(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 398 376**

(51) Int. CI.:

G06F 21/00 (2006.01)
H04L 9/00 (2006.01)
H04N 7/16 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.03.2007 E 07720574 (8)**

(97) Fecha y número de publicación de la concesión europea: **19.12.2012 EP 2006787**

(54) Título: **Método, sistema, equipo de abonado y servidor multimedia para la protección digital de los derechos de autor**

(30) Prioridad:

29.03.2006 CN 200610034794

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.03.2013

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
HUAWEI ADMINISTRATION BUILDING BANTIAN LONGGANG DISTRICT. SHENZHEN GUANGDONG PROVINCE 518129, CN

(72) Inventor/es:

YANG, JIAN y
ZHAO, QIN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, sistema, equipo de abonado y servidor multimedia para la protección digital de los derechos de autor

Campo de la invención

La presente invención se refiere a un método y sistema de protección digital de los derechos de autor, un Equipo de Usuario y un servidor multimedia.

Antecedentes de la invención

En los últimos años, se han desarrollado, en gran medida, aplicaciones de una tecnología multimedia basada en una red cableada de banda ancha; además, se ha contrastado una tecnología multimedia basada en una red de comunicaciones móviles.

Los flujos de datos multimedia son medios que pueden transmitirse en un modo de transmisión continua a través de una red. No es necesario descargar el fichero completo antes de que se ejecuten dichos medios sino que, por el contrario, solamente el contenido de la parte inicial del fichero se memoriza en una memoria y paquetes de datos se memorizan, de forma intermedia, en un Equipo de Usuario y los datos multimedia se proporcionan correctamente a la salida. Con el modo de transmisión continua, un usuario puede utilizar un fichero multimedia después de un retardo inicial de solamente varios o decenas de segundos, antes de que se descargue completamente el fichero multimedia completo. El resto del fichero se descarga posteriormente desde el servidor *background* de segundo plano, de modo que el usuario pueda utilizar el fichero mientras lo recibe.

Los derechos de autor son un aspecto importante a considerar con respecto a la transmisión de flujo de datos multimedia. La Gestión Digital de Derechos (DRM) es una tecnología para evitar que los datos multimedia digitales (tales como un juego, un tono de llamada, una imagen, una señal de audio y una señal de vídeo) se dupliquen o utilicen de forma ilícita y se ha desarrollado frecuentemente en una red cableada.

Actualmente, se realizaron numerosas investigaciones en DRM móvil a escala mundial. Un estándar de DRM móvil, establecido por la Alianza Móvil Abierta (OMA), se ha soportado y aceptado en gran medida. La OMA emitió la más reciente versión de OMA DRM V2.0 el 14 de junio de 2005, que establece un modelo de seguridad-confianza basado en una arquitectura de Infraestructura de Claves Públicas (PKI) del DRM móvil, un estándar de lenguaje de descripción de derechos, Formato de Contenido de DRM (DCF) y Protocolo de Adquisición de Objetos de Derechos (ROAP).

Un sistema de OMA DRM incluye un Agente de DRM de un Equipo de Usuario, un Emisor de Contenidos (CI), un Emisor de Derechos (RI) y elementos similares. En una solución de protección digital de derechos de autor de multimedia por la OMA, los flujos de datos multimedia se memorizan en un servidor correspondiente. Un flujo de datos multimedia es encriptado y una clave de desencriptación está disponible en un Objeto de Derecho (RO), según se indica en la Figura 1, el RO incluye una regla de uso de derechos de autor 110 y una clave de desencriptación de flujo de datos multimedia (por ejemplo, Clave de Encriptación de Contenido (CEK)) 120. Después de que se obtenga el RO por el Agente de DRM del Equipo de Usuario, el flujo de datos multimedia se puede desencriptar con la clave de desencriptación en el RO para su utilización, aunque se esté descargando todavía los flujos de datos multimedia. Un procedimiento de interacción particular se ilustra en la Figura 2, que incluye:

Etapa 11: Un Equipo de Usuario se conecta a una página web de un CI, encuentra flujo de datos multimedia de interés y solicita su descarga;

Etapa 12: El Emisor de Contenidos genera el Token de información de dirección del flujo de datos multimedia;

Etapas 13A y 13B: El CI envía el Token al Equipo de Usuario y un RI, respectivamente;

Etapa 14: Un servidor de flujos de datos multimedia y el Emisor de Derechos negocian para generar un RO;

Etapa 15: El Equipo de Usuario solicita el RO al Emisor de Derechos, siendo el Token transmitido en la demanda;

Etapa 16: El RI envía el RO al Equipo de Usuario;

Etapa 17: Una vez establecida una sesión entre el Equipo de Usuario y el servidor de flujos de datos multimedia, el servidor transmite al Equipo de Usuario el flujo de datos multimedia protegido con DRM que se encripta con la CEK.

Después de obtener el flujo de datos multimedia protegido con DRM, el Equipo de Usuario desencripta el flujo de datos multimedia con el CEK en el RO y ejecuta el fichero multimedia.

En la técnica anterior, la desencriptación de un flujo de datos multimedia se realiza en la capa de aplicación del Equipo de Usuario. En este caso, se establece un requisito estricto para el Equipo de Usuario, que da lugar a un aumento en el coste adicional del Equipo de Usuario.

Además, en la puesta en práctica de un servicio multimedia tal como TV móvil y descarga de ficheros, el método y sistema de protección digital de derechos de autor, en la técnica anterior, tiene una alta exigencia para el Equipo de Usuario, lo que da lugar a un aumento en el coste adicional del Equipo de Usuario.

Los servicios de autenticación y de encriptación se proporcionan en la Seguridad de Protocolo de Internet (IPSec) utilizando una criptografía operativamente fuerte. La autenticación garantiza que los datos procedan del emisor previsto y no se modifiquen durante la transmisión y la encriptación puede evitar que un paquete de datos sea objeto de lectura sin autorización. Estos servicios permiten que se establezca un canal seguro en una red sin confianza contrastada. La IPSec proporciona los servicios de encriptación y autenticación en la capa de protocolo de Internet (IP) de la pila de protocolos de red. La IPSec funciona en la capa de IP y puede proteger cualquier comunicación transmitida a través de IP.

El documento WO2005107259A1 da a conocer un método para el flujo continuo de contenido digital a través de Internet con un protocolo de seguridad.

El documento XP00915737 “IPSec” Internet Citation que se recupera desde http://en.wikipedia.org/w/index.php?title=IPsec&oldid=45401965> da a conocer un estándar denominado IPSec para asegurar la comunicación de IP mediante encriptación y/o autenticación de todos los paquetes de IP.

Sumario de la invención

Formas de realización de la invención dan a conocer un método y sistema de protección digital de derechos de autor y un servidor multimedia, con el fin de reducir el coste de un Equipo de Usuario.

Según una forma de realización de la invención, se da a conocer un Equipo de Usuario, que puede realizar la protección digital de los derechos de autor con un más bajo coste.

