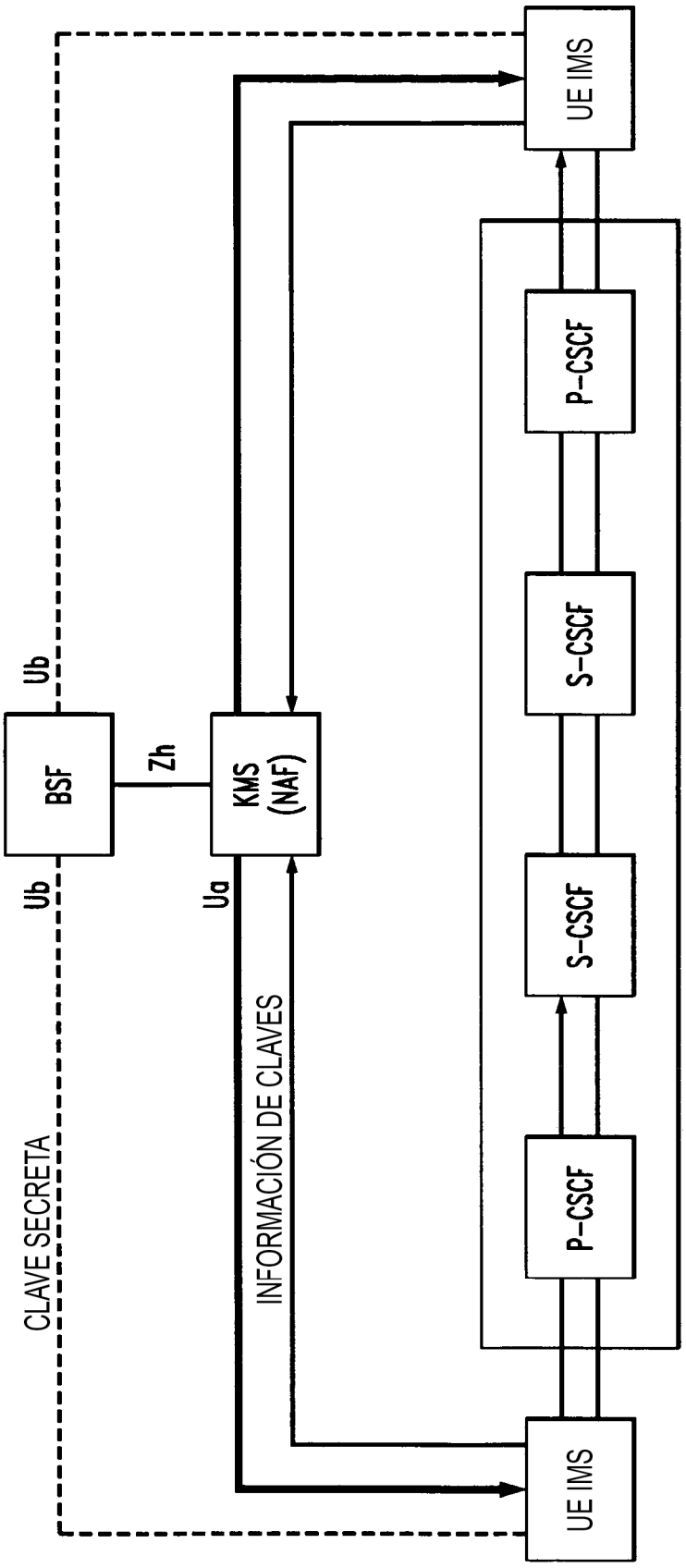

UE IMS
P-CSCF
S-CSCF
S-CSCF
P-CSCF
UE IMS
Ub
BSF
Zh
KMS (NAF)
Ub
Ua
CLAVE SECRETA
INFORMACIÓN DE CLAVES

FIG. 8

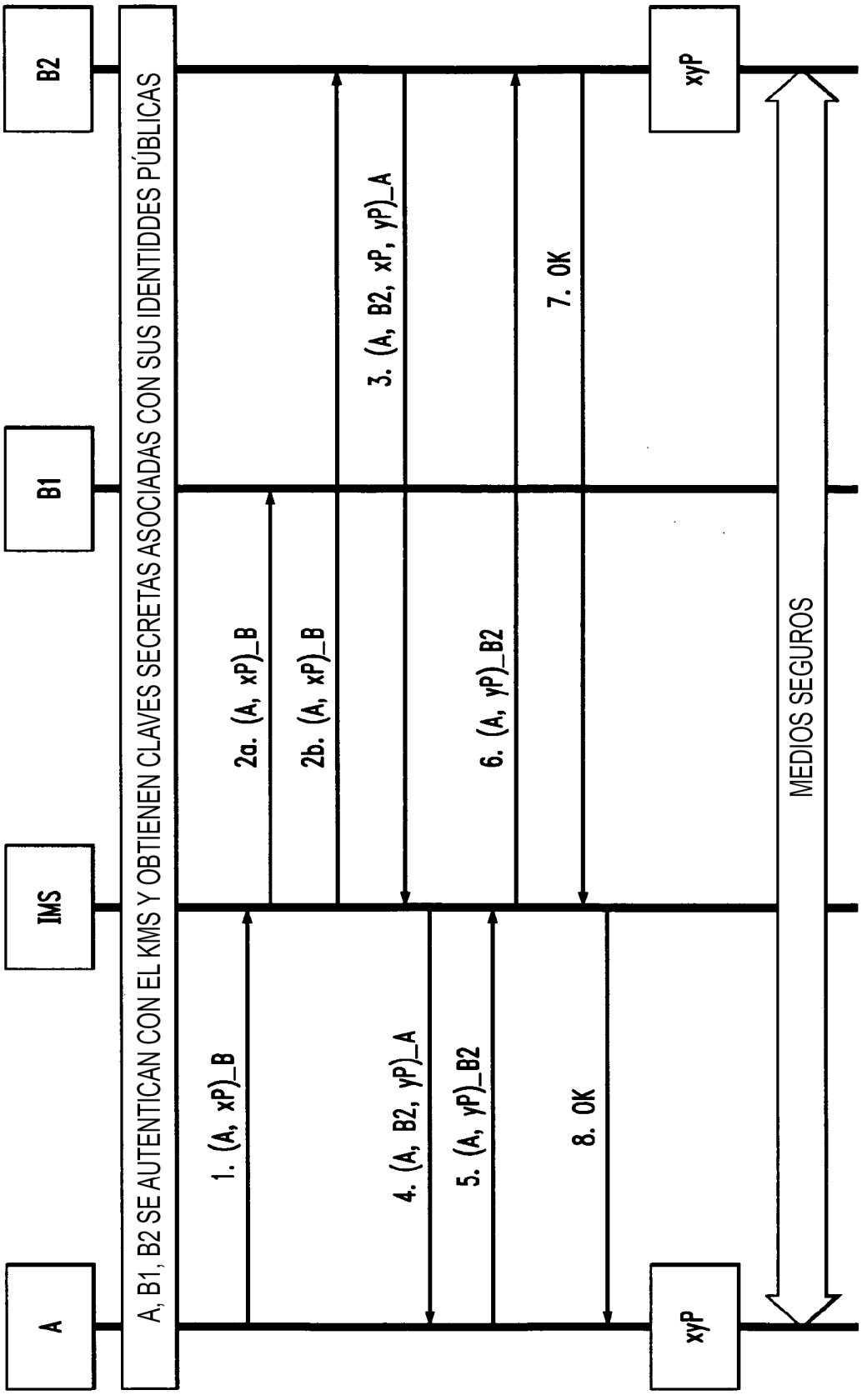

A
IMS
B1
B2
xyP
xyP
A, B1, B2 SE AUTENTICAN CON EL KMS Y OBTIENEN CLAVES SECRETAS ASOCIADAS CON SUS IDENTIDES PÚBLICAS
1. (A, xP)_B
2a. (A, xP)_B
2b. (A, xP)_B
3. (A, B2, xP, yP)_A
4. (A, B2, yP)_A
5. (A, yP)_B2
6. (A, yP)_B2
7. OK
8. OK
MEDIOS SEGUROS

