(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 623 796**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.03.2010 PCT/CN2010/071186**

(87) Fecha y número de publicación internacional: **29.12.2010 WO10148672**

(96) Fecha de presentación y número de la solicitud europea: **22.03.2010 E 10791178 (6)**

(97) Fecha y número de publicación de la concesión europea: **01.03.2017 EP 2448172**

(54) Título: **Método y Sistema para retrasar la transmisión de información de medios en un Subsistema Multimedia por Protocolo de Internet (IP)**

(30) Prioridad:

26.06.2009 CN 200910142257

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.07.2017

(73) Titular/es:

ZTE CORPORATION (100.0%)
ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District
Shenzhen, Guangdong 518057, CN

(72) Inventor/es:

TIAN, TIAN;
ZHU, YUNWEN;
WEI, YINXING y
TENG, ZHIMENG

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Método y Sistema para retrasar la transmisión de información de medios en un Subsistema Multimedia por Protocolo de Internet (IP).

Campo de la invención

La presente invención se refiere al campo de las comunicaciones, y, en particular, a un método y un sistema para transmitir la información de medios en diferido en un Subsistema Multimedia por Protocolo de Internet (IP).

Antecedentes de la invención

En la tecnología de seguridad de medios del Subsistema Multimedia por IP (IMS) se proponen requisitos para el envío de información de medios en diferido al buzón de medios de la parte receptora. En general, esta situación se produce cuando la parte emisora (usuario A) envía la información de medios a la parte receptora (usuario B), y el usuario B se encuentra en un estado fuera de línea (pueden ser muchos los motivos que den como resultado que el usuario B esté fuera de línea, por ejemplo que el mismo deje de funcionar, que no haya iniciado una sesión, que se encuentre fuera del área de servicio, etcétera). En esta situación, debido a la indisponibilidad del usuario B, no puede utilizarse el mecanismo de negociación de claves que requiere que las dos partes estén en línea, y debe introducirse un Servidor de Gestión de Claves (KMS), en calidad de tercero de confianza, para lograr que las partes en comunicación puedan obtener la clave de medios compartida, a través de un modo asíncrono.

En la actualidad, en cuanto al envío seguro de la información de medios en diferido, existen dos soluciones en los documentos técnicos en relación con la seguridad de los medios del Subsistema Multimedia por IP (IMS): una de ellas se basa en un Sistema Basado en Tiques (TBS), y la otra se basa en el protocolo de Otway Rees (este es un protocolo de autenticación y de intercambio de códigos). No obstante, tanto una como otra de entre las dos técnicas anteriores presentan defectos, los cuales se describirán respectivamente en lo sucesivo en la presente de forma detallada.

La Fig. 1 es un diagrama esquemático de una infraestructura de las soluciones para la seguridad del plano de medios en el IMS basadas en el TBS y el protocolo de Otway Rees en la técnica anterior, en la que

el usuario A (UE-A) y el usuario B (UE-B) son respectivamente la parte emisora y la parte receptora de la información de medios;

el Servidor de Gestión de Claves (KMS) es un tercero de confianza que lleva a cabo la función de gestión y distribución de claves;

la P-CSCF (Función de Control de Sesión de Llamada Proxy) y la S-CSCF (Función de Control de Sesión de Llamada de Servicio) son elementos de red del IMS; y

en el presente documento no se describen de forma detallada funciones de otros elementos de red de la Fig. 1. Consúltense otros documentos relacionados.

La Fig. 2 es un diagrama de flujo de un método para establecer un canal de medios entre la parte llamante (usuario A) y la parte a la que se llama (usuario B), sobre la base de la infraestructura mostrada en la Fig. 1. Tal como se muestra en la Fig. 2, es necesario ejecutar las siguientes etapas con el fin de establecer el canal de medios seguro entre el usuario A y el usuario B, y para enviar la información de medios a través del canal de medios.

Etapa 201, el usuario A y el usuario B establecen respectivamente una conexión protegida con el KMS en un modo de Arquitectura de Inicialización Genérica.

En caso de que no pueda utilizarse la GBA, el usuario A y el usuario B pueden establecer una conexión protegida con el KMS basándose en otros métodos de autenticación.

Etapa 202, el usuario A envía una solicitud para demandar una clave de medios y un tique al KMS.

Etapa 203, el KMS genera la clave de medios y el tique, y devuelve la clave de medios y el tique al usuario A.

Etapa 204, el usuario A envía un mensaje INVITE que comprende el tique, al usuario B, a través de la red del IMS.

Etapa 205, después de recibir el mensaje INVITE que comprende el tique, la red del IMS envía el mensaje INVITE al usuario B,

en donde los elementos autorizados en la red del IMS pueden enviar el tique al KMS para obtener la clave de medios.

Etapa 206, después de recibir el mensaje INVITE, el usuario B envía el tique comprendido en el mensaje INVITE, al KMS, para obtener la clave de medios.

Etapa 207, el KMS verifica la identidad del usuario B. Después de que se haya aprobado la verificación, el KMS extrae la clave de medios y la envía al usuario B.

Etapa 208, el usuario B acepta satisfactoriamente la solicitud de llamada del usuario A.

Lo anteriormente mencionado es el proceso en el que la parte llamante (usuario B) se encuentra en el estado en línea. Cuando el usuario B está fuera de línea, lo cual significa que se encuentra en unas circunstancias en la que se emite información de medios en diferido, no se proporciona en ningún documento pertinente ningún método de implementación detallado. En la técnica anterior se aportan únicamente un diagrama esquemático de una infraestructura de una solución de seguridad para la información de medios en diferido en el IMS, tal como se muestra en la Fig. 3, y una breve introducción. La breve introducción es la siguiente.

En primer lugar, el usuario A envía el tique al servidor de buzón del usuario B, a través de un mensaje INVITE, y, a continuación, el usuario A envía la información de medios al servidor del buzón del usuario B. Cuando el usuario B inicia una sesión, el usuario B obtiene el tique a partir del servidor de buzón, y a continuación, envía el tique al KMS. Seguidamente, el KMS envía la clave de medios al usuario B.

Resumiendo, el envío de información de medios en diferido se puede lograr a través del TBS, aunque el método de implementación es relativamente complicado, es decir, con independencia de si el usuario B ha iniciado sesión, tanto el usuario A como el usuario B tienen que interaccionar con el KMS.

En comparación con la solución basada en el TBS, la solución basada en el protocolo de Otway Rees de la seguridad de los medios en el IMS, utiliza una infraestructura de red similar, y reduce la interacción de señalización con el KMS. Sin embargo, puesto que, en la solución basada en el protocolo de Otway Rees, la clave de medios se puede utilizar repetidamente, es necesario que el KMS almacene la clave de medios generada, lo cual provocará un problema en relación con la característica de funcionamiento por estados del KMS (concretamente, el problema de que el KMS no puede dar respuesta al excesivo requisito de almacenamiento). Otro defecto de la solución basada en el protocolo de Otway Rees es que, si se produce la expiración de la clave compartida entre la parte emisora y el KMS, después de un inicio de sesión la parte receptora obtiene la información cifrada con la clave cuya expiración se ha producido, y reenvía esta información al KMS, y a continuación el KMS no puede descifrar la información cifrada. Por lo tanto, el KMS no puede regenerar la clave de medios de acuerdo con la información en esta situación. Como consecuencia, la parte receptora no puede obtener la clave de medios, y no puede descifrar la información de medios cifrada para obtener la información de medios.

La publicación de solicitud de patente US n.º 2003/0147536 A1, de D.E. Andivahis et al, publicada el 7 de agosto de 2003, da a conocer un sistema de mensajería electrónica segura a través del uso auditable de pares de claves privada/pública.

La publicación de solicitud de patente US n.º 2008/0165972 A1, de C.A. Worthington, publicada el 10 de julio de 2008, da a conocer un método de cifrado de correos electrónicos.

El documento “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage”, publicado por G. Ateniese *et al.*, el 11 de enero de 2006, para la *International Association for Cryptologic Research*, da a conocer un esquema de re-cifrado proxy que permite que un destinatario use su clave secreta para abrir un texto cifrado calculado bajo la clave pública de otra entidad.

Sumario de la invención

La presente invención supera los defectos de la técnica anterior al proporcionar un método y un sistema para transmitir información de medios en diferido en el Subsistema Multimedia por IP, con el resultado de que no es necesario que el KMS almacene y mantenga la clave de medios generada.