Un método de protección digital de los derechos de autor, dado a conocer en otra forma de realización de la invención, incluye: la negociación entre un servidor multimedia y un Emisor de Derechos para generar un Objeto de Derecho que transmite información para establecer un canal de comunicación encriptado; el establecimiento, por un Equipo de Usuario, del canal de comunicación encriptado para el servidor multimedia utilizando la información para establecer el canal de comunicación encriptado soportado en el Objeto de Derecho, a la recepción del Objeto de Derecho y el envío, por el servidor multimedia, de datos multimedia al Equipo de Usuario a través del canal de comunicación encriptado.

Un sistema de protección digital de derechos de autor se da a conocer en otra forma de realización de la invención y este sistema incluye un servidor multimedia y un Emisor de Derechos.

El servidor multimedia está adaptado para memorizar datos multimedia, para negociar con el Emisor de Derechos para generar un Objeto de Derecho que transmite información para establecer un canal de comunicación encriptado; para negociar con un Equipo de Usuario la utilización de la información para establecer el canal de comunicación encriptado y para enviar datos multimedia bajo protección de derechos de autor al Equipo de Usuario a través del canal de comunicación encriptado y

El Emisor de Derechos está adaptado para negociar con el servidor multimedia para generar el Objeto de Derecho que transmite información para establecer el canal de comunicación encriptado y para enviar el Objeto de Derecho al Equipo de Usuario.

Un servidor multimedia se da a conocer en otra forma de realización de la invención, que incluye: una unidad de memorización de datos multimedia adaptada para memorizar datos multimedia; una unidad de negociación de Objeto de Derecho adaptada para negociar con un Emisor de Derechos para generar un Objeto de Derecho que transmite información para establecer un canal de comunicación encriptado; una unidad de negociación de canal adaptada para negociar con un Equipo de Usuario utilizando la información para establecer el canal de comunicación encriptado y una unidad de provisión de datos multimedia adaptada para proporcionar los datos multimedia bajo protección de los derechos de autor al Equipo de Usuario a través del canal de comunicación encriptado.

Un Equipo de Usuario se da a conocer en otra forma de realización de la invención, que incluye: un explorador adaptado para explorar información multimedia proporcionada por un Emisor de Contenidos y para solicitar la descarga de datos multimedia; un Agente de DRM adaptado para obtener información para establecer un canal de comunicación encriptado soportado en un Objeto de Derecho recibido y para establecer el canal de comunicación encriptado con un servidor multimedia utilizando la información y un procesador multimedia adaptado para procesar los datos multimedia transmitidos a través del canal de comunicación encriptado.

En las formas de realización de la invención, por medio de la encriptación de una ruta lógica en lugar de los datos multimedia, el coste adicional requerido para desencriptar los datos multimedia en la capa de aplicación del cliente pueden evitarse. Por lo tanto, se disminuyen las exigencias de rendimiento para un Equipo de Usuario y se mejora la experiencia del usuario. Además, se establece una ruta lógica dedicada entre el dispositivo del cliente y un servidor multimedia, de modo que se reduce un riesgo de que los datos multimedia sean interceptados y capturados por una entidad tercera y se mejora la seguridad de las comunicaciones extremo a extremo.

Breve descripción de los dibujos

La Figura 1 es un diagrama esquemático que ilustra la configuración de un RO en la técnica anterior;

La Figura 2 es un diagrama esquemático que ilustra el procedimiento de interacción de DRM de flujo de datos multimedia en la técnica anterior;

La Figura 3 es un diagrama esquemático que ilustra la configuración de un RO según una primera forma de realización de la invención;

La Figura 4 es un diagrama esquemático que ilustra el procedimiento de interacción del método DRM de flujo de datos multimedia según una forma de realización de la invención;

La Figura 5 es un diagrama que ilustra el procedimiento de una primera fase de la Asociación de Seguridad (SA) de IPSec según se representa en la Figura 4,

La Figura 6 es un diagrama esquemático del sistema de DRM según una forma de realización de la invención;

La Figura 7 es un diagrama de flujo del método de protección digital de derechos de autor según una segunda forma de realización de la invención y

La Figura 8 es un diagrama de bloques del sistema de protección digital de derechos de autor según la segunda forma de realización de la invención.

Descripciones detalladas de las formas de realización preferidas

Formas de realización de la invención se describen, a continuación, haciendo referencia a los dibujos adjuntos.

Según una forma de realización de la invención, se da a conocer una solución de gestión digital de derechos de flujo de datos multimedia basada en IPSec, en donde se encripta una ruta lógica entre un servidor de flujo de datos multimedia y un Equipo de Usuario y la información de autenticación 310 para establecer el canal de comunicación de IPSec entre el Equipo de Usuario y el servidor de flujo de datos multimedia, en lugar de la clave para la ruta lógica, se memoriza en el RO, según se representa en la Figura 3.

Un procedimiento de interacción particular, según la forma de realización de la invención se ilustra en la Figura 4 y dicho procedimiento incluye:

Etapa 41: Un Equipo de Usuario se conecta a una página web de un Emisor de Contenidos, encuentra flujo de datos multimedia de interés y solicita la descarga de dicho flujo de datos multimedia;

Etapa 42: El Emisor de Contenidos genera un Token;

Etapas 43A y 43B: El Emisor de Contenidos envía el Token al Equipo de Usuario y a un Emisor de Derechos;

Etapa 44: un servidor de flujos de datos multimedia y el Emisor de Derechos negocian para generar un RO.

En la etapa 44, el RO generado por el servidor de flujos de datos multimedia y el Emisor de Derechos, mediante negociación, transmite información de autenticación para establecer un canal de comunicación IPSec entre el Equipo de Usuario y el servidor de flujos de datos multimedia.

Etapa 45: El Equipo de Usuario solicita el RO desde el Emisor de Derechos, con el Token siendo transmitido en la demanda;

Etapa 46: El Emisor de Derechos envía el RO al Equipo de Usuario,

Etapa 47A: El Equipo de Usuario y el servidor de flujos de datos multimedia negocian para establecer una primera fase de SA y para la autenticación del canal de comunicación a establecerse de forma secuencial mediante negociación; la autenticación se realiza por el Equipo de Usuario y el servidor de flujos de datos multimedia con la información de autenticación transmitida en el RO;

Etapa 47B: El Equipo de Usuario y el servidor de flujo de datos multimedia negocian para establecer una segunda fase de SA, de modo que se establezca un canal de comunicación de IPSec y

Etapa 48: El servidor de flujos de datos multimedia transmite el flujo multimedia al Equipo de Usuario a través del canal de comunicación.

El Equipo de Usuario ejecuta el flujo multimedia en conformidad con una regla de uso de derechos de autor en el RO.

En la etapa 44, en la generación del RO, el servidor de flujo de datos multimedia y el Emisor de Derechos negocian la información de autenticación para establecer el canal de comunicación IPSec. En el establecimiento del SA mediante negociación en la etapa 47A, la información de autenticación se utiliza cuando la identidad y los datos de verificación se entregan entre sí. El procedimiento puede proseguir con la segunda fase de SA de IPSec solamente si se realiza satisfactoriamente la autenticación en la etapa 47A, con el fin de negociar una clave para la encriptación de un paquete de datos de IP.

La primera fase de SA de IPSec suele incluir las tres etapas siguientes.

Una primera etapa incluye la negociación de reglas.

