(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 373 254**

(51) Int. CI.:
H04L 29/06 (2006.01)
H04N 7/173 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08760193 .6**
(96) Fecha de presentación: **29.05.2008**
(97) Número de publicación de la solicitud: **2279598**
(97) Fecha de publicación de la solicitud: **02.02.2011**

(54) Título: **SEGURIDAD IPTV EN UNA RED DE COMUNICACIÓN.**

(45) Fecha de publicación de la mención BOPI:
01.02.2012

(45) Fecha de la publicación del folleto de la patente:
01.02.2012

(73) Titular/es:
Telefonaktiebolaget L M Ericsson (PUBL)
164 83 Stockholm, SE

(72) Inventor/es:
EDLUND, Peter;
ÅSTRÖM, Bo y
LINDHOLM, Fredrik

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Seguridad IPTV en una red de comunicación

Campo técnico

La invención se refiere al campo de la Seguridad IPTV en una Red de Comunicación, y en particular al campo del establecimiento de una sesión IPTV segura.

Antecedentes

Los servicios de difusión sobre una red IP se conocen como IPTV. La IPTV se difunde típicamente usando una red de acceso de banda ancha, en la que los canales se transmiten sobre una red de banda ancha desde una súper cabecera hasta un receptor multimedia digital (STB) del usuario final. Un ejemplo de un servicio IPTV es la TV de Difusión, en la cual la mayoría de los canales IPTV comunes, así como canales adicionales con baja penetración, se transmiten sobre una red de difusión desde una súper cabecera hasta un receptor multimedia digital (STB) del usuario final. Para minimizar el ancho de banda requerido para estas transmisiones es deseable usar las técnicas de multidifusión a través de la red.

De manera similar, en las redes móviles es deseable usar la entrega de difusión/multidifusión de la TV Móvil (MTV). El Servicio de Multidifusión de Difusión Multimedia (MBMS) y la Difusión de Vídeo Digital – De Mano (DVB-H) son ejemplos de tecnologías de difusión de MTV. Un teléfono móvil (tal como un Equipo de Usuario, UE) que tiene un cliente MTV se puede pensar como un equivalente a un STB en las implementaciones de MTV que reciben contenido de una súper cabecera.

En una adaptación típica el contenido se entrega por una Función de Entrega de Medios (MDF) que es un servidor de entrega de contenidos controlado por un Servidor de Aplicaciones (AS) del Subsistema Multimedia IP (IMS) para TV móvil (que usa un portador del Servicio de Multidifusión de Difusión Multimedia, MBMS, o un portador del Servicio de Paquetes Conmutados, PSS) o un IMS AS para IPTV (que usa entrega unidifusión o multidifusión).

La siguiente descripción se refiere a un UE por simplicidad, aunque se apreciará que igualmente aplica donde se recibe IPTV en otro tipo de receptor de IPTV tal como un STB. Con referencia a la Figura 1 aquí dentro, y antes de que pueda comenzar la comunicación entre la MDF y el UE 1, el UE 1 y la función de control de entrega de contenido (una Función de Aplicación de Red, NAF 2, que puede ser un MTV AS o un IPTV AS) debe participar en un procedimiento de Autentificación Genérica de Inicialización (GBA) (mostrado en los pasos S1 a S8) para establecer las claves de GBA (la Ks_naf de la que se derivan la MUK y la MRK. La Ks_naf se describe más adelante) para la autentificación y la protección del servicio.

El resultado de un procedimiento GBA exitoso es el establecimiento de un identificador de transacción de inicialización (BTID), generado por una Función de Servidor de Inicialización (BSF) 3, y una clave compartida, la Ks_Naf que se genera localmente por un USIM/SIM 4 en el UE 1 durante la inicialización (S5). El BTID se arrastra por el UE 1 desde la BSF 3 mediante el uso de HTTP, mostrado en el paso S4 de la Figura 1. La Ks_Naf y el B_TID se almacenan como un parte del contexto del UE en un área asegurada en el UE (S4). La Ks_Naf está disponible para el uso posterior para derivar las claves específicas de aplicaciones (MUK, MRK) y para cifrar claves de Largo Plazo (MKS) cuando se entrega al UE 1.

La BSF 3 recupera una clave de contenidos (Ck) y una clave de integridad (Ik), que se envían como parte de un Vector de Autentificación desde un Servidor Local de Abonado (HSS) 5 durante el procedimiento de GBA. La Ks_naf se calcula por la BSF 3 concatenando la Ck y la Ik (y una operación similar se realiza por el USIM/SIM 4 en el UE 1) y se almacena en la BSF 3 para referencia futura por el UE 1.

Para recuperar los datos entregados usando HTTP desde un MTV AS/IPTV AS/BM-SC (NAF), el UE primero debe ser autentificado por el MTV AS. Ejemplos de tales datos incluyen una Guía Electrónica de Programas (EPG) o una Guía Electrónica de Servicios (ESG). Para autentificar el UE, el UE señala el BTID y la Ks_naf en una petición HTTP (HTTP acepta la autentificación como se define en la RFC 2617) enviada desde el UE 1 al MTV AS.

Cuando un UE 1 está implicado en un procedimiento de señalización HTTP donde se usa la GBA para propósitos de autentificación, el UE 1 interactúa con una entidad funcional llamada el Intermediario de Autentificación (AP), no se muestra en la Figura 1. El AP conoce el BTID que representa el UE 1 durante este proceso y la Ks_naf que corresponde con el BTID.

Con referencia a la Figura 2, se ilustra el procedimiento por el cual un nodo tal como la NAF recupera las claves de largo plazo. Los procedimientos de señalización de MTV requieren la entrega de claves de largo plazo para proteger el contenido IPTV que va a ser enviado al UE 1. Durante estos procedimientos de señalización, el UE 1 interactúa con el MTV AS, que no es consciente del BTID usado en los procedimientos de señalización anteriores. No obstante, el MTV AS requiere la Ks_naf para usarla para el cifrado de las claves de contenido de largo plazo como parte de los procedimientos de acceso de contenido. No obstante, el MTV AS no tiene acceso a la Ks_naf, que se almacena en la BSF 2, y así no es posible actualmente.

La WO 2007/085186 describe un método de gestión de claves de secuencias de medios, pero no proporciona un modo de proteger las claves enviadas al UE. La WO 2007/008120 se refiere a mejorar la protección de privacidad y la autentificación, pero requiere que se contacte una NAF cada vez que el UE debe ser autentificado, conduciendo al desperdicio de señalización.

Resumen

Los inventores se han dado cuenta que hay un problema en la autentificación de un Equipo de Usuario u otro dispositivo de recepción de IPTV antes de comenzar una sesión. Se propone un método para proporcionar un Servidor de Aplicaciones de TV Móvil con un BTID asociado con el UE y que permite al MTV AS actuar como una Función de Aplicación de Red en la arquitectura GBA.