Para resolver el problema antes mencionado, la presente invención proporciona un método para transmitir información de medios en diferido en el Subsistema Multimedia por IP. Este método comprende:

una parte emisora de la información de medios envía parámetros de generación de clave cifrados usando una Ka, a un servidor de buzón de una parte receptora de la información de medios; guardando el servidor de buzón los parámetros de generación de clave cifrados, y enviando los parámetros de generación de clave cifrados a un Servidor de Gestión de Claves (KMS); en donde la Ka es una clave compartida de la parte emisora y el KMS;

el KMS obtiene parámetros de generación de clave a través de un descifrado usando la Ka correspondiente, genera la clave de medios K con los parámetros generados de clave, y reenvía la K a la parte emisora a través del servidor de buzón de la parte receptora;

la parte receptora obtiene los parámetros de generación de clave cifrados provenientes del servidor de buzón, y, a continuación, envía los parámetros de generación de clave cifrados, obtenidos, al KMS;

el KMS obtiene los parámetros de generación de clave usando Ka para descifrar los parámetros de generación de clave cifrados, enviados por la parte receptora, y a continuación, genera la K con los parámetros de generación de clave y envía la K a la parte receptora; y

la parte receptora obtiene la información de medios cifrada por la parte emisora con la K, del servidor de buzón, y, a continuación, descifra la información de medios cifrada usando la K.

Además, antes de enviar la K a la parte emisora, el KMS también cifra la Ka usando una clave privada Kkms, y, a continuación, envía la Ka cifrada al servidor de buzón para que sea guardada;

cuando la parte receptora obtiene del servidor de buzón los parámetros de generación de clave cifrados, el servidor de buzón también envía la Ka cifrada a la parte receptora; cuando la parte receptora envía los parámetros de generación de clave cifrados al KMS, la parte receptora también envía la Ka cifrada al KMS; y

después de recibir la Ka cifrada, el KMS obtiene la Ka a través de un descifrado usando la Kkms.

Además, en la etapa en la que los parámetros de generación de clave cifrados se envían al KMS, la parte emisora envía los parámetros de generación de clave cifrados al KMS en las siguientes etapas: la parte emisora envía los parámetros de generación cifrados, dentro del mensaje de solicitud de llamada, al servidor de buzón; el servidor de buzón guarda los parámetros de generación de clave cifrados, y, a continuación, envía el mensaje de solicitud de obtención de clave de medios que comprende los parámetros de generación de clave cifrados, al KMS; y

antes de la etapa en la que la clave de medios K se genera con los parámetros de generación de clave, el método comprende además la siguiente etapa: el KMS verifica el identificador de la parte emisora, el identificador de la parte receptora y el identificador del servidor de buzón, y la K que se va a generar, únicamente después de que se hayan aprobado todas las verificaciones.

Adicionalmente, en la etapa en la que K se reenvía a la parte emisora a través del servidor de buzón de la parte receptora, el KMS envía la K a la parte emisora en las siguientes etapas:

el KMS cifra la K generada con la Ka, y, a continuación, envía la K cifrada al servidor de buzón;

el servidor de buzón envía la K cifrada dentro del mensaje de respuesta de llamada a la parte emisora; y

el método comprende además la etapa en la que la parte emisora obtiene la K a través de un descifrado usando la Ka.

Adicionalmente, en la etapa en la que K se envía a la parte receptora, el KMS envía la K a la parte receptora en las siguientes etapas:

el KMS cifra la K generada con una clave Kb compartida con la parte receptora, y, a continuación, envía la K cifrada a la parte receptora, y

el método comprende además la etapa en la que la parte receptora obtiene la K a través de un descifrado usando la Kb.

Adicionalmente, los parámetros de generación de clave cifrados comprenden un número aleatorio generado por la parte emisora y/o un cuanto de tiempo.

Además, el mensaje de solicitud de llamada comprende: textos en claro del identificador de la parte emisora y el identificador de la parte receptora, y texto cifrado del identificador de la parte emisora y el identificador de la parte receptora, cifrado con la Ka; y

el mensaje de solicitud de obtención de la clave de medios comprende: textos en claro del identificador de la parte emisora y el identificador de la parte receptora, textos cifrados del identificador de la parte emisora y el identificador de la parte receptora, cifrados con la Ka, y textos cifrados del identificador de la parte emisora y el identificador del servidor de buzón, cifrados con una clave Km compartida por el servidor de buzón y el KMS; y

en la etapa de verificación, el KMS verifica el identificador de la parte emisora, el identificador de la parte receptora y el identificador del servidor de buzón en las siguientes etapas: verificar si el identificador de la parte emisora obtenido a través del descifrado es idéntico al texto en claro del identificador de la parte emisora; verificar si el identificador de la parte receptora obtenido a través del descifrado es idéntico al texto en claro del identificador de la parte receptora; y verificar si el identificador del servidor de buzón obtenido a través del descifrado es idéntico al identificador del servidor de buzón correspondiente al identificador de la parte receptora.

La presente invención proporciona también un sistema para transmitir información de medios en diferido en un Subsistema Multimedia por IP, y el sistema comprende una parte emisora de información de medios, una parte receptora de la información de medios, un Servidor de Gestión de Claves (KMS) y un servidor de buzón de la parte receptora de la información de medios, en el que

la parte emisora está configurada para enviar parámetros de generación de clave cifrados con una Ka al servidor de buzón; el servidor de buzón guarda los parámetros de generación de clave cifrados, y, a continuación, envía los parámetros de generación de clave cifrados al KMS, siendo la Ka una clave compartida de la parte emisora y el KMS;

el KMS está configurado para obtener los parámetros de generación de clave usando la Ka correspondiente para descifrar, para generar una clave de medios K con los parámetros de generación de clave descifrados, y para enviar la K a la parte emisora;

la parte receptora está configurada para obtener del servidor de buzón los parámetros de generación de clave cifrados, y, a continuación, para enviar al KMS los parámetros de generación de clave cifrados, obtenidos;

después de recibir los parámetros de generación de clave cifrados, enviados por la parte receptora, el KMS está configurado además para obtener los parámetros de generación de clave usando la Ka con el fin de descifrar los parámetros de generación de clave cifrados, para generar la K con los parámetros de generación de clave descifrados y enviar la K a la parte receptora; y

la parte receptora está configurada además para obtener la información de medios cifrada por la parte emisora con la K del servidor de buzón, y, a continuación, para descifrar la información de medios cifrada usando la K.

Además, antes de que se envíe la K a la parte emisora, el KMS está configurado además para cifrar la Ka usando la clave privada Kkms, y, a continuación, para enviar la Ka cifrada al servidor de buzón para que sea guardada;

cuando la parte receptora obtiene los parámetros de generación de clave cifrados del servidor de buzón, el servidor de buzón está configurado además para enviar la Ka cifrada a la parte receptora, y la parte receptora está configurada además para enviar la Ka cifrada y los parámetros de generación de clave cifrados al KMS; y

después de recibir la Ka cifrada, el KMS está configurado además para obtener la Ka a través de un descifrado usando la Kkms.

Adicionalmente, la parte emisora está configurada además para generar un número aleatorio y/o una marca de tiempo, y para cifrar el número aleatorio y/o la marca de tiempo generados usando la Ka, y, a continuación, para enviar el número aleatorio y/o la marca de tiempo generados, cifrados, al KMS a través del servidor de buzón, como parámetros de generación de clave cifrados.

La presente invención proporciona también un terminal emisor para transmitir información de medios en diferido en un Subsistema Multimedia por IP.

El terminal emisor está configurado para enviar parámetros de generación de clave cifrados con una Ka a un servidor de buzón de una parte receptora, de manera que el servidor de buzón puede guardar los parámetros de generación de clave cifrados y enviar los parámetros de generación de clave a un Servidor de Gestión de Claves (KMS);

el terminal emisor está configurado además para recibir una clave de medios K enviada por el KMS a través del servidor de buzón del terminal receptor, en donde la K es la clave de medios generada con los parámetros de generación de clave que obtiene el KMS usando la Ka correspondiente para descifrar los parámetros de generación de clave cifrados, recibidos; la Ka es la clave compartida del terminal emisor y el KMS; y

el terminal emisor está configurado además para cifrar la información de medios con la K con el fin de transmitir la información de medios.

Adicionalmente, el terminal emisor está configurado además para generar un número aleatorio y/o una marca de tiempo, y para cifrar el número aleatorio y/o la marca de tiempo generados usando la Ka, y, a continuación, para

enviar el número aleatorio y/o la marca de tiempo generados, cifrados, al KMS a través del servidor de buzón, como parámetros de generación de clave cifrados.