FIG. 9

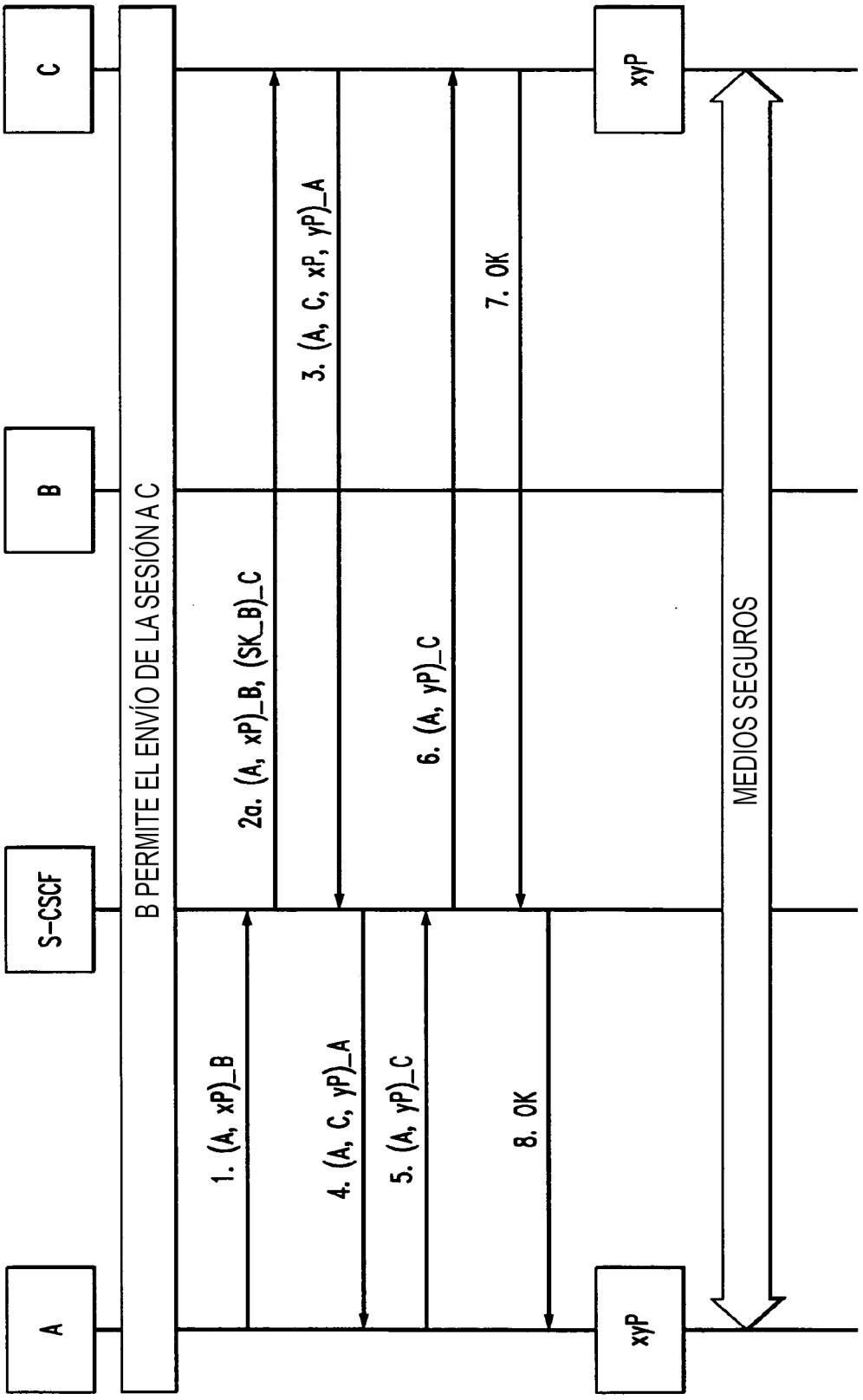

A
S-CSCF
B
C
xyP
xyP
B PERMITE EL ENVÍO DE LA SESIÓN A C
1. (A, xP)_B
2a. (A, xP)_B, (SK_B)_C
3. (A, C, xP, yP)_A
4. (A, C, yP)_A
5. (A, yP)_C
6. (A, yP)_C
7. OK
8. OK
MEDIOS SEGUROS