De acuerdo con un primer aspecto de la invención, allí se proporciona un método para establecer una sesión IPTV segura. Un Servidor de Aplicaciones (AS) recibe un mensaje de invitación desde un nodo de recepción de IPTV tal como un teléfono móvil o un Receptor Multimedia Digital (STB) para poner en marcha una sesión IPTV. El mensaje de invitación incluye un Identificador de Transacción de Inicialización (BTID) asociado con el nodo de recepción. El AS envía una petición de autentificación a un Servidor de Protección de Acceso de Servicio, la petición de autentificación que incluye el BTID. El AS entonces recibe desde el Servidor de Protección de Acceso de Servicio una respuesta de autentificación, que incluye una clave de largo plazo asociada con el nodo de recepción de IPTV, la clave de largo plazo que se ha proporcionado previamente al nodo de recepción de IPTV. Se envía una petición a un nodo proveedor de contenido IPTV, la petición que identifica el nodo de recepción de IPTV. El AS entonces cifra una clave de cifrado de medios que se usa para cifrar los medios enviada por el proveedor de contenido de IPTV, usando la clave de largo plazo recibida. Una respuesta de invitación se envía entonces al nodo de recepción de IPTV, la respuesta que incluye la clave de cifrado de medios cifrada. La invención dota el AS con una clave de largo plazo que se puede usar para cifrar la clave de cifrado de medios.

Como opción, el mensaje de invitación es un mensaje de Invitación del Protocolo de Inicio de Sesiones (SIP), y el BTID está incluido en una cabecera de Autorización Intermediaria. El Servidor de Protección de Acceso de Servicio es opcionalmente una Función de Servidor de Inicialización (BSF). La invención es particularmente adecuada para usar en el campo de la IPTV Móvil, y así como otra opción, la sesión de IPTV es una sesión de IPTV Móvil, y el AS es un IPTV AS Móvil.

Opcionalmente, la sesión IPTV es o bien una difusión de IPTV lineal, una unidifusión de IPTV lineal, o una unidifusión de Vídeo bajo Demanda.

Opcionalmente, si la sesión de IPTV es una unidifusión entonces la clave de cifrado de medios es una clave de contenido, y si la sesión de IPTV es una difusión entonces la clave de cifrado de medios es una clave de grupo.

En una realización opcional, la clave de cifrado de medios se envía desde el AS al nodo proveedor de contenido de IPTV, y en una realización alternativa la clave de cifrado de medios se recibe en el AS desde el nodo proveedor de contenido de IPTV. La clave de cifrado de medios se puede enviar desde el AS al nodo proveedor de contenido de IPTV para uso posterior por el nodo proveedor de contenido de IPTV en los medios cifrados enviados al nodo de recepción de IPTV. Alternativamente, donde se genera la clave de cifrado de medios por el nodo proveedor de contenido de IPTV, le proporciona al AS permitir al AS cifrarlo usando la clave de largo plazo y enviarla al nodo de recepción de IPTV. Donde la clave de cifrado de medios es una clave de contenido, el AS la envía opcionalmente al nodo proveedor de contenido de IPTV.

De acuerdo con un segundo aspecto de la invención, allí se proporciona un AS. El AS comprende un primer receptor para recibir un mensaje de invitación desde un nodo de recepción de IPTV para poner en marcha una sesión de IPTV. El mensaje de invitación incluye un BTID asociado con el nodo de recepción de IPTV. Se proporciona un primer transmisor para enviar una petición de autentificación a un Servidor de Protección de Acceso de Servicio, la petición de autentificación que incluye el BTID. Se proporciona un segundo receptor para recibir desde el Servidor de Protección de Acceso de Servicio una respuesta de autentificación, la respuesta de autentificación que incluye una clave de largo plazo asociada con el nodo de recepción de IPTV. Señalar que la clave de largo plazo ya ha sido proporcionada al nodo de recepción de IPTV. Se usa un segundo transmisor para enviar una petición a un nodo proveedor de contenido de IPTV, la petición que identifica el nodo de recepción de IPTV. Se proporciona un procesador para cifrar una clave de cifrado de medios usando la clave de largo plazo recibida. La clave de cifrado de medios es la clave usada por el nodo proveedor de contenido de IPTV para cifrar el contenido de IPTV enviado al nodo de recepción de IPTV. Se proporciona un tercer transmisor para enviar un mensaje de respuesta de invitación al nodo de recepción de IPTV, el mensaje de respuesta de invitación que incluye la clave de cifrado de medios cifrada. Esto permite al nodo de recepción de IPTV acceder a la clave de cifrado de medios para descifrar los medios posteriormente enviados a él desde el nodo proveedor de contenido de IPTV.

El AS comprende además opcionalmente un tercer receptor para recibir un mensaje desde el nodo proveedor de contenido de IPTV que incluye la clave de cifrado de medios, en un escenario donde el nodo proveedor de contenido de IPTV genera la clave de cifrado de medios. Alternativamente, el segundo transmisor se dispone para enviar la clave de cifrado de medios en la petición al nodo proveedor de contenido de IPTV para uso posterior por el nodo

proveedor de contenido de IPTV en los medios de cifrado enviados al nodo de recepción de IPTV.

Como opción, el mensaje de invitación es un mensaje de Invitación de SIP, y el BTID se incluye en una cabecera de Autorización Intermediaria. El AS es opcionalmente un IPTV AS Móvil y la sesión IPTV es una sesión de IPTV Móvil. La sesión de IPTV es opcionalmente o bien una difusión de IPTV lineal, una unidifusión de IPTV lineal, o una unidifusión de Vídeo bajo Demanda.

De acuerdo con un tercer aspecto de la invención, allí se proporciona un nodo de recepción de IPTV que comprende una memoria para almacenar un BTID y una clave de largo plazo asociada con el nodo de recepción de IPTV. Se proporciona un transmisor para enviar a un AS un mensaje de invitación para iniciar una sesión de IPTV, el mensaje de invitación que incluye el BTID. Se proporciona un primer receptor para recibir desde el AS un mensaje de respuesta, el mensaje de respuesta que incluye una clave de cifrado de medios cifrada usando la clave de largo plazo. Esta se puede descifrar usando un primer procesador y la clave de largo plazo almacenada. Se proporciona un segundo receptor para recibir el contenido de medios de IPTV enviado desde un nodo proveedor de contenido de IPTV, el contenido de medios de IPTV que se ha cifrado usando la clave de cifrado de medios. Se usa entonces un segundo procesador para descifrar el contenido de medios de IPTV usando la clave de cifrado de medios descifrada. Esto permite a un espectador ver los medios de IPTV.

Como opción, el nodo de recepción de IPTV es el Equipo de Usuario. Como opción adicional, el mensaje de invitación es un mensaje de Invitación de SIP, y el BTID se incluye en la cabecera de Autorización Intermediaria.

Breve descripción de los dibujos

La Figura 1 ilustra esquemáticamente en un diagrama de bloques una arquitectura y señalización de Autentificación Genérica de Inicialización;

La Figura 2 es un diagrama de señalización que muestra la señalización requerida para que una NAF obtenga una clave de largo plazo;

La Figura 3 es un diagrama de señalización que muestra la señalización requerida para poner en marcha un canal de IPTV de difusión con un cliente de MTV de acuerdo con una realización de la invención;

La Figura 4 es un diagrama de señalización que muestra la señalización requerida para poner en marcha una sesión de unidifusión de Vídeo bajo Demanda de acuerdo con una realización de la invención;

La Figura 5 es un diagrama de señalización que muestra la señalización requerida para poner en marcha una sesión de unidifusión de TV lineal de acuerdo con una realización de la invención;

La Figura 6 ilustra esquemáticamente en un diagrama de bloques un Servidor de Aplicaciones de acuerdo con una realización de la invención; y

La Figura 7 ilustra esquemáticamente en un diagrama de bloques un nodo de recepción de IPTV de acuerdo con una realización de la invención.