La presente invención proporciona también un Servidor de Gestión de Claves (KMS) para transmitir información de medios en diferido en un Subsistema Multimedia por IP, en el que

el KMS está configurado para:

recibir parámetros de generación de clave cifrados, enviados por un servidor de buzón de una parte receptora, estando los parámetros de generación de clave cifrados cifrados con una Ka y son enviados por un terminal emisor al servidor de buzón para que sean guardados en el servidor de buzón;

obtener los parámetros de generación de clave usando la Ka correspondiente para descifrar; generar una clave de medios K con los parámetros de generación de clave descifrados, y enviar la K al terminal emisor a través del servidor de buzón del terminal receptor; la Ka es la clave compartida del terminal emisor y el KMS;

recibir los parámetros de generación de clave cifrados, enviados por el terminal receptor, y los parámetros de generación de clave cifrados son obtenidos por el terminal receptor a partir del servidor de buzón; y

obtener los parámetros de generación de clave usando la Ka para descifrar los parámetros de generación de clave cifrados, recibidos del terminal receptor, y generar la K con los parámetros de generación de clave, y enviar la K al terminal receptor.

Además, el KMS está configurado además para cifrar la Ka usando una clave privada Kkms, y a continuación para enviar la Ka cifrada al servidor de buzón para que se guarde en el servidor; y

el KMS está configurado además para recibir la Ka cifrada, enviada por el terminal receptor, en donde la Ka cifrada se envía al terminal receptor a través del servidor de buzón, mientras que el terminal receptor envía los parámetros de generación de clave cifrados al KMS.

Además, el KMS está configurado además para cifrar la K generada usando una clave Kb compartida con el terminal receptor antes de enviar la K al terminal receptor, y, a continuación, para enviar la K cifrada al terminal receptor.

Además, el KMS está configurado además para verificar el identificador de la parte emisora, el identificador de la parte receptora y el identificador del servidor de buzón, y la K se generará únicamente después de que se haya aprobado la verificación.

La presente invención proporciona también un terminal receptor para transmitir información de medios en diferido en un Subsistema Multimedia por IP.

El terminal receptor está configurado para:

obtener parámetros de generación de clave cifrados, que se han cifrado con una clave Ka de un servidor de buzón, la cual es enviada por un terminal emisor al servidor de buzón, siendo la Ka la clave compartida del terminal emisor y un Servidor de Gestión de Claves (KMS);

enviar los parámetros de generación de clave cifrados, obtenidos, al KMS;

recibir una clave K, siendo la K enviada por el KMS y se genera con los parámetros de generación de clave que obtiene el KMS usando la Ka para descifrar los parámetros de generación de clave cifrados, después de recibir los parámetros de generación de clave cifrados enviados por el terminal receptor; y

obtener la información de medios cifrada por el terminal emisor con la K del servidor de buzón, y, a continuación, descifrar la información de medios cifrada usando la K.

Además, el terminal receptor está configurado además para obtener la K usando una clave Kb compartida con el KMS, y antes de que la K se envíe al terminal receptor, el KMS está configurado además para cifrar la K generada usando la Kb.

En resumen, en comparación con la técnica anterior, después de que se obtenga la clave compartida, la presente invención reduce la interacción de señalización entre la parte emisora de la información de medios y el KMS, consigue que disminuya la presión de almacenamiento del KMS, resuelve el problema provocado por la expiración de la clave compartida entre la parte emisora de la información de medios y el KMS, y logra el envío seguro de la información de medios en diferido en el IMS.

Breve descripción de los dibujos

La Fig. 1 es un diagrama esquemático de una infraestructura de las soluciones basadas en el TBS y el protocolo de Otway Rees, para la seguridad de los medios en el IMS en la técnica anterior.

La Fig. 2 es un diagrama de flujo de un método para establecer un canal de medios entre la parte llamante y la parte a la que se llama sobre la base de la infraestructura mostrada en la Fig. 1;

la Fig. 3 es un diagrama esquemático de una infraestructura de una solución para la seguridad de la información de medios en diferido en el IMS en la técnica anterior;

la Fig. 4 es un diagrama de flujo de un método para negociar una clave entre la parte emisora de información de medios en diferido y el servidor de buzón de la parte receptora de información de medios en diferido, basándose en el KMS, de acuerdo con la forma de realización de la presente invención;

la Fig. 5 es un diagrama de flujo de un método para obtener la clave de medios a través de la parte receptora (usuario B) de información de medios en diferido, que interacciona con el servidor de buzón de la parte receptora de la información de medios en diferido, y el KMS de acuerdo con la forma de realización de la presente invención; y

la Fig. 6 es un diagrama esquemático de una estructura de un sistema para transmitir información de medios en diferido en el Subsistema Multimedia por IP, según la forma de realización de la presente invención.

Descripción detallada de formas de realización

La idea central de la presente invención es que:

la parte emisora de información de medios envía los parámetros de generación de clave (que pueden ser un número aleatorio) cifrados por medio de una clave Ka compartida con el KMS, al servidor de buzón de la parte receptora de información de medios, el servidor de buzón guarda los parámetros de generación de clave y envía los parámetros de generación de clave al KMS;

el KMS obtiene los parámetros de generación de clave usando la Ka para descifrar, genera una clave de medios K usando los parámetros de generación de clave, y envía la clave de medios K a la parte emisora de información de medios; después de recibir la clave de medios K, la parte emisora de información de medios cifra la información de medios usando la clave de medios K, y envía la información de medios cifrada al servidor de buzón de la parte receptora de información de medios; y

después de que la parte receptora de información de medios se sitúe en línea, la parte receptora obtiene los parámetros de generación de clave guardados en el servidor de buzón, y envía los parámetros de generación de clave al KMS; el KMS obtiene los parámetros de generación de clave a través del descifrado con Ka, y regenera la clave de medios K usando los parámetros de generación de clave, y envía la clave de medios K a la parte receptora de la información de medios; la parte receptora de la información de medios descifra la información de medios cifrada, recibida por el servidor de buzón, a través del descifrado con la clave de medios K.

La presente invención se describirá de forma detallada en lo sucesivo en el presente documento, y en relación con las formas de realización y dibujos de la misma.

La Fig. 4 es un diagrama de flujo de un método para negociar una clave entre la parte emisora (usuario A) de información de medios en diferido, y el servidor de buzón de la parte receptora (usuario B) de información de medios en diferido, basándose en el KMS, de acuerdo con la forma de realización de la presente invención; después de que este proceso haya finalizado, el usuario A y el servidor de buzón del usuario B completan la verificación de las identidades mutuamente, y solamente el usuario A obtiene la clave de medios K que se usa para cifrar la información de medios. Tal como se muestra en la Fig. 4, el método comprende las siguientes etapas:

Etapa 401: el usuario A y el Servidor de Gestión de Claves (KMS) obtienen la clave compartida Ka usando la negociación de la Arquitectura de Inicialización General (GBA).

En el caso de que no esté disponible el modo GBA, el usuario A puede negociar con el KMS para obtener la clave compartida Ka en otros modos de autenticación.

Etapa 402, el servidor de buzón del usuario B puede negociar con el KMS para obtener la clave compartida Km usando la GBA, la Seguridad de Capa de Transporte (TLS), la Seguridad del Protocolo de Internet (IPSec), etcétera.

La secuencia de etapa 401 y Etapa 402 no es fija, y se puede invertir.

Etapa 403, el usuario A genera un número aleatorio Ra.

Etapa 404, el usuario A envía una solicitud de llamada (tal como un mensaje INVITE) al usuario B a través de la red del IMS, y la solicitud de llamada comprende los siguientes parámetros: el ID-A (el identificador del usuario A), el ID-B (el identificador del usuario B) y el Ea (Ra, ID-A, ID-B),

en donde el Ea (Ra, ID-A, ID-B) es el texto cifrado del número aleatorio Ra, el ID-A y el ID-B usando la clave compartida Ka.

Etapa 405, la red del IMS reenvía la solicitud de llamada del usuario A al servidor de buzón del usuario B.

Etapa 406, después de recibir la solicitud de llamada del usuario A, el servidor de buzón del usuario B envía la solicitud de obtención de la clave de medios al KMS, y la solicitud comprende los siguientes parámetros del ID-A, el ID-B, el Ea (Ra, ID-A, ID-B) y el Em (ID-A, ID-Bm),

en donde el ID-Bm es el identificador del servidor de buzón del usuario B, y el Em (ID-A, ID-Bm) es el texto cifrado del ID-A y el ID-Bm usando la clave compartida Km.