En la primera etapa, se negocian cuatro parámetros obligatorios:

(1) algoritmo de encriptación: se selecciona DES o 3DES;

(2) algoritmo de Hash: se selecciona MD5 o SHA;

(3) método de autenticación: autenticación de certificado, autenticación de claves compartidas preestablecidas o se selecciona la autenticación de Kerberos v5 y

(4) selección del grupo de conversación de Diffie-Hellman.

Una segunda etapa incluye el intercambio de claves.

A pesar del término de “intercambio de claves”, no se intercambia ninguna clave real entre el Equipo de Usuario y el servidor de flujo de datos multimedia, sino que se intercambia alguna información importante básica requerida para generar una clave compartida. El intercambio puede ser público o bajo protección. El Equipo de Usuario y el servidor de flujos de datos multimedia pueden generar, respectivamente, la misma clave maestra compartida después de que se intercambien entre sí los materiales para la generación de claves, con el fin de proteger al procedimiento de autenticación siguiente.

Una tercera etapa incluye la autenticación.

Una entidad de comunicación y un canal de comunicación son objeto de autenticación con el uso de la clave maestra compartida y del algoritmo de negociación determinado en la primera etapa. En la tercera etapa, han de autenticarse la confidencialidad y la integridad de la totalidad de las cargas útiles de entidades, incluyen un tipo de entidad, un número de puerto y un protocolo, que se pueden poner en práctica con la clave maestra compartida generada en la segunda etapa.

Según la forma de realización de la presente invención, en la etapa 47A, el procedimiento particular en el que el Equipo de Usuario y el servidor de flujos de datos multimedia establecen la primera fase de SA se representa en la Figura 5 y el procedimiento incluye lo que sigue.

Etapa 51: Un Equipo de Usuario envía una regla de Intercambio de Claves de Internet (IKE) local a un servidor de flujos de datos multimedia;

Etapa 52: El servidor de flujos de datos multimedia confirma el algoritmo utilizado por el Equipo de Usuario, busca una regla de adaptación local y envía la regla confirmada por el servidor de flujo de datos multimedia al Equipo de Usuario,

Etapas 53A y 53B: A la recepción de la regla confirmada desde el lado opuesto (esto es, el servidor de flujo de datos multimedia), el Equipo de Usuario proporciona información para la generación de claves; el servidor de flujo de datos multimedia y el Equipo de Usuario intercambian la información para la generación de claves y generan, respectivamente, una clave;

Etapa 54: El Equipo de Usuario entrega datos de verificación e identidad al servidor de flujo de datos multimedia; con la información de autenticación transmitida en el RO que se incluye en los datos de verificación e identidad; después de comprobar la identidad del Equipo de Usuario, el servidor de flujos de datos multimedia envía sus datos de identidad y verificación al Equipo de Usuario y

Etapa 55: La primera fase de SA se realiza después de que el Equipo de Usuario y el servidor de flujo de datos multimedia concluyan la verificación de la identidad y la verificación del procedimiento de intercambio.

Una puesta en práctica alternativa del método según la forma de realización de la invención puede incluir lo que sigue.

En la etapa 44, la información de confirmación de uso de derechos de autor para el Equipo de Usuario se transmite en el RO generado por el servidor de flujo de datos multimedia y el Emisor de Derechos mediante negociación; en la etapa 47, el Equipo de Usuario proporciona la información de confirmación de uso de derechos de autor transmitida en el RO al servidor de flujo de datos multimedia, cuando se solicita la descarga de contenidos desde el servidor de flujo de datos multimedia y el servidor de flujo de datos multimedia realiza la autenticación de la información de confirmación de derechos de autor y si se realiza satisfactoriamente la autenticación, el servidor de flujo de datos multimedia y el Equipo de Usuario negocian SA y establecen un canal de comunicación IPSec. Los procedimientos de la negociación de SA y el establecimiento de la comunicación IPSec se pueden poner en práctica según la técnica anterior y por ello, no se describirá aquí de nuevo.

Después de que se establezca el canal de comunicación IPSec entre el servidor de flujo de datos multimedia y el Equipo de Usuario, se transmite un flujo multimedia desde el servidor de flujo de datos multimedia al Equipo de Usuario a través del canal de comunicación IPSec y se ejecuta por el Equipo de Usuario en conformidad con la regla de uso de derechos de autor en el RO.

El canal de comunicación IPSec, establecido en la forma de realización de la invención, está en un modo de establecer un túnel de IPSec. Se apreciará que otros modos, tales como un modo de transporte, se pueden utilizar también en esta forma de realización.

Además, si lo permite la capacidad del Equipo de Usuario, el método según la forma de realización de la invención se puede utilizar en relación con el método de DRM de flujo de datos multimedia en la técnica anterior. Dicho de otro modo, los contenidos del flujo de datos multimedia y el canal de transmisión para el flujo de datos multimedia se pueden encriptar y la información para establecer el canal de comunicación IPSec y la CEK se incluyen en el RO. El Equipo de Usuario y el sistema DRM, en la forma de realización de la invención, se representan en la Figura 6. El sistema incluye un servidor de flujo de datos multimedia 620, un Emisor de Contenidos 630 y un Emisor de Derechos 640. El Equipo de Usuario 610 incluye: un explorador 611 para explorar información de flujo de datos multimedia proporcionada por el Emisor de Contenidos 630 y solicitando la descarga del flujo de datos multimedia; un Agente de DRM 612 para obtener información para establecer un canal de comunicación encriptado soportado en un RO recibido y establecer el canal de comunicación encriptado con el servidor de flujo de datos multimedia 620 utilizando la información y un reproductor de flujo de datos multimedia 613 para reproducir los flujos de datos multimedia transmitidos a través del canal de comunicación encriptado.

El servidor de flujo de datos multimedia 620 está adaptado para memorizar contenidos de flujo de datos multimedia, para negociar el Emisor de Derechos 640 para generar un RO que transmita la información para establecer un canal de comunicación encriptado, para establecer el canal de comunicación encriptado mediante negociación con el Equipo de Usuario 610 utilizando la información y para proporcionar los flujos de datos multimedia bajo protección de derechos de autor al Equipo de Usuario 610 a través del canal de comunicación encriptado.

El Emisor de Contenidos 630 está adaptado para proporcionar al Equipo de Usuario 610 información de flujo de datos multimedia y para proporcionar al Equipo de Usuario 610 un Token y enviar el Token al Emisor de Derechos 640 cuando el Equipo de Usuario 610 solicite la descarga de flujo de datos multimedia.

El Emisor de Derechos 640 está adaptado para negociar con el servidor de flujos de datos multimedia 620 para generar un RO que transmita la información para establecer un canal de comunicación encriptado, en función del Token enviado desde el CI 630 y para enviar el RO al Equipo de Usuario 610.

En una puesta en práctica particular según la forma de realización de la presente invención, el canal de comunicación encriptado se establece utilizando IPSec. En este caso, el servidor de flujos de datos multimedia 620 y el Equipo de Usuario 610 incluyen un controlador de IPSec 621 y un controlador de IPSec 614, respectivamente. El controlador de IPSec 614 está adaptado para establecer un canal de comunicación encriptado con el controlador de IPSec 621 del servidor de flujo de datos multimedia 620 utilizando la información para establecer el canal de comunicación encriptado, cuando se solicita por el Agente de DRM 612.