Descripción detallada

Cuando un terminal tal como un UE (o cualquier otro nodo de recepción para recibir IPTV) desea acceder a un canal de IPTV (que puede ser difundido, unidifundido, multidifundido, Vídeo bajo Demanda o cualquier otro tipo de entrega que requiere protección de contenido de medios), envía un mensaje de Invitación de SIP. En una red IMS, el mensaje de Invitación de SIP se envía a una Función de Control de Sesión de Llamada Intermediaria (P-CSCF). El mensaje de Invitación de SIP se encamina a un Servidor de Aplicaciones (AS) tal como un Servidor de Aplicaciones de TV Móvil (MTV AS). De acuerdo con la invención, el UE incluye el BTID en una Cabecera de Autorización Intermediaria en el mensaje de Invitación de SIP. El BTID permite al MTV AS para recuperar la Ks_naf a partir de la BSF, y el MTV AS entonces puede usar la Ks_naf para cifrar las claves de contenido de largo plazo cuando se entregan al UE.

Con referencia ahora a la Figura 3, allí se muestra la señalización para poner en marcha una difusión de TV lineal con un cliente de MTV 6 de acuerdo con una primera realización específica de la invención. La difusión en este ejemplo está en el contexto de un entorno de MTV, y así el cliente de MTV 6 es parte del Equipo de Usuario 1. Se apreciará que la siguiente señalización se puede modificar para poner en marcha una difusión de TV lineal con un nodo de recepción de IPTV distinto, tal como un STB. La siguiente numeración corresponde con la numeración en la Figura 2.

S9. El cliente de MTV 6 envía un mensaje de Invitación de SIP a una P-CSCF 7. El mensaje de Invitación de SIP incluye una indicación de que se requiere una entrega de IPTV de difusión Lineal. El BTID, que previamente se ha proporcionado al UE en un procedimiento de inicialización de GBA, se incluye en la Cabecera de Autorización Intermediaria del mensaje SIP.

S10. La Invitación de SIP se reenvía desde la P-CSCF 7 a una Función de Control de Sesión de Llamada de

Servicio (S-CSCF) 8 en la red de IMS.

S11. La S-CSCF 8 reenvía la invitación SIP al MTV AS 9.

S12-13. El MTV AS 9 usa el BTID recibido para autentificar el cliente de MTV 6 con la BSF 3, y para recuperar los atributos de la Ks_naf y la Ks_naf específicos desde la BSF 3. Tales atributos incluyen el periodo de validez del tiempo de vida de la Ks_naf, un sello de tiempo etc.

S14-15. El MTV AS 9, proporciona una MSK (Clave de Sesión de MBMS) y una MTK (Clave de Tráfico de MBMS) para el cifrado en un BM-SC 10, o MTK MSK cifrados juntos con la MTK o (MSK) y las Claves de Tráfico de MBMS (MTK). El BM-SC 10 es responsable de proporcionar la TV de difusión lineal al cliente de MTV 6 y la distribución de las claves de tráfico actualizadas a los clientes que acceden a la sesión de MBMS.

S16. El MTV AS 9 cifra las claves de sesión usando la Ks_naf recuperada.

S16a. Un mensaje 200 OK de SIP se envía desde el MTV AS 9 a la S-CSCF 8, el mensaje 200 OK que incluye las claves de sesión MSK cifradas usando la Ks_naf recuperada.

S17. El mensaje 200 OK de SIP se envía desde la S-CSCF 8 a la P-CSCF 7.

S18-19. La funcionalidad de Control de Política y de Tarificación (PCC) del IMS se usa, aunque la PCRF 11 no realiza ningún refuerzo de política o reserva de recursos o asignación de un portador (definido por los requerimientos de QoS) para la entrega de IPTV de difusión o multidifusión.

S20. El mensaje 200 OK de SIP se envía desde la P-CSCF 7 al cliente de MTV 6, que dota el cliente de MTV con las claves de sesión MSK.

S21. El contenido de medios cifrado se entrega desde el BM-SC 10 al cliente de MTV 6. El cliente de MTV 6 usa la MSK recibida para descifrar las claves de contenido que se envían como parte del contenido de medios, que permite al cliente de MTV 6 descifrar el contenido de medios. El usuario final puede ver entonces el contenido de medios.

Se debería señalar que las claves de contenido se pueden refrescar más tarde. Esto se realiza mediante la inclusión de una clave de tráfico cifrada MSK MKT en los datos de medios enviados al cliente de MTV.

La primera realización específica de la invención permite al MTV AS 6 recibir el BTID asociado con un UE y el material clave de manera que el MTV AS puede actuar como una NAF en la arquitectura de GBA. El MTV AS se dota por lo tanto con el BTID que se usa más tarde para recuperar la Ks_naf desde la BSF 3, que a su vez se usa para cifrar las claves de sesión MSK para usar por el cliente de MTV 6.

Volviendo ahora a la Figura 4, allí se ilustra la señalización para poner en marcha una unidifusión de Vídeo bajo Demanda (VoD) de acuerdo con una segunda realización específica de la invención. La siguiente numeración corresponde a la numeración en la Figura 3:

S22. El cliente de MTV 6 envía un mensaje de Invitación de SIP a una P-CSCF 7. El mensaje de Invitación de SIP incluye una indicación de que se requiere la entrega de VoD de IPTV. El BTID, que se ha proporcionado previamente al UE en un procedimiento de inicialización de GBA, se incluye en la Cabecera de Autorización Intermediaria del mensaje de SIP.

S23. La Invitación de SIP se reenvía desde la P-CSCF 7 a una Función de Control de Sesión de Llamada de Servicio (S-CSCF) 8 en la red de IMS.

S24. La S-CSCF 8 reenvía la invitación de SIP al MTV AS 9

S25-26. El MTV AS 9 usa el BTID recibido para autentificar al cliente de MTV 6 con la BSF 3, y para recuperar los atributos de la Ks_naf y la Ks_naf específica a partir de la BSF 3. Tales atributos incluyen el periodo de validez del tiempo de vida de la Ks_naf, un sello de tiempo etc.

S 27-28. El MTV AS 9 y un Servidor de Contenidos 12 para proporcionar los medios de VoD al cliente de MTV 6 negocian las claves de contenido.

S 29-32. El MTV AS 9 y un Servidor de Contenidos 12 configuran el Servidor de Contenidos 12 con respecto a la entrega de contenido sobre una conexión RTP/UDP mediante la invocación de un procedimiento de puesta en marcha del RTSP para secuencias de audio y vídeo entre el Servidor de Contenidos 12 y el terminal.

S33. El MTV AS 9 cifra las claves de contenido usando la Ks_naf recuperada.

S33a. Se envía un mensaje 200 OK de SIP desde el MTV AS 9 a la S-CSCF 8, el mensaje 200 OK que incluye las claves de contenidos cifradas usando la Ks_naf recuperada.

S34. El mensaje 200 OK de SIP se envía desde la S-CSCF 8 a la P-CSCF 7.