Etapa 407, el KMS usa Ka para descifrar Ea (Ra, ID-A, ID-B), y verifica si el ID-A y el ID-B obtenidos a través del descifrado son idénticos a los textos en claro del ID-A y el ID-B; el KMS usa Km para descifrar Em (ID-A, ID-Bm), y verifica si el ID-A obtenido a través del descifrado es idéntico al texto en claro del ID-A, y si el ID-Bm es el identificador del servidor de buzón correspondiente al ID-B; en caso de que todas las verificaciones resulten satisfactorias (es decir, el ID-A y el ID-B obtenidos a través del descifrado son idénticos a los textos en claro del ID-A y el ID-B, y el ID-Bm es el identificador del servidor de buzón correspondiente al ID-B), el número aleatorio Ra y el ID-A obtenidos a través del descifrado se usan para generar la clave de medios K usando la Función de Derivación de Claves (KDF) de medios.

Etapa 408, el KMS obtiene el Ea(Ra, K) cifrando el número aleatorio Ra y la clave de medios K usando la Ka, y obtiene el Ekms(Ka) cifrando la Ka con la clave privada Kkms, y envía Ea(Ra, K) y Ekms(Ka) dentro del mensaje de respuesta de obtención de la clave de medios al servidor de buzón del usuario B;

después de que el Ekms(Ka) se envíe al servidor de buzón del usuario B, el KMS puede eliminar la Ka.

Etapa 409, después de recibir el Ea(Ra, K) y el Ekms(Ka), el servidor de buzón del usuario B envía un mensaje de respuesta de llamada (tal como el mensaje 200 OK) que comprende el Ea(Ra, K) al usuario A a través de la red del IMS, y almacena el Ekms(Ka) junto con el ID-A, el ID-B y el Ea(Ra, ID-A, ID-B) previamente recibidos.

Etapa 410, la red del IMS envía el mensaje 200 OK que comprende el Ea(Ra, K) al usuario A, y el usuario A obtiene la clave de medios K a través de un descifrado del Ea(Ra, K).

Etapa 411, después de obtener la clave de medios K, el usuario A puede enviar de forma segura la información de medios al servidor de buzón del usuario B usando la clave de medios K. Puesto que el servidor de buzón del usuario B no puede obtener la clave de medios K, se garantiza la seguridad de la transmisión de extremo-a-extremo.

La Fig. 5 es un diagrama de flujo de un método para obtener la clave de medios a través de la parte receptora (usuario B) de la información de medios en diferido interaccionando con el servidor de buzón de la parte receptora de la información de medios en diferido y el KMS, de acuerdo con la forma de realización de la presente invención. Después de que haya finalizado el proceso, el usuario B obtiene la clave de medios K; tal como se muestra en la Fig. 5, el método comprende las siguientes etapas.

Etapa 501, el usuario B y el Servidor de Gestión de Claves (KMS) obtienen la clave compartida Kb usando la negociación de la Arquitectura de Inicialización General (GBA).

En caso de que no esté disponible el modo GBA, el usuario B puede negociar con el KMS para obtener la clave compartida Kb en otros modos de autenticación.

Etapa 502, el usuario B envía la solicitud de información de medios en diferido al servidor de buzón, y la solicitud comprende el ID-B el cual es el identificador del usuario B.

Etapa 503, el servidor de buzón devuelve la respuesta de información de medios en diferido el usuario B, y la respuesta comprende los siguientes parámetros: el ID-A, el ID-B, el Ekms(Ka) y el Ea(Ra, ID-A, ID-B).

Etapa 504, el usuario B envía la solicitud de obtención de la clave de medios al KMS, y la solicitud comprende los siguientes parámetros: el ID-A, el ID-B, el Ea(Ra, ID-A, ID-B), el Ekms(Ka) y el Eb(ID-A, ID-B),

en donde el Eb(ID-A, ID-B) es el texto cifrado del ID-A y el ID-B usando la clave compartida Kb.

Etapa 505, el KMS obtiene la Ka usando Kkms para descifrar el Ekms (Ka); el KMS usa la Ka y la Kb respectivamente para descifrar el Ea (Ra, ID-A, ID-B) y el Eb(ID-A, ID-B), y verifica si el ID-A y el ID-B obtenidos a través del descifrado son idénticos a los textos en claro del ID-A y el ID-B; en caso de que toda la verificación resulte satisfactoria (es decir, el ID-A y el ID-B obtenidos a través del descifrado son idénticos a los textos en claro del ID-A y el ID-B), el KMS usa el número aleatorio Ra y el ID-a obtenidos a través del descifrado, para generar la clave de medios K usando la Función de Derivación de Claves (KDF) de los medios.

Etapa 506, el KMS obtiene el Eb(K) cifrando la clave de medios K con la Kb, y envía la respuesta de obtención de la clave de medios que comprende el Eb(K) al usuario B.

Así, el usuario B puede obtener la clave de medios K a través del descifrado del Eb(K), y descifra la información de medios cifrada obtenida del servidor de buzón usando la clave de medios K, con lo cual se logra la seguridad de la transmisión de extremo-a-extremo.

De acuerdo con el principio básico de la presente invención, la forma de realización antes mencionada puede presentar diversos cambios, tales como:

I. En la forma de realización antes mencionada, después de cifrar la clave compartida Ka con la Kkms, el KMS envía la clave compartida cifrada Ka al servidor de buzón del usuario B; la clave compartida Ka es obtenida por el usuario B y es devuelta al KMS, y el KMS obtiene la Ka usando la Kkms para el descifrado. En otras formas de realización de la presente invención, el KMS puede almacenar la clave compartida Ka. Ciertamente, cuando se usa este esquema técnico, es necesario que el KMS almacene y mantenga la clave compartida Ka, lo cual hace que aumenten las cargas de almacenamiento y de procesado del KMS.

II. En la forma de realización antes mencionada, el KMS toma el número aleatorio Ra y el ID-A generados por el usuario A como parámetros de generación de la clave (en donde el número aleatorio Ra se transmite en el modo cifrado y se almacena en el servidor de buzón del usuario B), al mismo tiempo, el número aleatorio Ra se toma también como parámetro para evitar un ataque de repetición. En otras formas de realización de la presente invención, como parámetros de generación de clave pueden usarse otros parámetros generados por el usuario o el número aleatorio Ra junto con otros parámetros. Ciertamente, para garantizar la transmisión y el almacenamiento seguros de los parámetros de generación de clave, es necesario que al menos uno de los parámetros de generación de clave se cifre con la Ka, y el parámetro generalmente es el número aleatorio generado por el usuario A y/u otros parámetros con la propiedad del número aleatorio (tales como la marca de tiempo, etcétera).

III. En la forma de realización antes mencionada, después de generar la clave de medios K, el KMS cifra la clave de medios K respectivamente usando las claves compartidas con el usuario B y el usuario A, y envía la clave de medios cifrada al usuario A y al usuario B respectivamente. En otras formas de realización de la presente invención, el KMS puede enviar la clave de medios K en otros modos de seguridad.

La Fig. 6 es un diagrama esquemático de una estructura de un sistema para transmitir información de medios en diferido en el Subsistema Multimedia por IP; el sistema comprende una parte emisora de información de medios (usuario A), una parte receptora de información de medios (usuario B), un KMS y un servidor de buzón del usuario B; en donde:

el usuario A está configurado para enviar los parámetros de generación de clave al servidor de buzón, y el servidor de buzón está configurado para guardar los parámetros de generación de clave y enviar los parámetros de generación de clave al KMS;

el KMS está configurado para descifrar los parámetros de generación de clave usando la Ka que ha sido guardada por el KMS, y para generar una clave de medios K con los parámetros de generación de clave descifrados, y, a continuación, enviar la K al usuario A, en donde la Ka es la clave compartida del usuario A y el KMS;

el usuario B está configurado para obtener los parámetros de generación de clave a partir del servidor de buzón y, a continuación, para enviar los parámetros de generación de clave obtenidos al KMS;

después de recibir los parámetros de generación de clave enviados por el usuario B, el KMS está configurado también para descifrar los parámetros cifrados usando la Ka en los parámetros de generación de clave usando la Ka, y para generar la K con los parámetros de generación de clave descifrados, y, a continuación, enviar la K al usuario B; y

el usuario B está configurado también para obtener la información de medios cifrada por el usuario A usando la K del servidor de buzón y, a continuación, para descifrar la información de medios cifrada usando K.