Con referencia a la Figura 7, un diagrama de flujo del método de protección digital de derechos de autor, según la segunda forma de realización de la invención, se representa en dicha Figura y el método incluye lo que sigue.

Etapa 71: Un Equipo de Usuario solicita la descarga de datos multimedia desde un Emisor de Contenidos;

Etapa 72: A la recepción de la solicitud, el Emisor de Contenidos da instrucciones a un servidor multimedia y a un Emisor de Derechos para generar un RO mediante negociación;

En esta etapa, el RO generado por el servidor multimedia y el RI mediante negociación transmite la información para establecer un canal de comunicación encriptado entre el Equipo de Usuario y el servidor multimedia.

Etapa 73: Una vez generado el RO, el Emisor de Contenidos envía al Equipo de Usuario un mensaje que transmite información de indicación, tal como un RUL, correspondiente al RO.

Etapa 74: El Equipo de Usuario solicita el RO desde el Emisor de Derechos, con la información de indicación que se transmite en la demanda.

Etapa 75: El Emisor de Derechos envía el RO al Equipo de Usuario;

Etapa 76: El Equipo de Usuario y el servidor multimedia establecen el canal de comunicación encriptado mediante negociación utilizando la información para establecer el canal de comunicación encriptado transmitida en el RO y

Etapa 77: El servidor multimedia transmite datos multimedia al Equipo de Usuario a través del canal de comunicación encriptado.

El Equipo de Usuario procesa los datos multimedia según la regla de uso de derechos de autor en el RO. Si los datos multimedia es un flujo multimedia, el proceso, en particular, puede ser la reproducción del flujo de datos multimedia. Dicho de otro modo, un reproductor de flujo de datos multimedia es simplemente una puesta en práctica ilustrativa de un procesador de datos multimedia.

En la segunda forma de realización anterior, el Emisor de Contenidos notifica al Equipo de Usuario el mensaje en el que se genera el RO y el Equipo de Usuario solicita obtener el RO desde el Emisor de Derechos. Existe otra manera para permitir al Equipo de Usuario obtener el RO, por ejemplo, el Emisor de Contenidos puede enviar el RO al Equipo de Usuario, por su propia iniciativa, después de que se genere el RO.

Además, el servidor multimedia puede ser un servidor de flujos de datos multimedia u otro tipo de servidor multimedia, tal como un servidor que proporciona un servicio de TV móvil o un servicio de descarga de ficheros.

El IPSec se puede utilizar para el procedimiento de establecer el canal de comunicación encriptado mediante negociación en la etapa 76; además, se pueden establecer otras rutas lógicas, que no se describirán aquí con más detalle.

Con referencia a la Figura 8, se representa un diagrama de bloques del sistema de protección digital de derechos de autor, según la segunda forma de realización de la presente invención.

El sistema de protección digital de derechos de autor incluye un servidor multimedia 620, un Emisor de Contenidos 630 y un Emisor de Derechos 640.

El servidor multimedia 620 está adaptado para memorizar datos multimedia; para negociar con el Emisor de Derechos 640 para generar una información de transmisión de RO para establecer un canal de comunicación encriptado; para negociar con un Equipo de Usuario con el uso de la información para establecer el canal de comunicación encriptado y para enviar datos multimedia bajo protección de derechos de autor al Equipo de Usuario con el canal de comunicación encriptado.

El Emisor de Contenidos 630 está adaptado para proporcionar la información multimedia para el Equipo de Usuario; para dar instrucciones al servidor multimedia 620 y al Emisor de Derechos 640 para negociar la generación de una información de transmisión de RO para establecer el canal de comunicación encriptado, cuando el Equipo de Usuario solicita la descarga de los datos multimedia y para enviar información de indicación correspondiente al RO al Equipo de Usuario.

El Emisor de Derechos 640 está adaptado para negociar con el servidor multimedia 620 para generar la información de transmisión de RO para establecer el canal de comunicación encriptado en función de la notificación desde el Emisor de Contenidos 630 y para enviar el RO al Equipo de Usuario en función de la información de indicación desde el usuario.

El servidor multimedia 620 puede ser un servidor de flujo de datos multimedia u otro servidor multimedia que proporcione otros servicios multimedia tal como un servicio de TV móvil y un servicio de descarga de ficheros.

En una forma de realización, el servidor multimedia 620 incluye: una unidad de memorización de datos multimedia 622 adaptada para memorizar datos multimedia; una unidad de negociación de RO 623 adaptada para negociar con un Emisor de Derechos 640 para generar una información de transmisión de RO para establecer un canal de comunicación encriptado, una unidad de negociación de canal 624 adaptada para negociar con un Equipo de Usuario la utilización de la información para establecer el canal de comunicación encriptado y una unidad de provisión de datos multimedia 625 adaptada para proporcionar datos multimedia bajo protección de derechos de autor para el Equipo de Usuario a través del canal de comunicación encriptado.

El IPSec se puede utilizar por el servidor multimedia y el Equipo de Usuario para establecer el canal de comunicación encriptado y la unidad de negociación de canal 624 puede ser un controlador IPSec.

Las formas de realización de la invención han sido descritas anteriormente, pero el alcance de la invención no está limitado a estas formas de realización. A un experto en esta técnica se le ocurrirá fácilmente toda clase de variaciones o sustituciones sin desviarse del alcance técnico de la invención cuyas modificaciones quedarán dentro del alcance de protección de la invención. En consecuencia, el alcance de la invención se definirá por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método de protección digital de derechos de autor, que comprende:

la negociación entre un servidor de flujo de datos multimedia y un Emisor de Derechos para generar una información de transmisión de Objeto de Derecho para establecer un canal de comunicación encriptado, en donde la información para establecer el canal de comunicación encriptado, que se soporta en el Objeto de Derecho, es información de autenticación parar establecer una comunicación de IPSec entre el Equipo de Usuario y el servidor de flujos de datos multimedia;

el establecimiento, por un Equipo de Usuario, del canal de comunicación encriptado para el servidor de flujos de datos multimedia utilizando la información para establecer el canal de comunicación encriptado que se transmite en el Objeto de Derecho, a la recepción del Objeto de Derecho y

el envío, por el servidor de flujo de datos multimedia, de datos multimedia al Equipo de Usuario a través del canal de comunicación encriptado;

en donde el establecimiento del canal de comunicación encriptado comprende: la negociación entre el Equipo de Usuario y el servidor de flujos de datos multimedia para establecer una primera fase de la Asociación de Seguridad de IPSec y una segunda fase de la asociación de seguridad de IPSec; en donde, al establecer la primera fase de la asociación de seguridad de IPSec, la información de autenticación para establecer la comunicación de IPSec transmitida en el Objeto de Derecho se utiliza para la verificación de la identidad del Equipo de Usuario y del servidor de flujo de datos multimedia;

en donde el canal de comunicación encriptado se establece con la seguridad de protocolo Internet (IPSec).

2. El método de protección digital de derechos de autor según la reivindicación 1, en donde la información para establecer el canal de comunicación encriptado, transmitida en el Objeto de Derecho, es información de confirmación del uso de derechos de autor.