S35-36. La funcionalidad de Control de Política y de Tarificación (PCC) del IMS realiza el control de política y el refuerzo y la reserva de recursos. En base a las reglas de PCC la PCRF 11 da instrucciones al GGSN para activar un contexto PDP secundario para que el portador transporte la secuencia de VoD para la entrega de IPTV unidifusión.

S37. El mensaje 200 OK de SIP se envía desde la P-CSCF 7 al cliente de MTV 6, dotando el cliente de MTV con las claves de contenido, las cuales el cliente de MTV 6 puede descifrar usando la Ks_naf.

S38-S41. La funcionalidad de PCC del IMS se usa para asignar un portador apropiado (QoS definida) para la entrega de IPTV unidifusión. Esta exposición de pasos muestra un establecimiento de portador controlado de red/contexto PDP, pero un establecimiento de portador controlado PDP sería igualmente aplicable para la invención.

S42. El cliente de MTV 6 requiere el contenido de VoD desde el Servidor de Contenidos 12.

S43. El Servidor de Contenidos responde con un mensaje 200 OK.

S44. El contenido de medios de VoD cifrado se entrega desde el Servidor de Contenidos 12 al cliente de MTV 6. El cliente de MTV 6 usa las claves de contenido descifradas para descifrar el contenido de medios. El usuario final puede ver entonces el contenido de medios.

Volviendo ahora a la Figura 6, allí de ilustra la señalización para poner en marcha una unidifusión de TV lineal de acuerdo con una tercera realización específica de la invención. La siguiente numeración corresponde a la numeración en la Figura 4:

S45. El cliente de MTV 6 envía un mensaje de Invitación de SIP a una P-CSCF 7. El mensaje de Invitación de SIP incluye una indicación de que se requiere la entrega lineal unidifusión. El BTID, que se ha proporcionado previamente al UE en el procedimiento de inicialización de la GBA, se incluye en la Cabecera de Autorización Intermediaria del mensaje SIP.

S46. La Invitación de SIP se reenvía desde la P-CSCF 7 a una Función de Control de Sesión de Llamada de Servicio (S-CSCF) 8 en la red IMS.

S47. La S-CSCF 8 reenvía la Invitación de SIP al MTV AS 9.

S48-49. El MTV AS 9 usa el BTID recibido para autentificar el cliente MTV 6 con la BSF 3, y para recuperar los atributos de la Ks_naf y la Ks_naf específicos, tales como un periodo de validez del tiempo de vida de la Ks_naf y un sello de tiempo a partir de la BSF 3.

S50-51. El MTV AS 9 y el Servidor de Contenidos 13 para proporcionar los medios de VoD al cliente de MTV 6 negocian las claves de contenido.

S52-55. El MTV AS 9 y el Servidor de Contenidos 13 negocian la puesta en marcha del RTSP para audio y vídeo.

S56. El MTV AS 9 cifra las claves de sesión usando la Ks_naf recuperada.

S56a. Un mensaje 200 OK de SIP se envía desde el MTV AS 9 a la S-CSCF 8, el mensaje 200 OK que incluye las claves de contenido cifradas usando la Ks_naf recuperada.

S57. El mensaje 200 OK de SIP se envía desde la S-CSCF 8 a la P-CSCF 7.

S58-59. La funcionalidad de Control de Política y Tarificación (PCC) del IMS realiza el control de política y refuerzo y reserva de recursos. En base a las reglas de PCC la PCRF 11 da instrucciones al GGSN para activar el contexto PDP secundario para que el portador transporte la secuencia de unidifusión para la entrega de IPTV.

S60. El mensaje 200 OK de SIP se envía desde la P-CSCF 7 al cliente de MTV 6, que dota al cliente de MTV con las claves de contenidos, que el cliente de MTV 6 puede descifrar usando la Ks_naf.

S61-S64. La funcionalidad de PCC del IMS se usa para asignar un portador adecuado (QoS definida) para la entrega de IPTV unidifusión. Esta exposición de pasos muestra un establecimiento de portador controlado de red/contexto PDP, pero un establecimiento de portador controlado del UE sería igualmente aplicable para la invención.

S65. El cliente de MTV 6 requiere el contenido unidifusión lineal desde el Servidor de Contenidos 13.

S66. El Servidor de Contenidos 13 responde con un mensaje 200 OK.

S67. Los medios lineales de IPTV unidifusión cifrados se entregan desde el Servidor de Contenidos 13 al cliente de MTV 6. El cliente de MTV 6 usa las claves de contenido descifradas para descifrar el contenido de medios. El

usuario final entonces puede ver el contenido de medios.

Con referencia ahora a la Figura 6, allí se ilustra esquemáticamente un Servidor de Aplicaciones de acuerdo con una realización de la invención. El Servidor de Aplicaciones es un MTV AS 9, como se describió anteriormente. El MTV AS 9 se dota con un primer receptor 14 para recibir el mensaje de Invitación de SIP desde el cliente de MTV 6. Como se describió anteriormente, el mensaje de Invitación de SIP incluye el BTID en la cabecera de Autorización Intermediaria. Se proporciona un primer transmisor 15 para enviar una petición de autentificación a la BSF 3, y se proporciona un segundo receptor 16 para recibir una respuesta desde la BSF 3. La respuesta incluye la Ks_naf. Se proporciona un segundo transmisor 17 para enviar una respuesta, que puede incluir una clave de cifrado de medios tal como una MSK+MTK, o una (MSK cifrada MTK)+MTK a un BM-SC 10 o un Servidor de Contenidos 13, y se proporciona un tercer receptor 18 para recibir una respuesta, que puede incluir una clave de cifrado de medios desde el nodo proveedor de contenido de televisión IP. Se usa un procesador 19 para cifrar la clave de cifrado de medios usando la Ks_naf recibida, y se proporciona un tercer transmisor 20 para enviar un 200 OK de SIP al cliente de MTV 6, el 200 OK que incluye la clave de cifrado de medios cifrada Ks_naf. Por supuesto, los transmisores pueden estar todos integrados en un transmisor único, y los receptores pueden estar todos integrados en un receptor único. Una memoria 21 también se proporciona para almacenar información tal como el BTID y la Ks_naf recibidos.

La Figura 7 está en el nodo de recepción de IPTV de acuerdo con una realización de la invención. El nodo de recepción de IPTV, en una red de MTV como se describió anteriormente, es un UE que comprende un cliente de MTV 6. El UE 22 se dota con una memoria 23 para almacenar el BTID y la Ks_naf proporcionados en los procedimientos de GBA. La memoria también almacena información asociada con la Ks_naf, tal como el periodo de validez del tiempo de vida de la Ks_naf. Se proporciona un transmisor 24 para enviar una Invitación de SIP al MTV AS 9, la Invitación de SIP que incluye el BTID en una cabecera de Autorización Intermediaria. Se proporciona un primer receptor 25 para recibir un 200 OK de SIP desde el MTV AS 9, el 200 OK de SIP que incluye las claves de cifrado de medios cifradas usando la Ks_naf. Se proporciona un primer procesador 26 para descifrar las claves de cifrado de medios usando la Ks_naf recuperada desde la memoria 23. Se proporciona un segundo receptor 27 para la recepción posterior del contenido de medios IPTV enviado desde el servidor de contenidos 13 o el BM-SC 10, el contenido que está cifrado usando las claves de cifrado de medios. Se proporciona un segundo procesador 28 para descifrar el contenido de medios de IPTV usando la clave de cifrado de medios descifrada. Por supuesto, los dos procesadores se pueden integrar en un procesador único, y los dos receptores se pueden integrar en un receptor único.