Las funciones concretas de cada elemento de red antes mencionado y la relación interactiva de mensajes entre los elementos de red se refieren a la descripción de la forma de realización del método que se muestra en la Fig. 4 y la Fig. 5.

La presente invención proporciona también un terminal emisor para transmitir información de medios en diferido en un Subsistema Multimedia por IP.

El terminal emisor está configurado para enviar parámetros de generación de clave cifrados con una Ka, a un servidor de buzón de una parte receptora, de manera que el servidor de buzón puede guardar los parámetros de generación de clave cifrados, y enviar los parámetros de generación de clave a un Servidor de Gestión de Claves (KMS);

el terminal emisor está configurado además para recibir una clave de medios K enviada por el KMS a través del servidor de buzón del terminal receptor, en donde la K es la clave de medios generada con los parámetros de generación de clave que obtiene el KMS usando la Ka correspondiente para descifrar los parámetros de generación de clave cifrados, recibidos; la Ka es la clave compartida del terminal emisor y el KMS; y

el terminal emisor está configurado además para cifrar la información de medios con la K con el fin de transmitir la información de medios.

Adicionalmente, el terminal emisor está configurado además para generar un número aleatorio y/o una marca de tiempo, a continuación para cifrar el número aleatorio y/o la marca de tiempo generados usando la Ka, y, a continuación, para enviar el número aleatorio y/o la marca de tiempo generados, cifrados, al KMS a través del servidor de buzón, como parámetros de generación de clave cifrados.

La presente invención proporciona también un Servidor de Gestión de Claves (KMS) para transmitir información de medios en diferido en un Subsistema Multimedia por IP, en donde

el KMS está configurado para:

recibir parámetros de generación de clave cifrados, enviados por un servidor de buzón de una parte receptora, en donde los parámetros de generación de clave cifrados están cifrados con una Ka y son enviados por un terminal emisor al servidor de buzón para que sean guardados en el servidor de buzón;

obtener los parámetros de generación de clave usando la Ka correspondiente para descifrar; generar una clave de medios K con los parámetros de generación de clave descifrados, y enviar la K al terminal emisor a través del servidor de buzón del terminal receptor; la Ka es la clave compartida del terminal emisor y el KMS;

recibir los parámetros de generación de clave cifrados, enviados por el terminal receptor, y los parámetros de generación de clave cifrados son obtenidos por el terminal receptor a partir del servidor de buzón; y

obtener los parámetros de generación de clave usando la Ka para descifrar los parámetros de generación de clave cifrados, recibidos del terminal receptor, y generar la K con los parámetros de generación de clave, y enviar la K al terminal receptor.

Además, el KMS está configurado además para cifrar la Ka usando una clave privada Kkms, y a continuación para enviar la Ka cifrada al servidor de buzón para que se guarde en el servidor; y

el KMS está configurado además para recibir la Ka cifrada, enviada por el terminal receptor, en donde la Ka cifrada se envía al terminal receptor a través del servidor de buzón, mientras que el terminal receptor envía los parámetros de generación de clave cifrados al KMS.

Además, el KMS está configurado además para cifrar la K generada usando una clave Kb compartida con el terminal receptor antes de enviar la K al terminal receptor, y, a continuación, para enviar la K cifrada al terminal receptor.

Además, el KMS está configurado además para verificar el identificador de la parte emisora, el identificador de la parte receptora y el identificador del servidor de buzón, y la K se generará únicamente después de que se haya aprobado la verificación.

La presente invención proporciona también un terminal receptor para transmitir información de medios en diferido en un Subsistema Multimedia por IP.

El terminal receptor está configurado para:

obtener parámetros de generación de clave cifrados, que se han cifrado con una clave Ka de un servidor de buzón, la cual es enviada por un terminal emisor al servidor de buzón, en donde la Ka es la clave compartida del terminal emisor y un Servidor de Gestión de Claves (KMS);

enviar los parámetros de generación de clave cifrados, obtenidos, al KMS;

recibir una clave K, en donde la K es enviada por el KMS y se genera con los parámetros de generación de clave que obtiene el KMS usando la Ka para descifrar los parámetros de generación de clave cifrados, después de recibir los parámetros de generación de clave cifrados enviados por el terminal receptor; y

obtener la información de medios cifrada por el terminal emisor con la K del servidor de buzón, y, a continuación, descifrar la información de medios cifrada usando la K.

Además, el terminal receptor está configurado además para obtener la K usando una clave Kb compartida con el KMS, y antes de que la K se envíe al terminal receptor, el KMS está configurado además para cifrar la K generada usando la Kb.

Aplicabilidad industrial

En comparación con la técnica anterior, después de obtener la clave compartida, la presente invención reduce la interacción de señalización entre la parte emisora de información de medios y el KMS, reduce la presión de almacenamiento del KMS, resuelve el problema provocado por la expiración de la clave compartida entre la parte emisora de información de medios y el KMS, y logra el envío seguro de información de medios en diferido en el IMS.

REIVINDICACIONES

1. Método para transmitir información de medios en diferido en un Subsistema Multimedia por IP, caracterizado por que comprende:

una parte emisora de la información de medios envía parámetros de generación de clave cifrados usando una Ka, a un servidor de buzón de una parte receptora de la información de medios; guardando el servidor de buzón los parámetros de generación de clave cifrados, y enviando los parámetros de generación de clave cifrados a un Servidor de Gestión de Claves, KMS, siendo la Ka una clave compartida de la parte emisora y el KMS;

el KMS obtiene los parámetros de generación de clave a través de un descifrado usando la Ka correspondiente, genera una clave de medios K con los parámetros de generación de clave, y reenvía la K a la parte emisora a través del servidor de buzón de la parte receptora;

la parte receptora obtiene los parámetros de generación de clave cifrados del servidor de buzón, y, a continuación, envía los parámetros de generación de clave cifrados obtenidos al KMS;

el KMS obtiene los parámetros de generación de clave usando la Ka para descifrar los parámetros de generación de clave cifrados enviados por la parte receptora, y a continuación, genera la K con los parámetros de generación de clave y envía la K a la parte receptora; y

la parte receptora obtiene la información de medios cifrada por la parte emisora con la K, del servidor de buzón, y, a continuación, descifra la información de medios cifrada usando la K.

2. Método según la reivindicación 1, caracterizado por que además comprende:

antes que la K sea enviada a la parte emisora, el KMS también cifra la Ka usando una clave privada Kkms, y, a continuación, envía la Ka cifrada al servidor de buzón para que sea guardada;

cuando la parte receptora obtiene los parámetros de generación de clave cifrados del servidor de buzón, el servidor de buzón también envía la Ka cifrada a la parte receptora; cuando la parte receptora envía los parámetros de generación de clave cifrados al KMS, la parte receptora también envía la Ka cifrada al KMS; y

después de recibir la Ka cifrada, el KMS obtiene la Ka a través de un descifrado usando la Kkms.

3. Método según la reivindicación 1 o 2, caracterizado por que

en la etapa, en la que los parámetros de generación de clave cifrados son enviados al KMS, la parte emisora envía los parámetros de generación de clave cifrados al KMS en las siguientes etapas: la parte emisora envía los parámetros de generación cifrados dentro del mensaje de solicitud de llamada, al servidor de buzón; el servidor de buzón guarda los parámetros de generación de clave cifrados, y, a continuación, envía el mensaje de solicitud de obtención de clave de medios que comprende los parámetros de generación de clave cifrados al KMS; y

antes de la etapa, en la que la clave de medios K es generada con los parámetros de generación de clave, el método comprende además la siguiente etapa: el KMS verifica el identificador de la parte emisora, el identificador de la parte receptora y el identificador del servidor de buzón, y la K que se va a generar, únicamente después de que todas las verificaciones hayan sido aprobadas.

4. Método según la reivindicación 3, caracterizado por que

en la etapa, en la que la K es reenviada a la parte emisora a través del servidor de buzón de la parte receptora, el KMS envía la K a la parte emisora en las siguientes etapas:

el KMS cifra la K generada con la Ka, y, a continuación, envía la K cifrada al servidor de buzón;

el servidor de buzón envía la K cifrada dentro del mensaje de respuesta de llamada a la parte emisora; y

el método además comprende la etapa, en la que la parte emisora obtiene la K a través de un descifrado usando la Ka.

5. Método según la reivindicación 1 o 2, caracterizado por que

en la etapa, en la que la K es enviada a la parte receptora, el KMS envía la K a la parte receptora en las siguientes etapas:

el KMS cifra la K generada con una clave Kb compartida con la parte receptora, y a continuación, envía la K cifrada a la parte receptora, y

el método además comprende la etapa, en la que la parte receptora obtiene la K a través de un descifrado usando la Kb.