FIG. 10

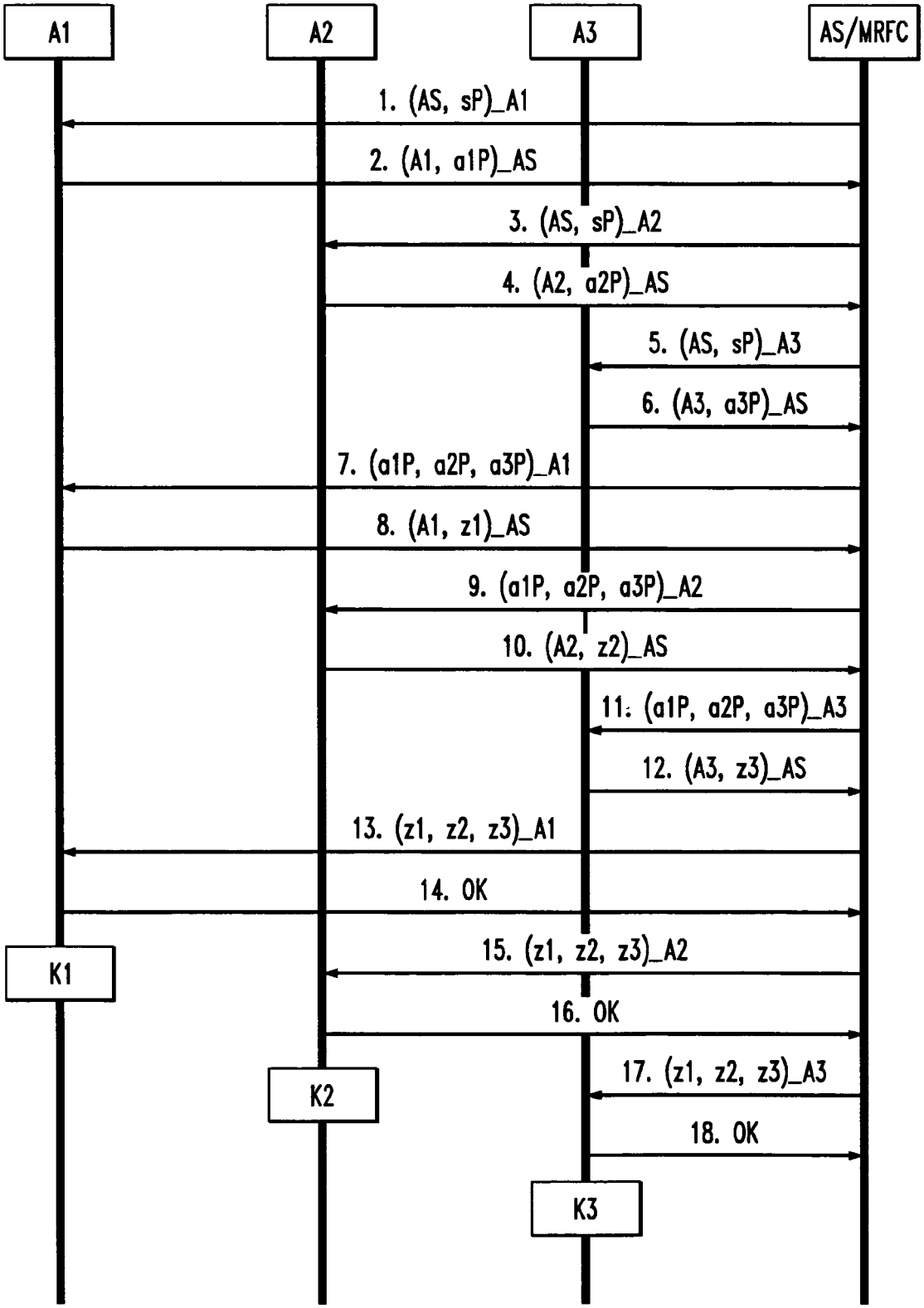
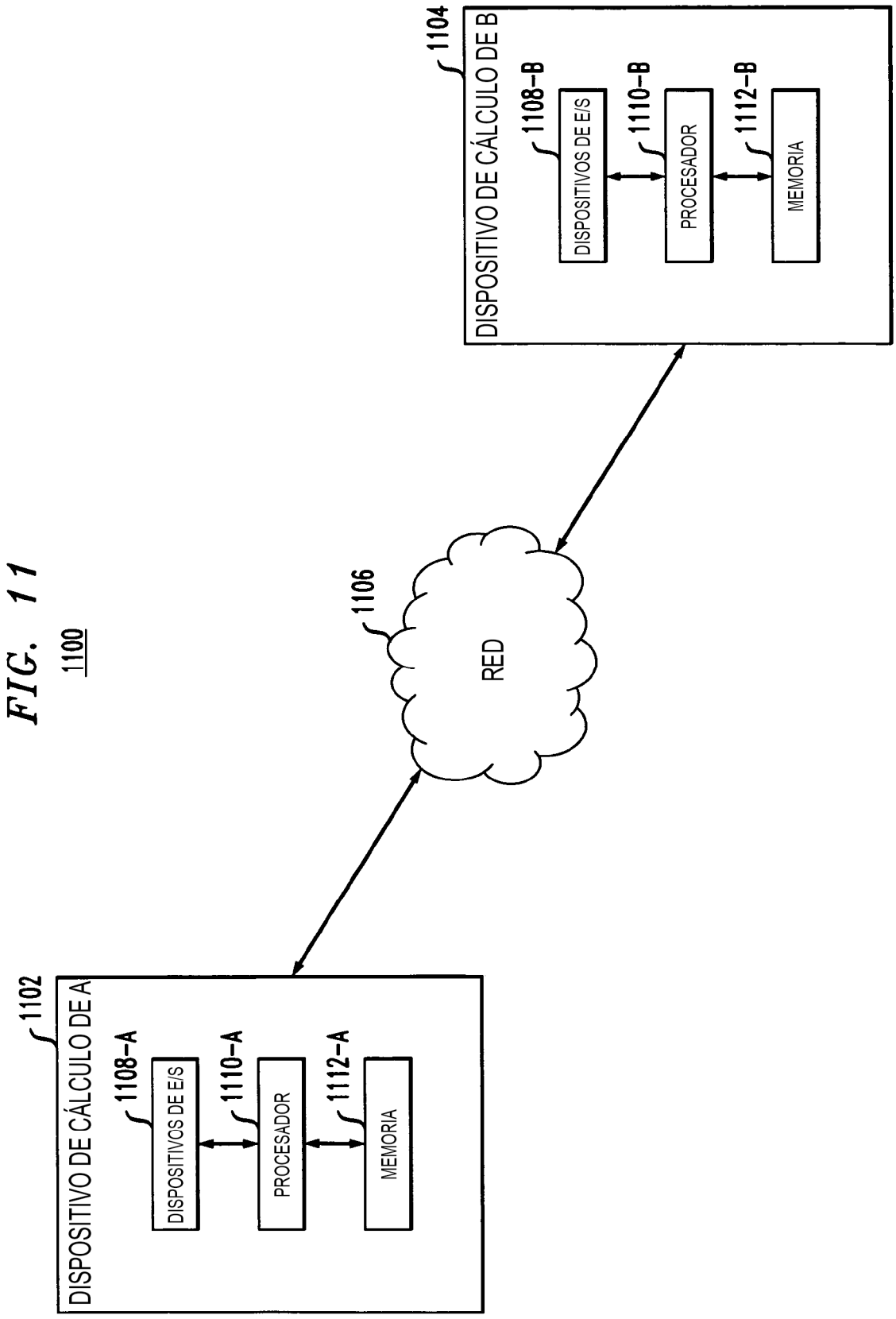

A1
A2
A3
AS/MRFC
1. (AS, sP)_A1
2. (A1, a1P)_AS
3. (AS, sP)_A2
4. (A2, a2P)_AS
5. (AS, sP)_A3
6. (A3, a3P)_AS
7. (a1P, a2P, a3P)_A1
8. (A1, z1)_AS
9. (a1P, a2P, a3P)_A2
10. (A2, z2)_AS
11. (a1P, a2P, a3P)_A3
12. (A3, z3)_AS
13. (z1, z2, z3)_A1
14. OK
15. (z1, z2, z3)_A2
16. OK
17. (z1, z2, z3)_A3
18. OK
K1
K2
K3

FIG. 11


1100
1102
DISPOSITIVO DE CÁLCULO DE A
1108-A
DISPOSITIVOS DE E/S
1110-A
PROCESADOR
1112-A
MEMORIA
1106
RED
1104
DISPOSITIVO DE CÁLCULO DE B
1108-B
DISPOSITIVOS DE E/S
1110-B
PROCESADOR
1112-B
MEMORIA