La invención asegura que un Servidor de Aplicaciones tal como un MTV AS recibe el BTID durante los procedimientos de acceso de contenido. Esto permite al MTV AS recuperar la clave Ks_naf desde la BSF, y reduce la señalización requerida ya que la NAF no necesita estar implicada. La Ks_naf se usa por el MTV AS para cifrar las claves de servicio (MSK), que son parte de la protección de contenido. Esto proporciona un procedimiento IMS común único para recuperar la Ks_naf y almacenarla en el MTV AS/IPTV para el servicio y la protección de contenido, independiente del tipo de acceso de servicio. Se requiere una sesión SIP única para poner en marcha el servicio y distribuir las claves de contenido derivadas de la Ks_naf al cliente de MTV. Adicionalmente, el BTID proporcionado al cliente en el procedimiento de GBA se puede reutilizar para varios tipos de señalización, tales como señalización HTTP y SIP.

Se apreciará por la persona experta en la técnica que se pueden hacer varias modificaciones a las realizaciones descritas anteriormente sin salirse del alcance de la presente invención. Por ejemplo, mientras que la descripción anterior trata la invención en el contexto de una red de TV Móvil, se apreciará que la invención también aplica a redes de IPTV de acceso fijo. La invención puede encontrar uso en servicios tales como servicios de conferencia multidifusión/difusión en Pulsar para Hablar sobre redes Celulares (PoC).

Las siguientes abreviaturas se han usado en esta especificación:

BM-SC:	Centro Multidifusión de Servicio de Difusión
BSF:	Función de Servidor de Inicialización
BTID:	ID de Transacción de Inicialización
CK:	Clave de Contenido
EPG:	Guía Electrónica de Programas
ESG:	Guía Electrónica de Servicios
GAA:	Arquitectura Genérica de Autentificación
GBA:	Arquitectura Genérica de Inicialización
HSS:	Servidor Local de Abonado

HTTP:	Protocolo de Transferencia Hipertexto
IK:	Clave de Integridad
IPTV AS:	Servidor de Aplicaciones de IPTV
Ks_naf:	Clave de largo plazo generada por la BSF como un resultado del procedimiento de GBA
Linear BC TV:	Canal de TV distribuido sobre portador de Difusión
MBMS:	Servicio de Multidifusión de Difusión Multimedia
MCF:	Función de Control de Medios
MDF:	Función de Entrega de Medios
MSK:	Clave de Sesión del MBMS
MTK:	Clave de Tráfico del MBMS
MTV AS:	Servidor de Aplicaciones de TV Móvil
MUK:	Clave de Usuario del MBMS
NAF:	Función de Aplicación de Red
SRTP:	Protocolo de Transporte en Tiempo Real Seguro
STB:	Receptor Multimedia Digital
UE:	Equipo de Usuario
URI:	Identificador de Recursos Uniforme
VoD:	Vídeo bajo Demanda

REIVINDICACIONES

1. Un método de establecimiento de una sesión de televisión IP segura, el método **caracterizado porque** comprende:

recibir (S11; S23; S47), en un Servidor de Aplicaciones (9), un mensaje de invitación desde un nodo de recepción de televisión IP (1) para poner en marcha una sesión de televisión IP, el mensaje de invitación que incluye un Identificador de Transacción de Inicialización asociado con el nodo de recepción;

enviar (S12; S25; S48) una petición de autentificación a un Servidor de Protección de Acceso de Servicio, la petición de autentificación que incluye el Identificador de Transacción de Inicialización;

recibir (S13; S26; S40) desde el Servidor de Protección de Acceso de Servicio una respuesta de autentificación, la respuesta de autentificación que incluye una clave de largo plazo asociada con el nodo de recepción de televisión IP, la clave de largo plazo que se ha proporcionado previamente al nodo de recepción de televisión IP;

enviar (S14; S27; S50) una petición a un nodo proveedor de contenidos de televisión IP, la petición que identifica el nodo de recepción de televisión IP;

cifrar (S16; S33; S56) una clave de cifrado de medios que usa la clave de largo plazo recibida, la clave de cifrado de medios para usar por el nodo proveedor de contenido de televisión IP para cifrar los medios; y

enviar (S16a; S33a; S56a) un mensaje de respuesta de invitación al nodo de recepción de televisión IP, el mensaje de respuesta de invitación que incluye la clave de cifrado de medios cifrada.

2. El método de acuerdo con la reivindicación 1, en el que el mensaje de invitación es un mensaje de Invitación del Protocolo de Inicio de Sesiones, y el Identificador de Transacción de Inicialización se incluye en una cabecera de Autorización Intermediaria.

3. El método de acuerdo con la reivindicación 1 o 2, en el que la sesión de televisión IP es una sesión de televisión IP Móvil, y el Servidor de Aplicaciones es un Servidor de Aplicaciones de televisión IP Móvil.

4. El método de acuerdo con las reivindicaciones 1, 2 o 3, en el que la sesión de televisión IP se selecciona desde una de una difusión de televisión IP lineal, una unidifusión de televisión IP lineal, y una unidifusión de Video bajo Demanda.

5. El método de acuerdo con cualquiera de las reivindicaciones 1 a 4, en el que el Servidor de Protección de Acceso de Servicio es una Función de Servidor de Inicialización.

6. El método de acuerdo con cualquiera de las reivindicaciones 1 a 5, en el que la clave de cifrado de medios se selecciona de una de una clave de grupo y una clave de contenido.

7. El método de acuerdo con cualquiera de las reivindicaciones 1 a 6, en el que la clave de cifrado de medios se envía desde el Servidor de Aplicaciones al nodo proveedor de contenidos de Televisión IP.

8. El método de acuerdo con cualquiera de las reivindicaciones 1 a 6, en el que la clave de cifrado de medios se recibe en el Servidor de Aplicaciones desde el nodo proveedor de contenido de Televisión IP.

9. Un Servidor de Aplicaciones (9) **caracterizado porque** comprende:

un primer receptor (14) para recibir un mensaje de invitación desde un nodo de recepción de televisión IP (1) para poner en marcha una sesión de televisión IP, el mensaje de invitación que incluye un Identificador de Transacción de Inicialización asociado con el nodo de recepción de televisión IP;

un primer transmisor (15) para enviar una petición de autentificación a un Servidor de Protección de Acceso de Servicio, la petición de autentificación que incluye el Identificador de Transacción de Inicialización;

un segundo receptor (16) para recibir desde el Servidor de Protección de Acceso de Servicio una respuesta de autentificación, la respuesta de autentificación que incluye una clave de largo plazo asociada con el nodo de recepción de televisión IP, la clave de largo plazo que se ha proporcionado previamente al nodo de recepción de televisión IP;

un segundo transmisor (17) para enviar una petición a un nodo proveedor de contenidos de televisión IP, la petición que identifica el nodo de recepción de televisión IP;

un procesador (19) para cifrar una clave de cifrado de medios que usa la clave de largo plazo recibida; y

un tercer transmisor (20) para enviar un mensaje de respuesta de la invitación al nodo de recepción de televisión IP, el mensaje de respuesta de invitación que incluye la clave de cifrado de medios cifrada.