6. Método según la reivindicación 1, caracterizado por que

los parámetros de generación de clave cifrados comprenden un número aleatorio generado por la parte emisora y/o una marca de tiempo.

7. Método según la reivindicación 3, caracterizado por que

el mensaje de solicitud de llamada comprende: unos textos en claro del identificador de la parte emisora y el identificador de la parte receptora, y un texto cifrado del identificador de la parte emisora y el identificador de la parte receptora cifrado con la Ka; y

el mensaje de solicitud de obtención de la clave de medios comprende: unos textos en claro del identificador de la parte emisora y el identificador de la parte receptora, unos textos cifrados del identificador de la parte emisora y el identificador de la parte receptora cifrados con la Ka, y unos textos cifrados del identificador de la parte emisora y el identificador del servidor de buzón cifrados con una clave Km compartida por el servidor de buzón y el KMS; y

en la etapa de verificación, el KMS verifica el identificador de la parte emisora, el identificador de la parte receptora y el identificador del servidor de buzón en las siguientes etapas: verificar si el identificador de la parte emisora obtenido a través del descifrado es idéntico al texto en claro del identificador de la parte emisora; verificar si el identificador de la parte receptora obtenido a través del descifrado es idéntico al texto en claro del identificador de la parte receptora; y verificar si el identificador del servidor de buzón obtenido a través del descifrado es idéntico al identificador del servidor de buzón correspondiente al identificador de la parte receptora.

8. Sistema para transmitir información de medios en diferido en un Subsistema Multimedia por IP, que comprende: una parte emisora de información de medios, una parte receptora de la información de medios, un Servidor de Gestión de Claves, KMS, y un servidor de buzón de la parte receptora de la información de medios, caracterizado por que

la parte emisora está configurada para enviar parámetros de generación de clave cifrados con una Ka al servidor de buzón, y el servidor de buzón está configurado para guardar los parámetros de generación de clave cifrados, y para enviar los parámetros de generación de clave cifrados al KMS, siendo la Ka una clave compartida de la parte emisora y el KMS;

el KMS está configurado para obtener los parámetros de generación de clave usando la Ka correspondiente para descifrar, para generar una clave de medios K con los parámetros de generación de clave descifrados, y para enviar la K a la parte emisora;

la parte receptora está configurada para obtener del servidor de buzón los parámetros de generación de clave cifrados, y, a continuación, para enviar al KMS los parámetros de generación de clave cifrados, obtenidos;

después de recibir los parámetros de generación de clave cifrados enviados por la parte receptora, el KMS está configurado además para obtener los parámetros de generación de clave usando la Ka para descifrar los parámetros de generación de clave cifrados, para generar la K con los parámetros de generación de clave descifrados y para enviar la K a la parte receptora; y

la parte receptora está configurada además para obtener la información de medios cifrada por la parte emisora con la K del servidor de buzón, y a continuación, para descifrar la información de medios cifrada usando la K.

9. Sistema según la reivindicación 8, caracterizado por que además comprende:

antes de que la K sea enviada a la parte emisora, el KMS está configurado además para cifrar la Ka usando la clave privada Kkms, y a continuación, para enviar la Ka cifrada al servidor de buzón para que sea guardada;

cuando la parte receptora obtiene los parámetros de generación de clave cifrados del servidor de buzón, el servidor de buzón está configurado además para enviar la Ka cifrada a la parte receptora, y la parte receptora está configurada además para enviar la Ka cifrada y los parámetros de generación de clave cifrados al KMS; y

después de recibir la Ka cifrada, el KMS está configurado además para obtener la Ka a través de un descifrado usando la Kkms.

10. Sistema según la reivindicación 8, caracterizado por que además comprende:

la parte emisora configurada además para generar un número aleatorio y/o una marca de tiempo y para cifrar el número aleatorio y/o la marca de tiempo generados usando la Ka, y a continuación, para enviar el número aleatorio y/o la marca de tiempo generados cifrados al KMS a través del servidor de buzón como los parámetros de generación de clave cifrados.

11. Terminal emisor para transmitir información de medios en diferido en un Subsistema Multimedia por IP, caracterizado por que

el terminal emisor está configurado para enviar parámetros de generación de clave cifrados con una Ka a un servidor de buzón de un terminal receptor, de manera que el servidor de buzón pueda guardar los parámetros de generación de clave cifrados y enviar los parámetros de generación de clave a un Servidor de Gestión de Claves, KMS;

el terminal emisor está configurado además para recibir una clave de medios K enviada por el KMS a través del servidor de buzón del terminal receptor, siendo la K la clave de medios generada con los parámetros de generación de clave que el KMS obtiene usando la Ka correspondiente para descifrar los parámetros de generación de clave cifrados recibidos; la Ka es la clave compartida del terminal emisor y el KMS; y

el terminal emisor está configurado además para cifrar la información de medios con la K para transmitir la información de medios.

12. Terminal receptor para transmitir información de medios en diferido en un Subsistema Multimedia por IP, caracterizado por que

el terminal receptor está configurado para:

obtener parámetros de generación de clave cifrados, que se han cifrado con una clave Ka de un servidor de buzón del terminal receptor, que un terminal emisor envía al servidor de buzón, siendo la Ka la clave compartida del terminal emisor y un Servidor de Gestión de Claves, KMS;

enviar los parámetros de generación de clave cifrados obtenidos al KMS;

recibir una clave K, siendo la K enviada por el KMS y generada con los parámetros de generación de clave que el KMS obtiene usando la Ka para descifrar los parámetros de generación de clave cifrados después de recibir los parámetros de generación de clave cifrados enviados por el terminal receptor; y

obtener la información de medios cifrada por el terminal emisor con la K del servidor de buzón, y, a continuación descifrar la información de medios cifrada usando la K.

13. Terminal receptor según la reivindicación 12, caracterizado por que

el terminal receptor está configurado además para obtener la K usando una clave Kb compartida con el KMS, y antes de que la K sea enviada al terminal receptor, el KMS está configurado además para cifrar la K generada usando la Kb.

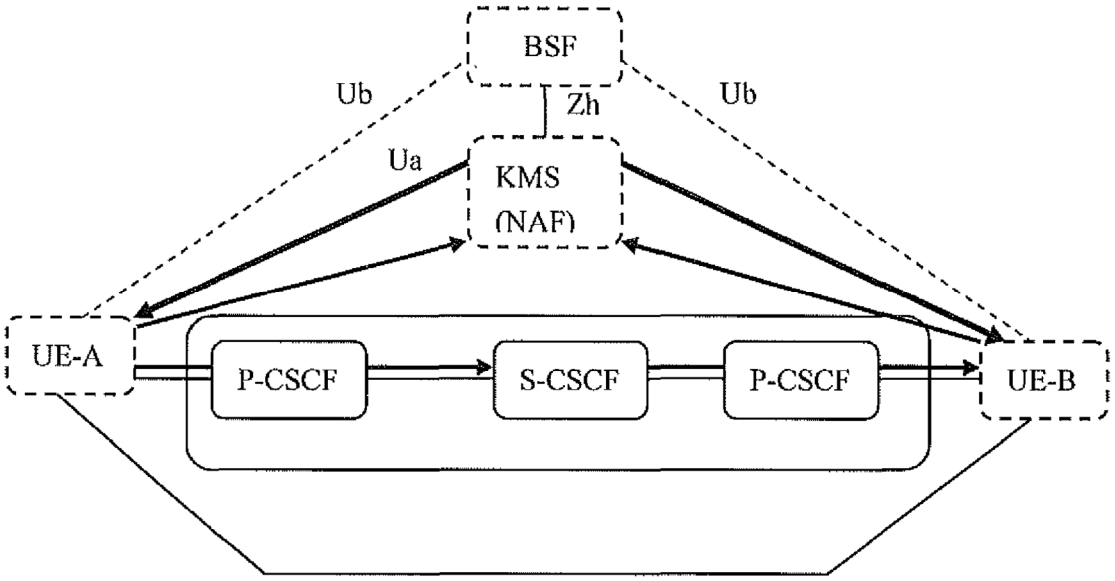
BSF
Ub
Zh
Ub
Ua
KMS
(NAF)
UE-A
P-CSCF
S-CSCF
P-CSCF
UE-B