3. El método de protección digital de derechos de autor según la reivindicación 2, en donde el establecimiento del canal de comunicación encriptado comprende: la autenticación, por el servidor de flujo de datos multimedia, de la información de confirmación del uso de los derechos de autor proporcionada por el Equipo de Usuario y la negociación entre el servidor de flujos de datos multimedia y el Equipo de Usuario para establecer el canal de comunicación encriptado, después de que se realice satisfactoriamente la autenticación.

4. El método de protección digital de derechos de autor según la reivindicación 1, en donde la recepción del Objeto de Derecho por el Equipo de Usuario comprende la recepción del Objeto de Derecho enviado desde el Emisor de Derechos o un Emisor de Contenidos.

5. Un sistema de protección digital de derechos de autor, que comprende un servidor de flujo de datos multimedia y un Emisor de Derechos, en donde:

el servidor de flujo de datos multimedia está adaptado para memorizar datos multimedia; para negociar con el Emisor de Derechos con el fin de generar una información de soporte de Objeto de Derecho para establecer un canal de comunicación encriptado; para negociar con un Equipo de Usuario la utilización de la información para establecer el canal de comunicación encriptado y para enviar datos multimedia, bajo protección de derechos de autor, al Equipo de Usuario a través del canal de comunicación encriptado y

el Emisor de Derechos está adaptado para negociar con el servidor de flujo de datos multimedia con el fin de generar la información de soporte de Objeto de Derecho para establecer el canal de comunicación encriptado y enviar el Objeto de Derecho al Equipo de Usuario;

en donde la información para establecer el canal de comunicación encriptado transmitida en el Objeto de Derecho es la información de autenticación para establecer la comunicación de IPSec entre el Equipo de Usuario y el servidor de flujos de datos multimedia y

en donde el establecimiento del canal de comunicación encriptado comprende: la negociación entre el Equipo de Usuario y el servidor de flujos de datos multimedia para establecer una primera fase de asociación de seguridad de IPSec y una segunda fase de asociación de seguridad de IPSec; en donde, al establecer la primera fase de la asociación de seguridad de IPSec, la información de autenticación para establecer la comunicación de IPSec transmitida en el Objeto de Derecho se utiliza para la verificación de identidad del Equipo de Usuario y del servidor de flujos de datos multimedia:

en donde el canal de comunicación encriptado se establece con la seguridad de protocolo de Internet (IPSec).

6. El sistema de protección digital de derechos de autor según la reivindicación 5 que comprende, además, un Emisor de Contenidos para proporcionar información multimedia para el Equipo de Usuario y dar instrucciones al servidor de flujos de datos multimedia y al Emisor de Derechos para negociar la generación del Objeto de Derecho cuando el Equipo de Usuario solicite la descarga de los datos multimedia.

7. El sistema de protección digital de derechos de autor según la reivindicación 5 que comprende, además, un Emisor de Contenidos, en donde

el Emisor de Contenidos está adaptado para proporcionar información multimedia para el Equipo de Usuario; para dar instrucciones al servidor de flujos de datos multimedia y al Emisor de Derechos para negociar la generación del Objeto de Derecho, cuando el Equipo de Usuario solicite la descarga de los datos multimedia y para enviar el Objeto de Derecho al Equipo de Usuario.

8. Un servidor de flujo de datos multimedia, que comprende:

una unidad de memorización de datos multimedia adaptada para memorizar datos multimedia;

una unidad de negociación de Objeto de Derecho adaptada para negociar con un Emisor de Derechos para generar una información de soporte del Objeto de Derecho para establecer un canal de comunicación encriptado, en donde la información para establecer el canal de comunicación encriptado, que se soporta en el Objeto de Derecho es la información de autenticación para establecer una comunicación de IPSec entre el Equipo de Usuario y el servidor de flujo de datos multimedia;

una unidad de negociación de canal, adaptada para negociar con un Equipo de Usuario la utilización de la información para establecer el canal de comunicación encriptado, en donde el establecimiento del canal de comunicación encriptado comprende: la negociación entre el Equipo de Usuario y el servidor de flujo de datos multimedia para establecer una primera fase de la asociación de seguridad de IPSec y una segunda fase de la asociación de seguridad de IPSec; en donde, al establecer la primera fase de la asociación de seguridad de IPSec, la información de autenticación para establecer la comunicación de IPSec transmitida en el Objeto de Derecho se utiliza para verificación de la identidad del Equipo de Usuario y del servidor de flujo de datos multimedia y

una unidad de provisión de datos multimedia adaptada para proporcionar los datos multimedia bajo protección de derechos de autor al Equipo de Usuario a través del canal de comunicación encriptado;

en donde el canal de comunicación encriptado se establece con la seguridad de protocolo de Internet (IPSec).

9. Un Equipo de Usuario que comprende:

un explorador adaptado para explorar información multimedia proporcionada por un Emisor de Contenidos y para solicitar la descarga de datos multimedia;

un Agente de DRM adaptado para obtener información para establecer un canal de comunicación encriptado que se soporta en un Objeto de Derecho recibido, en donde la información para establecer el canal de comunicación encriptado que se soporta en el Objeto de Derecho es la información de autenticación para establecer la comunicación de IPSec entre el Equipo de Usuario y el servidor de flujo de datos multimedia y para establecer el canal de comunicación encriptado con un servidor de flujo de datos multimedia utilizando la información, en donde el establecimiento del canal de comunicación encriptado comprende: la negociación entre el Equipo de Usuario y el servidor de flujo de datos multimedia para establecer una primera fase de asociación de seguridad de IPSec y una segunda fase de asociación de seguridad de IPSec; en donde, al establecer la primera fase de asociación de seguridad de IPSec, la información de autenticación para establecer la comunicación de IPSec, transmitida en el Objeto de Derecho, se utiliza para verificación de identidad del Equipo de Usuario y del servidor de flujo de datos multimedia y

un procesador multimedia adaptado para procesar los datos multimedia transmitidos a través del canal de comunicación encriptado;

en donde el canal de comunicación encriptado se establece con la seguridad de protocolo de Internet (IPSec).

10. El Equipo de Usuario según la reivindicación 9 que comprende, además, un controlador de IPSec, que está adaptado para establecer el canal de comunicación encriptado para el controlador de IPSec del servidor de flujo de datos multimedia utilizando la información para establecer el canal de comunicación encriptado, cuando se solicita por el Agente de Gestión Digital de Derechos.