10. El Servidor de Aplicaciones de acuerdo con la reivindicación 9, que además comprende un tercer receptor (18) para la recepción desde el nodo proveedor de contenidos de televisión IP un mensaje que incluye la clave de cifrado de medios.

11. El Servidor de Aplicaciones de la reivindicación 9, en el que el segundo transmisor se dispone para enviar la clave de cifrado de medios en la petición al nodo proveedor de contenidos de televisión IP.

12. El Servidor de Aplicaciones de acuerdo con cualquiera de las reivindicaciones 9 a 11, en el que el Servidor de Aplicaciones es un Servidor de Aplicaciones de televisión IP Móvil y la sesión de televisión IP es una sesión de televisión IP Móvil.

13. El Servidor de Aplicaciones de acuerdo con cualquiera de las reivindicaciones 9 a 12, en el que la sesión de televisión IP se selecciona de una de una difusión de televisión IP lineal, una unidifusión de televisión IP lineal, y una unidifusión de Vídeo bajo Demanda.

14. Un nodo de recepción de televisión IP (1) **caracterizado porque** comprende:

una memoria (23) para almacenar un Identificador de Transacción de Inicialización y una clave de largo plazo asociada con el nodo de recepción de televisión IP;

un transmisor (24) para enviar a un Servidor de Aplicaciones un mensaje de invitación para inicializar una sesión de televisión IP, el mensaje de invitación que incluye el Identificador de Transacción de Inicialización;

un primer receptor (25) para recibir desde el Servidor de Aplicaciones un mensaje de respuesta, el mensaje de respuesta que incluye una clave de cifrado de medios cifrada usando la clave de largo plazo;

un primer procesador (26) para descifrar la clave de cifrado de medios que usa la clave de largo plazo almacenada;

un segundo receptor (27) para recibir el contenido de medios de televisión IP enviado desde un nodo proveedor de contenidos de televisión IP, el contenido de medios de televisión IP que se cifra usando la clave de cifrado de medios;

un segundo procesador (28) para descifrar el contenido de medios de televisión IP usando la clave de cifrado de medios descifrada.

15. El nodo de recepción de televisión IP de acuerdo con la reivindicación 14, en el que el nodo de recepción de televisión IP es un Equipo de Usuario.

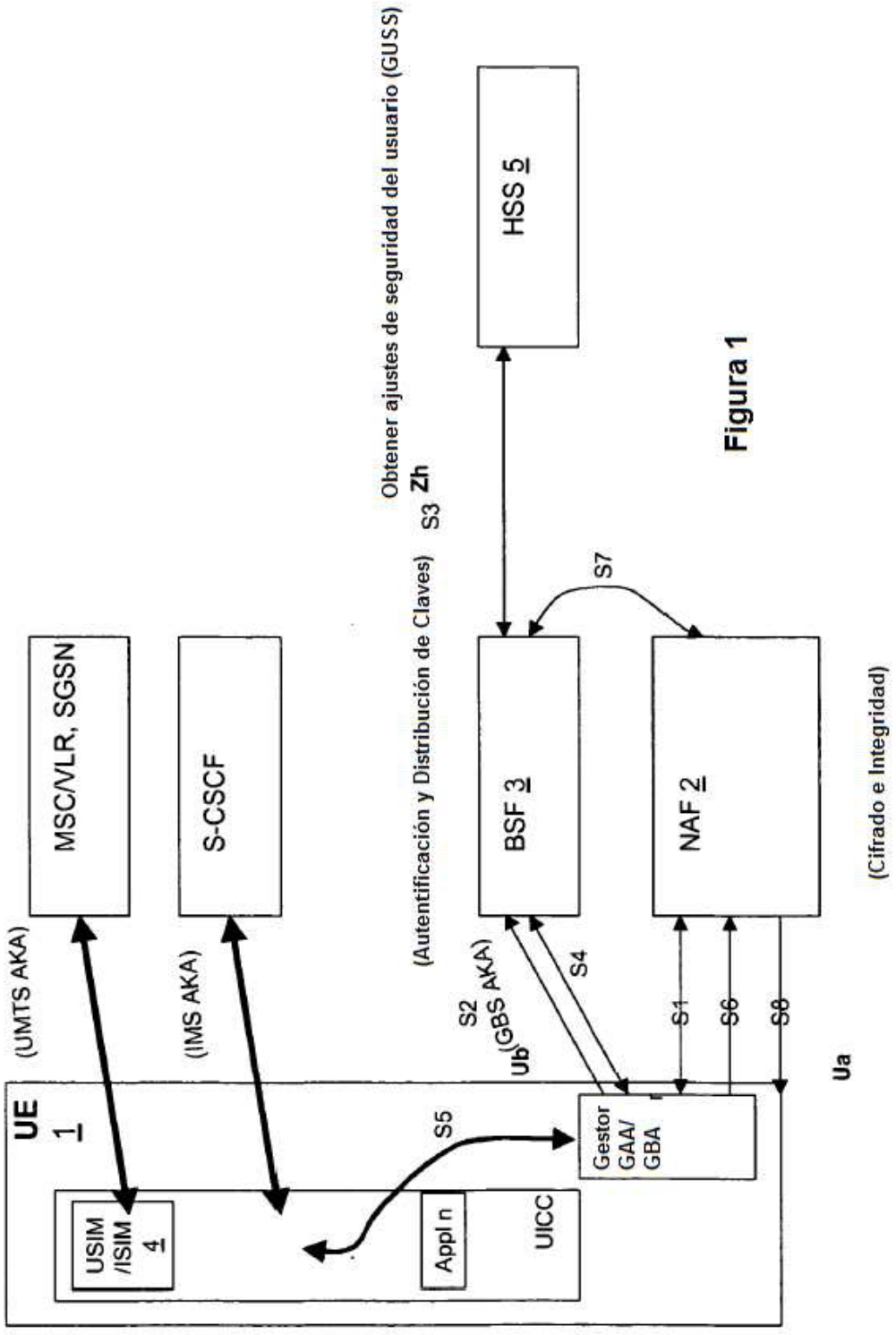
HSS 5
Obtener ajustes de seguridad del usuario (GUSS)
S3 Zh
(Autentificación y Distribución de Claves)
S7
MSC/VLR, SGSN
S-CSCF
BSF 3
NAF 2
(UMTS AKA)
(IMS AKA)
S2
(GBS AKA)
Ub
S4
S1
S6
S8
Ua
(Cifrado e Integridad)
UE 1
S5
Gestor GAA/ GBA
USIM /ISIM 4
Appl n
UICC