Fig.1

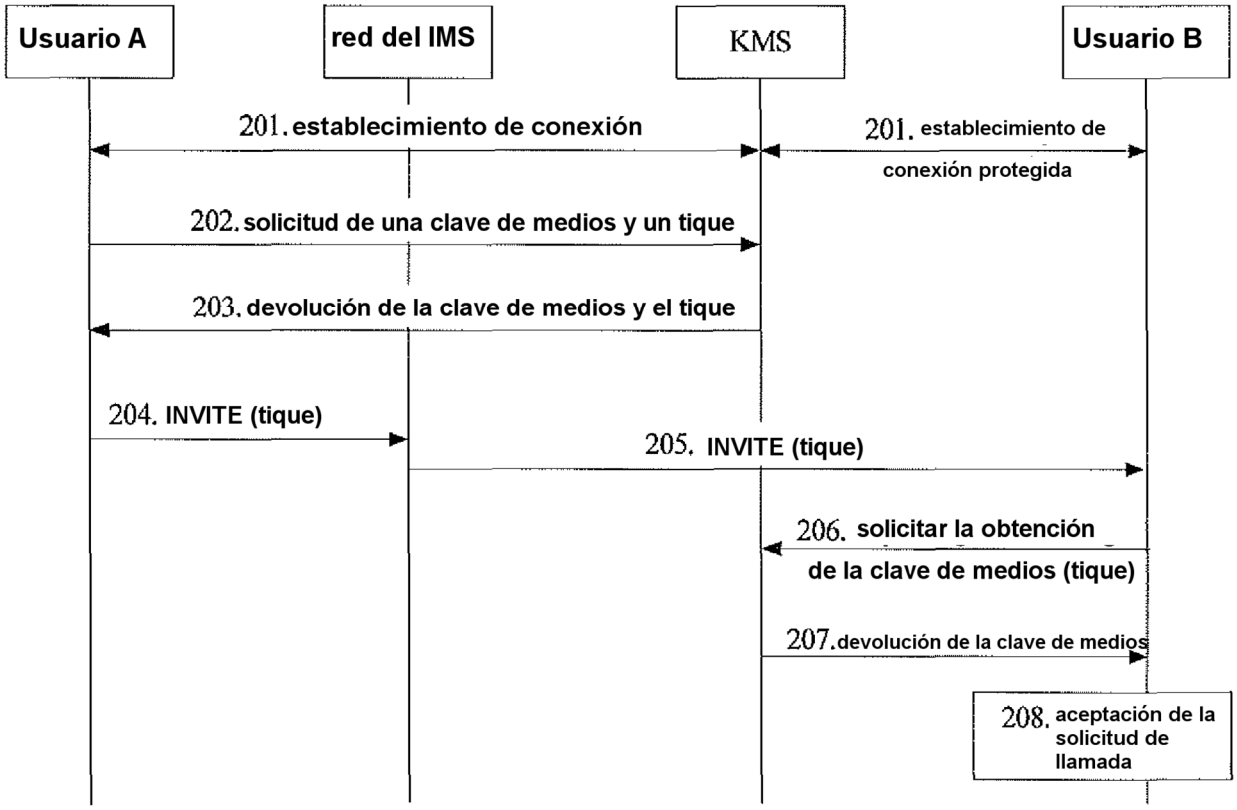
Usuario A
red del IMS
KMS
Usuario B
201. establecimiento de conexión
201. establecimiento de conexión protegida
202. solicitud de una clave de medios y un tique
203. devolución de la clave de medios y el tique
204. INVITE (tique)
205. INVITE (tique)
206. solicitar la obtención de la clave de medios (tique)
207. devolución de la clave de medios
208. aceptación de la solicitud de llamada

Fig.2

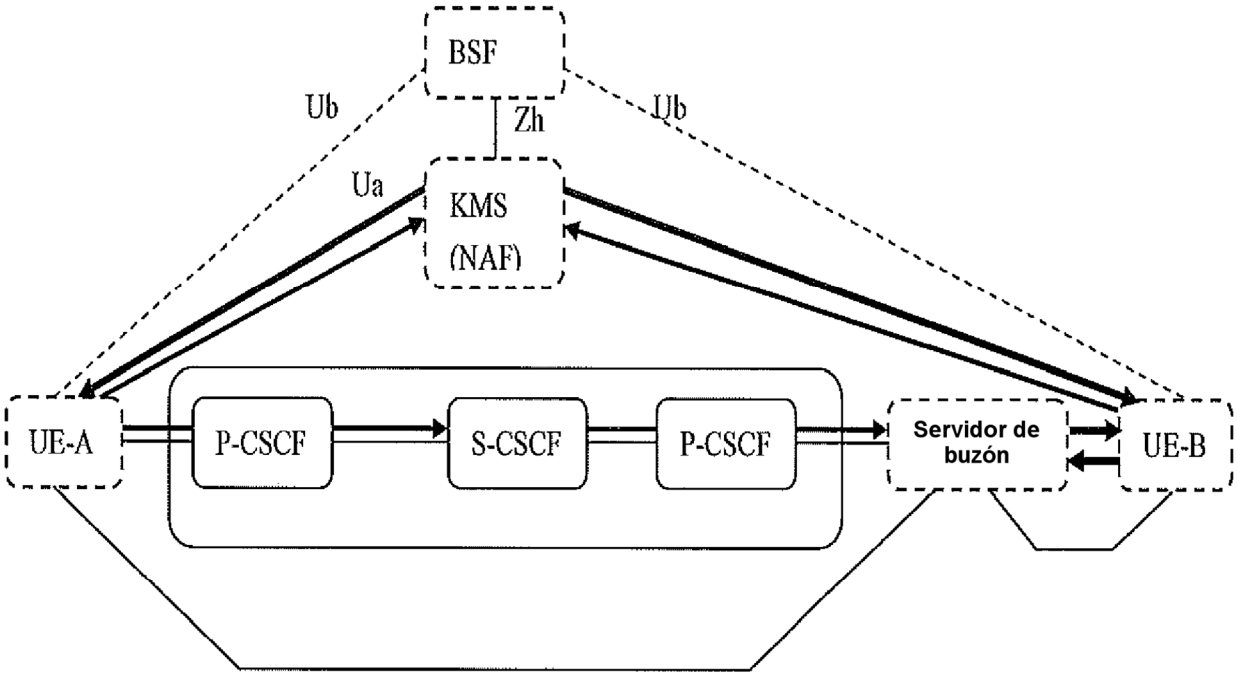
BSF
Ub
Zh
Ub
Ua
KMS
(NAF)
UE-A
P-CSCF
S-CSCF
P-CSCF
Servidor de buzón
UE-B