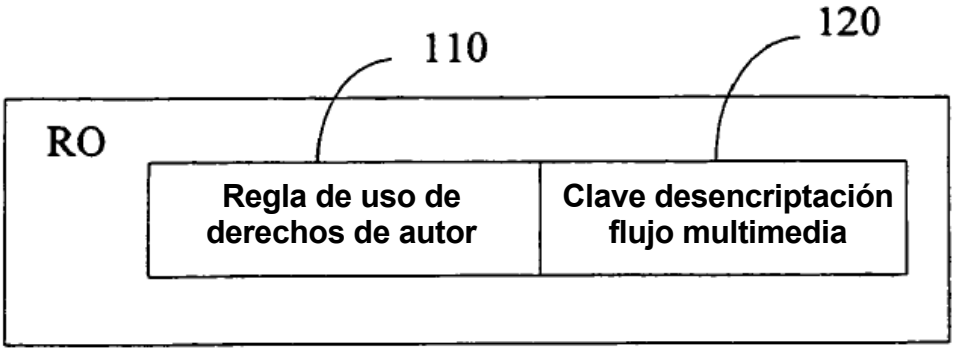

Figura 1

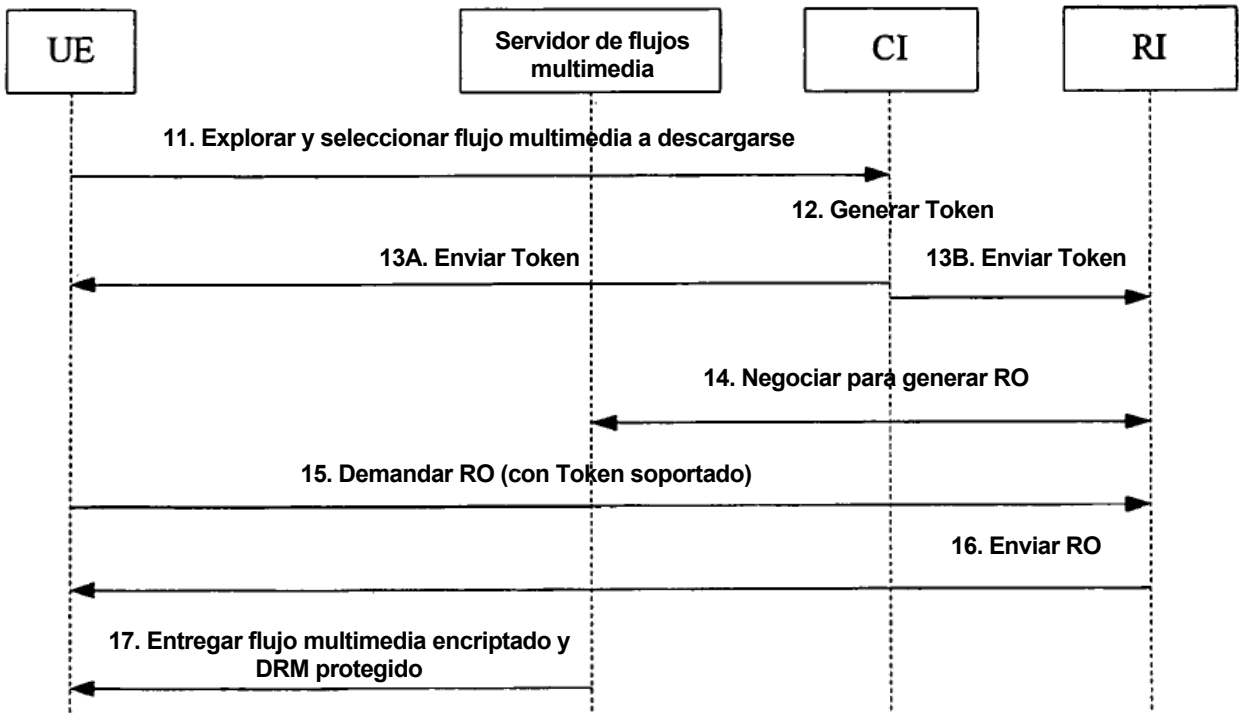

Figura 2

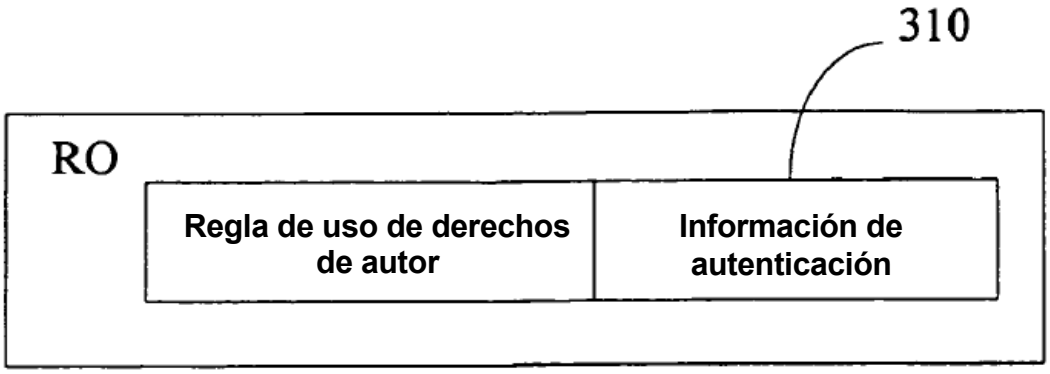

Figura 3

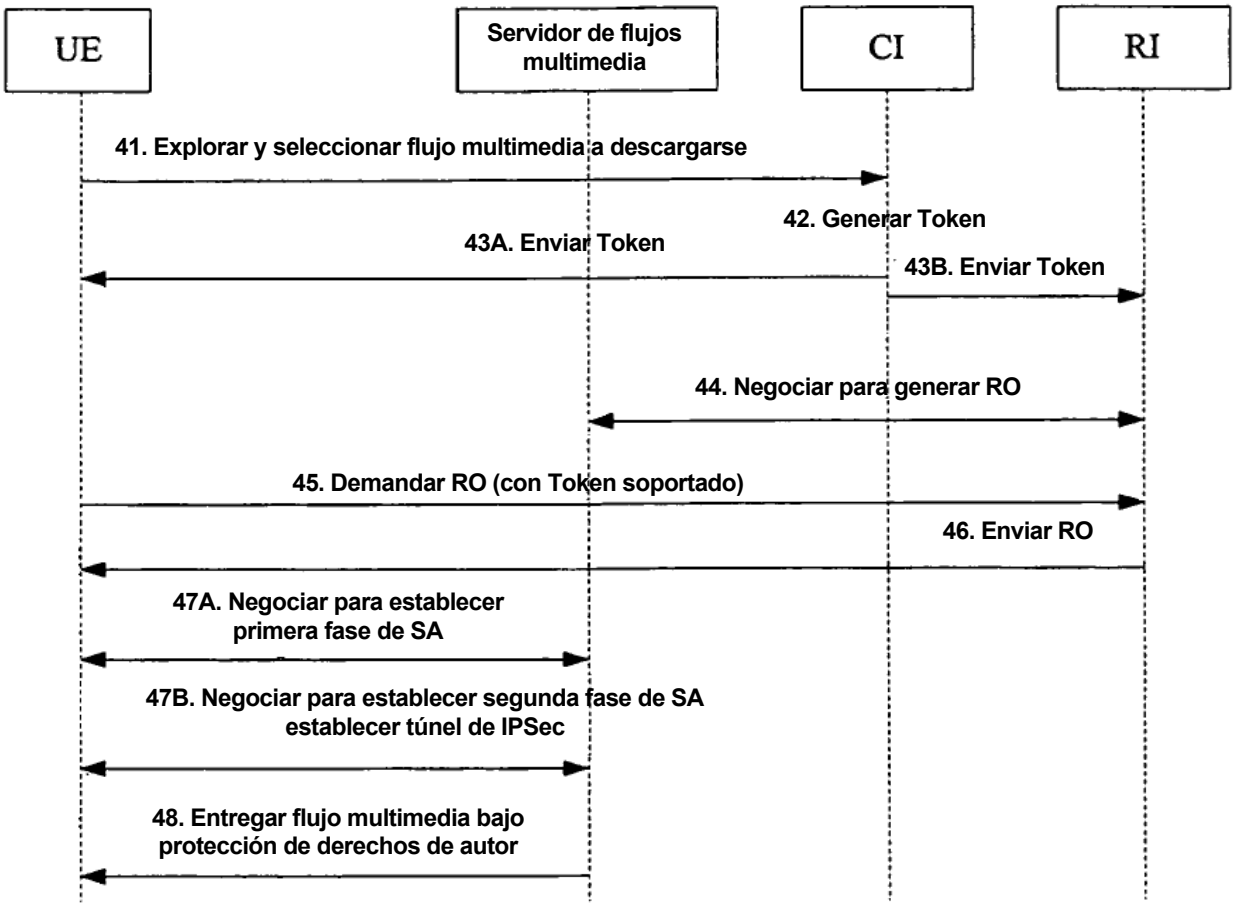

Figura 4

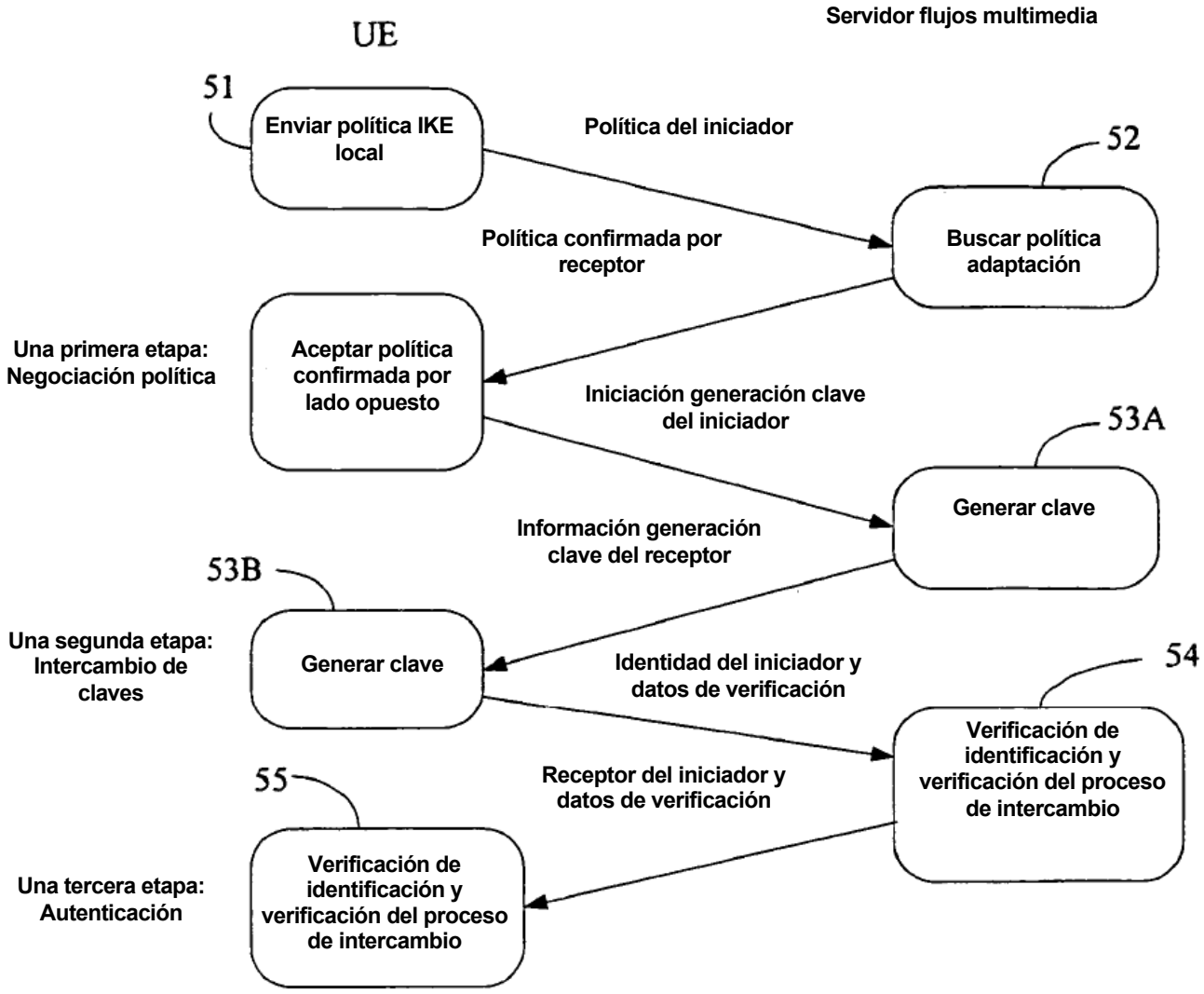
UE
Servidor flujos multimedia
51
Enviar política IKE local
Política del iniciador
52
Buscar política adaptación
Política confirmada por receptor
Una primera etapa: Negociación política
Aceptar política confirmada por lado opuesto
Iniciación generación clave del iniciador
53A
Generar clave
Información generación clave del receptor
53B
Una segunda etapa: Intercambio de claves
Generar clave
Identidad del iniciador y datos de verificación
54
Verificación de identificación y verificación del proceso de intercambio
Receptor del iniciador y datos de verificación
55
Una tercera etapa: Autenticación
Verificación de identificación y verificación del proceso de intercambio