Figura 1

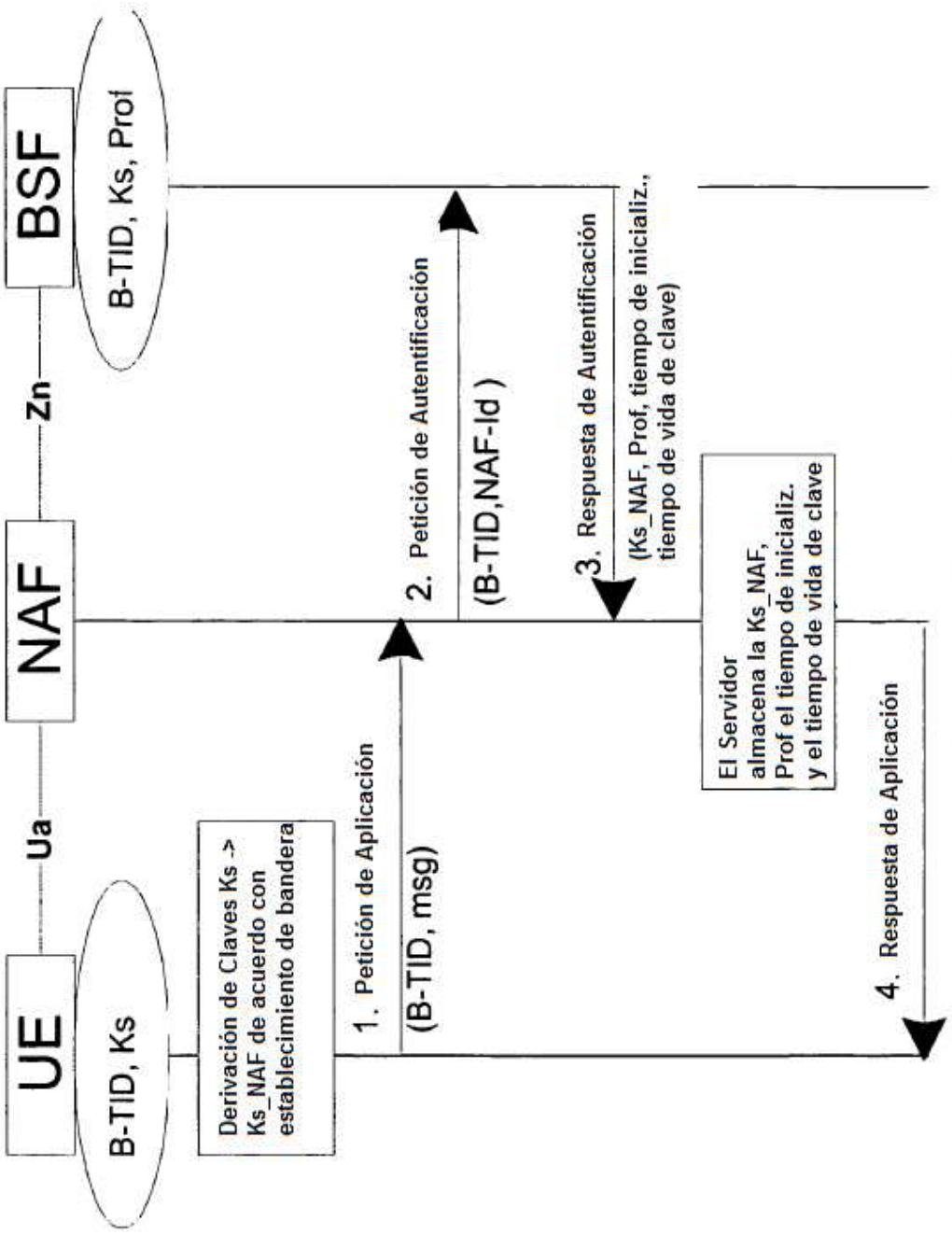
UE
Ua
NAF
Zn
BSF
B-TID, Ks
B-TID, Ks, Prof
Derivación de Claves Ks -> Ks_NAF de acuerdo con establecimiento de bandera
1. Petición de Aplicación
(B-TID, msg)
2. Petición de Autentificación
(B-TID,NAF-Id)
3. Respuesta de Autentificación
(Ks_NAF, Prof, tiempo de inicializ., tiempo de vida de clave)
El Servidor almacena la Ks_NAF, Prof el tiempo de inicializ. y el tiempo de vida de clave
4. Respuesta de Aplicación
msg es el conjunto de datos de aplic. específica
Prof es la parte de aplicación específica del perfil de usuario

Figura 2

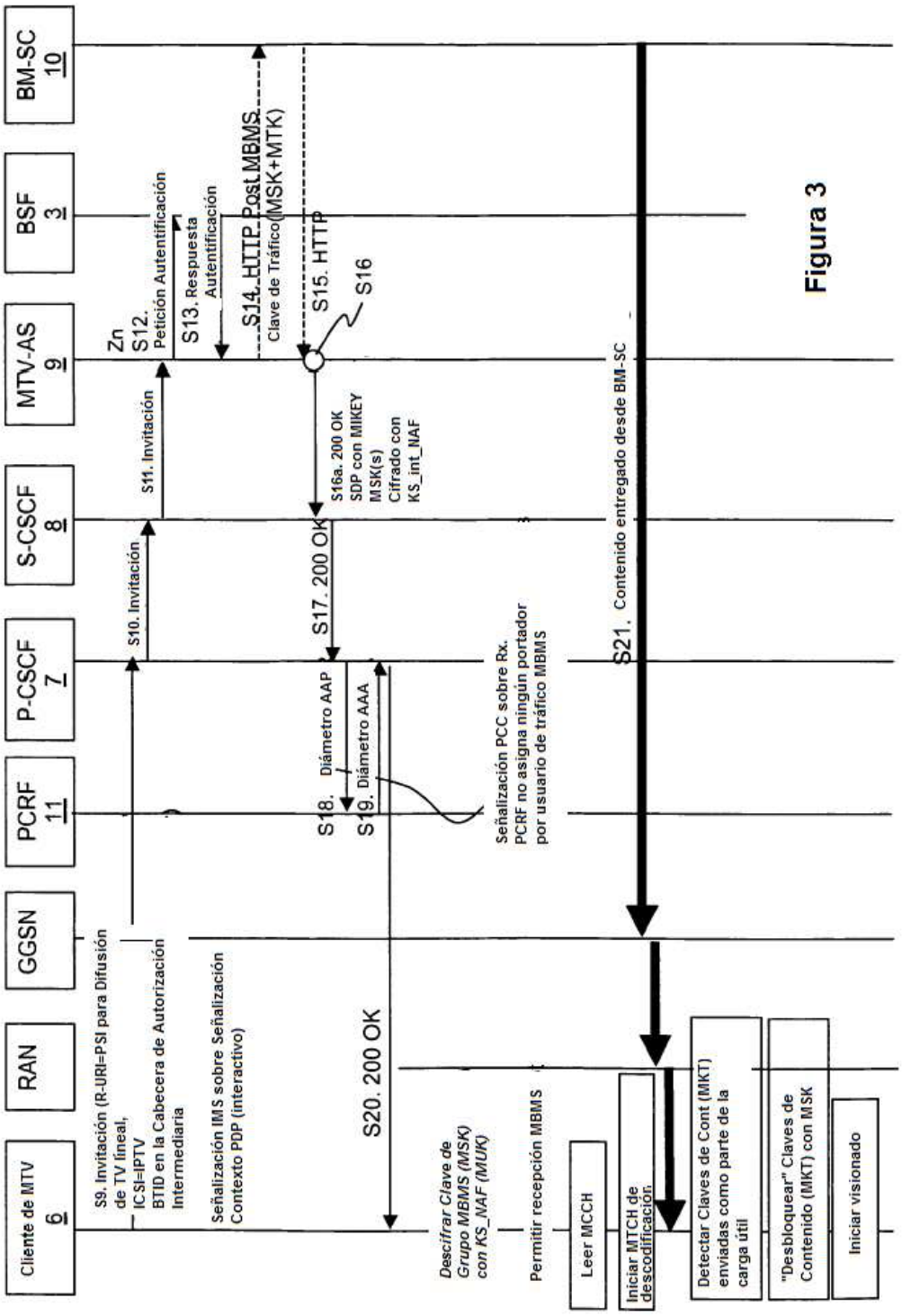
Cliente de MTV 6
RAN
GGSN
PCRF 11
P-CSCF 7
S-CSCF 8
MTV-AS 9
BSF 3
BM-SC 10
S9. Invitación (R-URI=PSI para Difusión de TV lineal, ICSI=IPTV BTID en la Cabecera de Autorización Intermediaria
Señalización IMS sobre Señalización Contexto PDP (interactivo)
S10. Invitación
S11. Invitación
Zn S12. Petición Autentificación
S13. Respuesta Autentificación
S14. HTTP Post MBMS Clave de Tráfico(MSK+MTK)
S15. HTTP
S16
S16a. 200 OK SDP con MIKEY MSK(s) Cifrado con KS_int_NAF
S17. 200 OK
S18. Diámetro AAP
S19. Diámetro AAA
Señalización PCC sobre Rx. PCRF no asigna ningún portador por usuario de tráfico MBMS
S21. Contenido entregado desde BM-SC
S20. 200 OK
Descifrar Clave de Grupo MBMS (MSK) con KS_NAF (MUK)
Permitir recepción MBMS
Leer MICCH
Iniciar MTCH de descodificación
Detectar Claves de Cont (MKT) enviadas como parte de la carga útil
"Desbloquear" Claves de Contenido (MKT) con MSK
Iniciar visionado