Fig.3

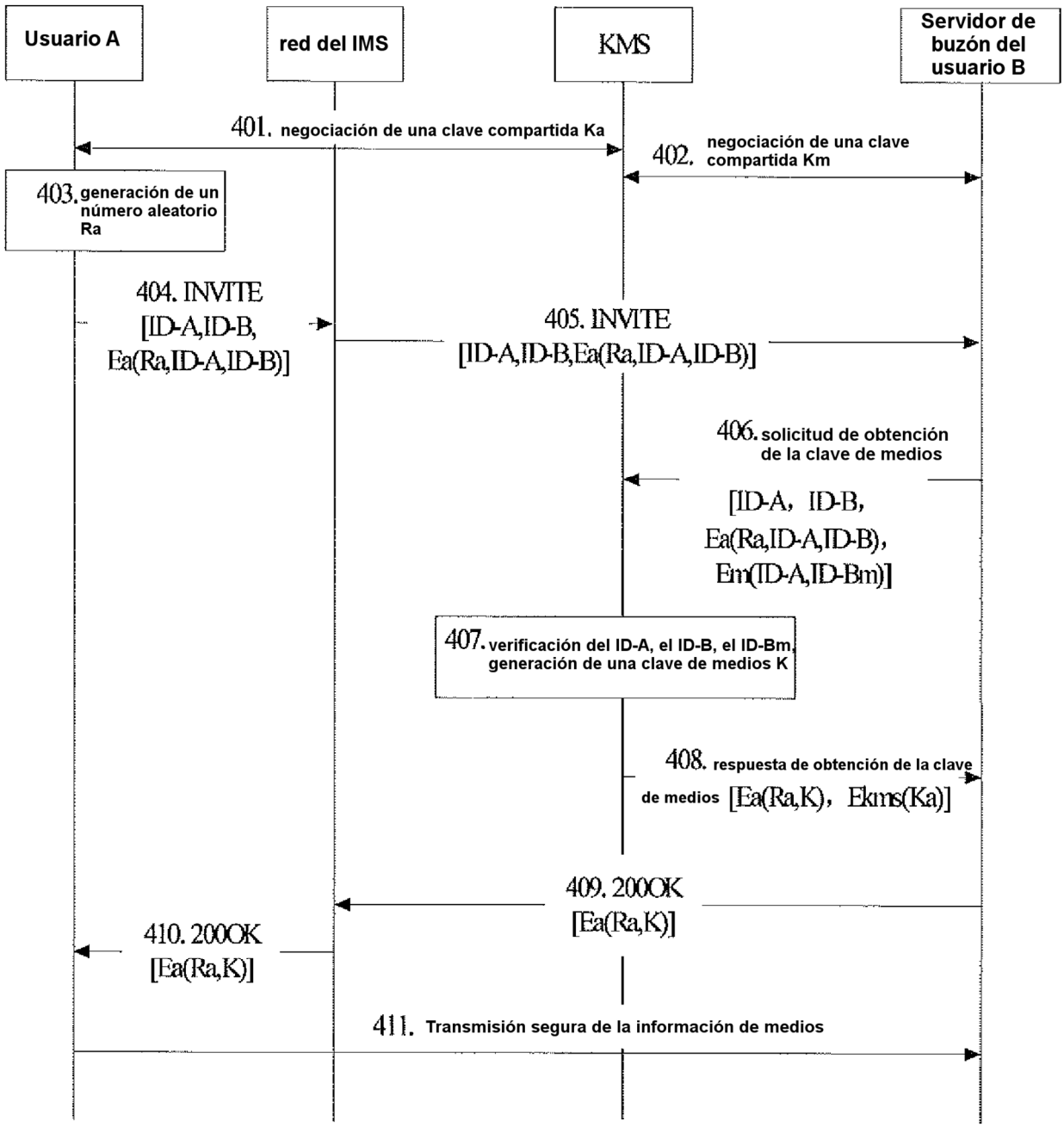
Usuario A
red del IMS
KMS
Servidor de buzón del usuario B
401. negociación de una clave compartida Ka
402. negociación de una clave compartida Km
403. generación de un número aleatorio Ra
404. INVITE [ID-A,ID-B, Ea(Ra,ID-A,ID-B)]
405. INVITE [ID-A,ID-B,Ea(Ra,ID-A,ID-B)]
406. solicitud de obtención de la clave de medios [ID-A, ID-B, Ea(Ra,ID-A,ID-B), Em(ID-A,ID-Bm)]
407. verificación del ID-A, el ID-B, el ID-Bm, generación de una clave de medios K
408. respuesta de obtención de la clave de medios [Ea(Ra,K), Ekms(Ka)]
409. 200OK [Ea(Ra,K)]
410. 200OK [Ea(Ra,K)]
411. Transmisión segura de la información de medios

Fig.4

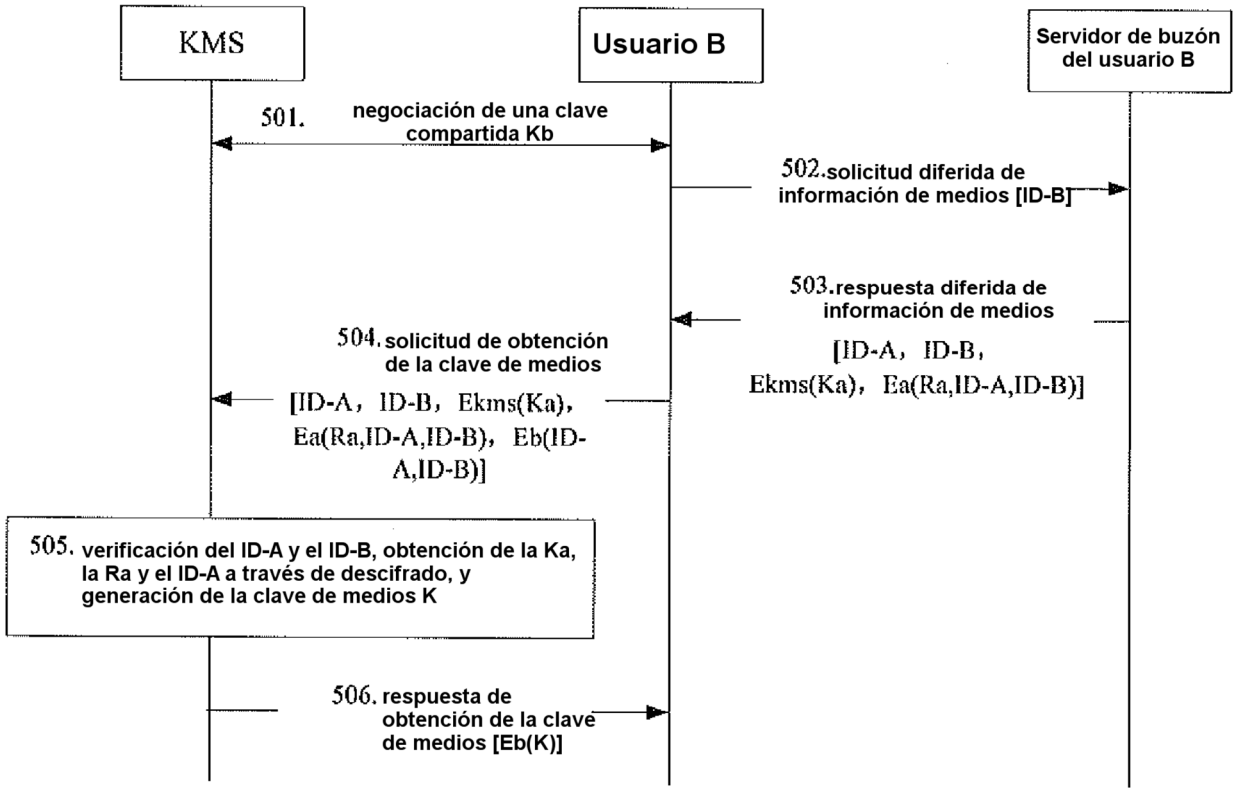
KMS
Usuario B
Servidor de buzón del usuario B
501. negociación de una clave compartida Kb
502. solicitud diferida de información de medios [ID-B]
503. respuesta diferida de información de medios [ID-A, ID-B, Ekms(Ka), Ea(Ra,ID-A,ID-B)]
504. solicitud de obtención de la clave de medios [ID-A, ID-B, Ekms(Ka), Ea(Ra,ID-A,ID-B), Eb(ID-A,ID-B)]
505. verificación del ID-A y el ID-B, obtención de la Ka, la Ra y el ID-A a través de descifrado, y generación de la clave de medios K
506. respuesta de obtención de la clave de medios [Eb(K)]

Fig.5

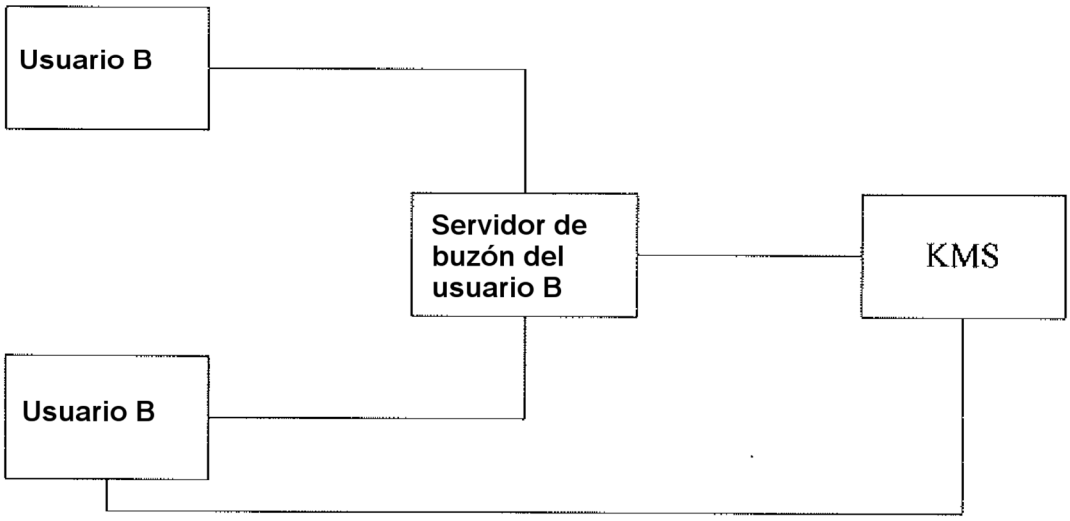
Usuario B
Servidor de buzón del usuario B
KMS
Usuario B

Fig.6