Figura 5

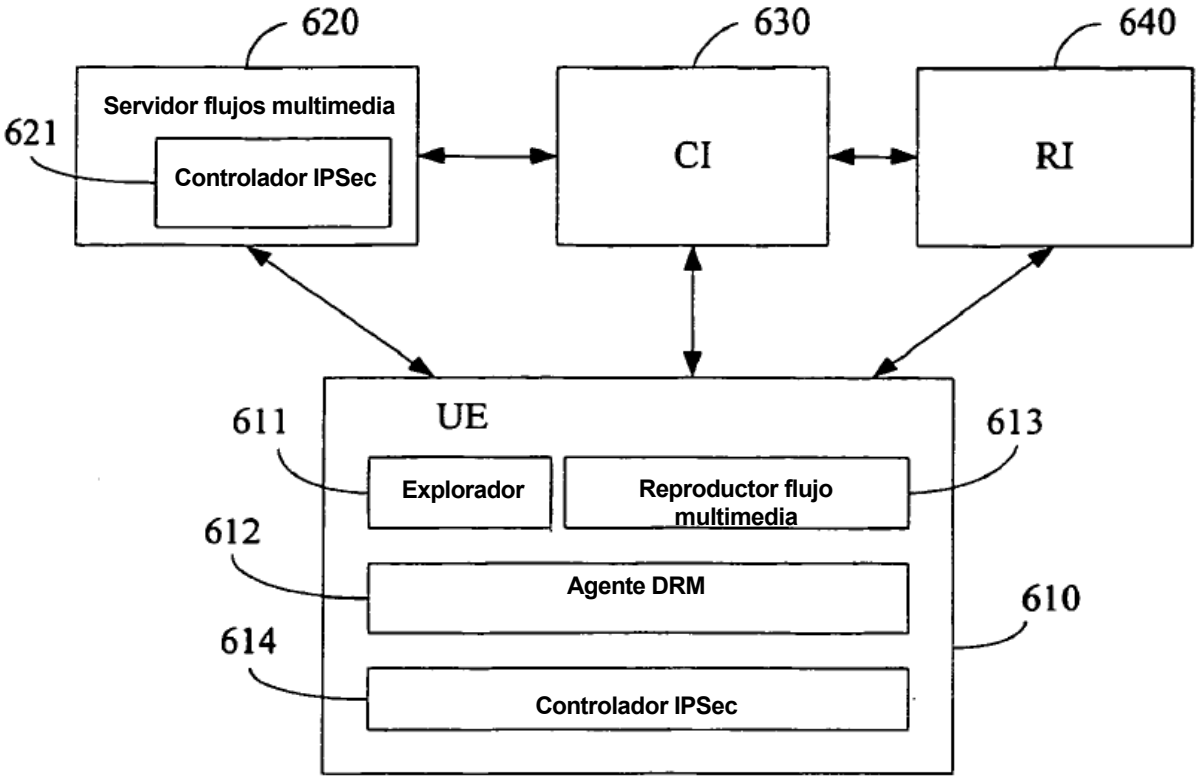

Figura 6

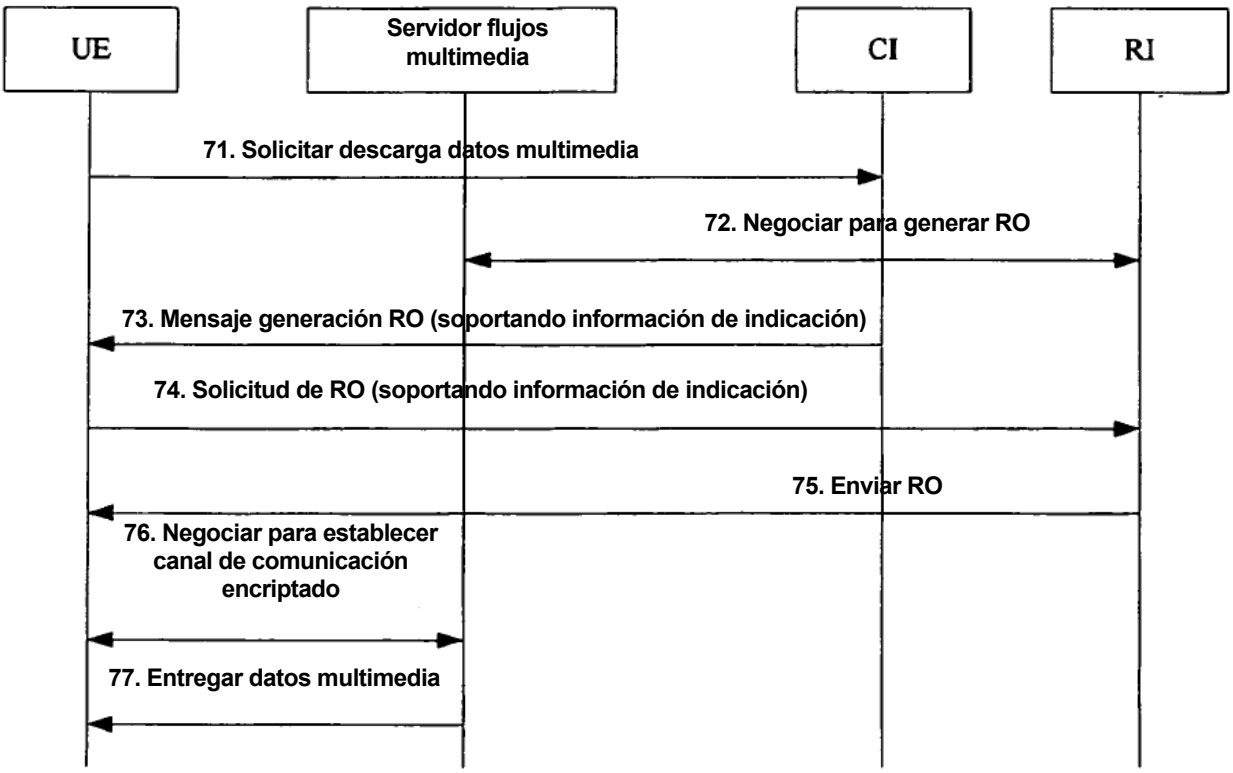

Figura 7

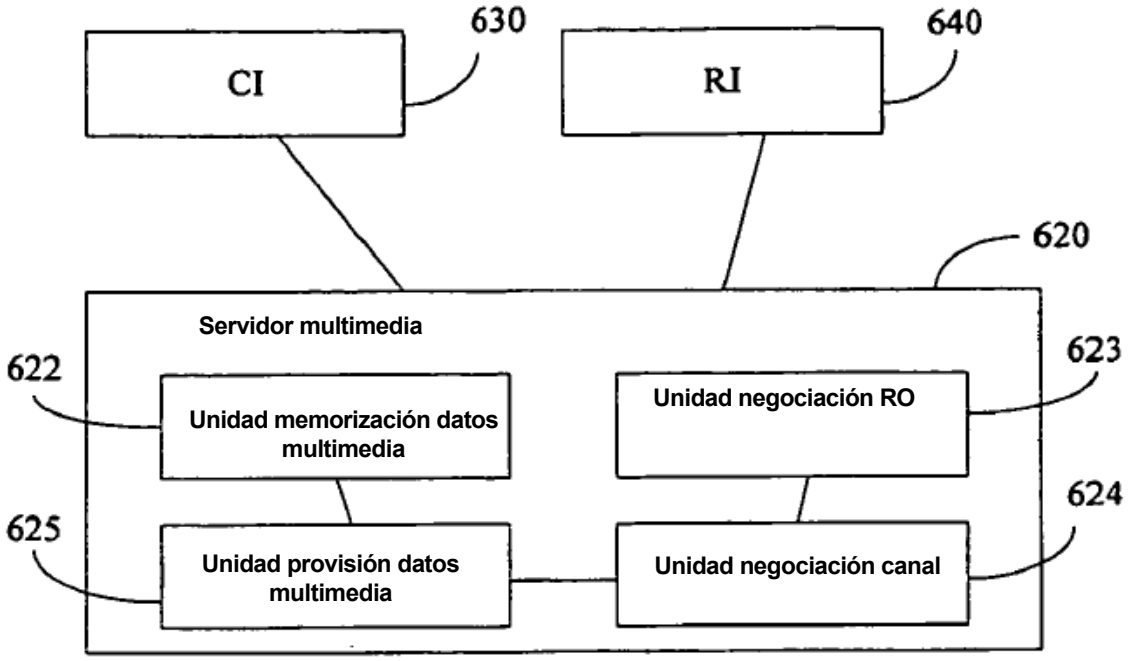
630
CI
640
RI
620
Servidor multimedia
622
Unidad memorización datos multimedia
623
Unidad negociación RO
624
625
Unidad provisión datos multimedia
Unidad negociación canal

Figura 8