Figura 3

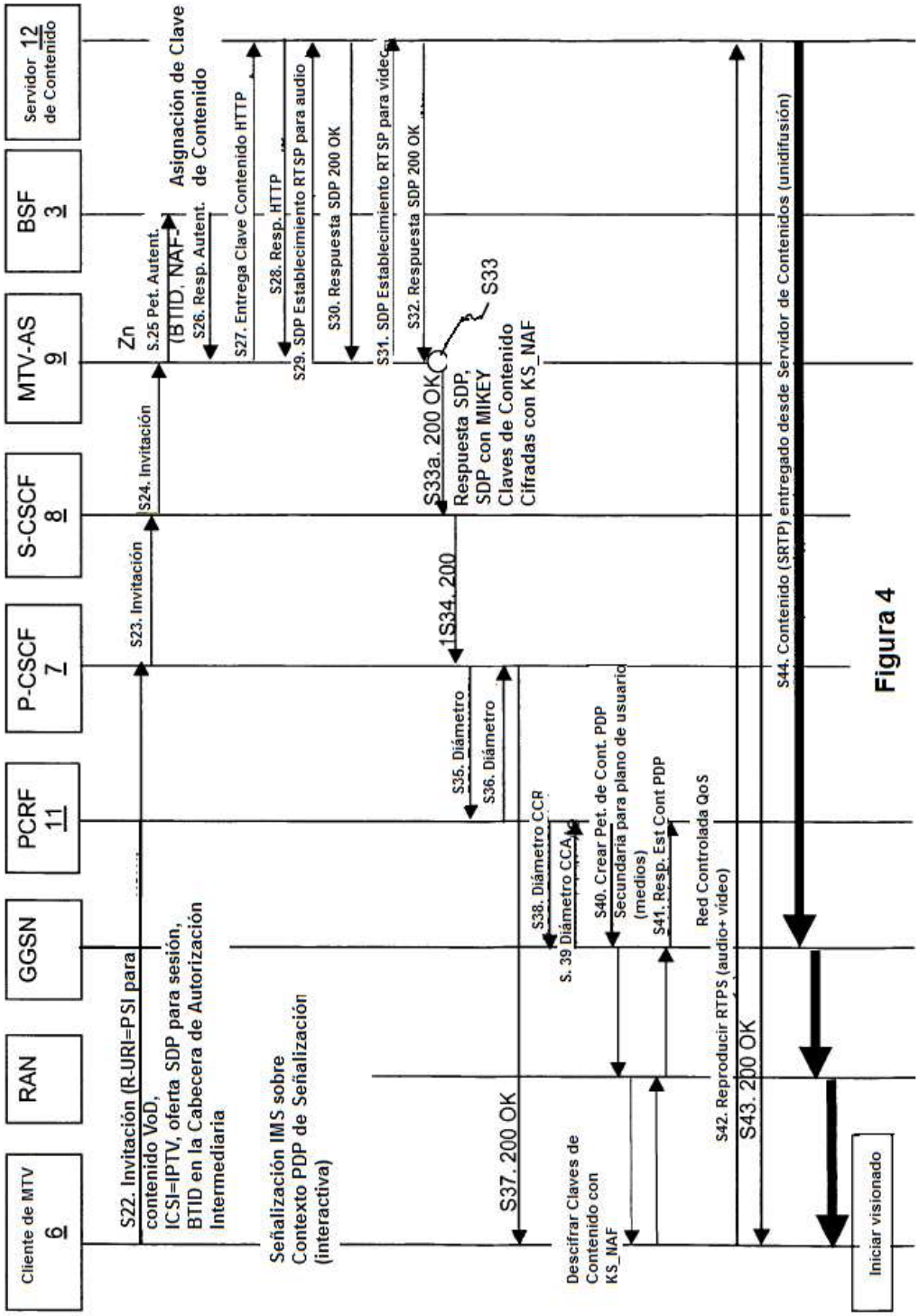
Cliente de MTV 6
RAN
GGSN
PCRF 11
P-CSCF 7
S-CSCF 8
MTV-AS 9
BSF 3
Servidor 12 de Contenido
S22. Invitación (R-URI=PSI para contenido VoD, ICSI=IPTV, oferta SDP para sesión, BTID en la Cabecera de Autorización Intermediaria
S23. Invitación
S24. Invitación
Zn
S.25 Pet. Autent. (BTID, NAF)
S26. Resp. Autent.
Asignación de Clave de Contenido
S27. Entrega Clave Contenido HTTP
S28. Resp. HTTP
S29. SDP Establecimiento RTSP para audio
S30. Respuesta SDP 200 OK
S31. SDP Establecimiento RTSP para video
S32. Respuesta SDP 200 OK
S33
S33a. 200 OK
Respuesta SDP, SDP con MIKEY Claves de Contenido Cifradas con KS_NAF
1S34. 200
S35. Diámetro
S36. Diámetro
S37. 200 OK
S38. Diámetro CCR
S. 39 Diámetro CCA
S40. Crear Pet. de Cont. PDP Secundaria para plano de usuario (medios)
S41. Resp. Est Cont PDP
Red Controlada QoS
Señalización IMS sobre Contexto PDP de Señalización (interactiva)
Descifrar Claves de Contenido con KS_NAF
S42. Reproducir RTPS (audio+ video)
S43. 200 OK
S44. Contenido (SRTP) entregado desde Servidor de Contenidos (unidifusión)
Iniciar visionado

Figura 4

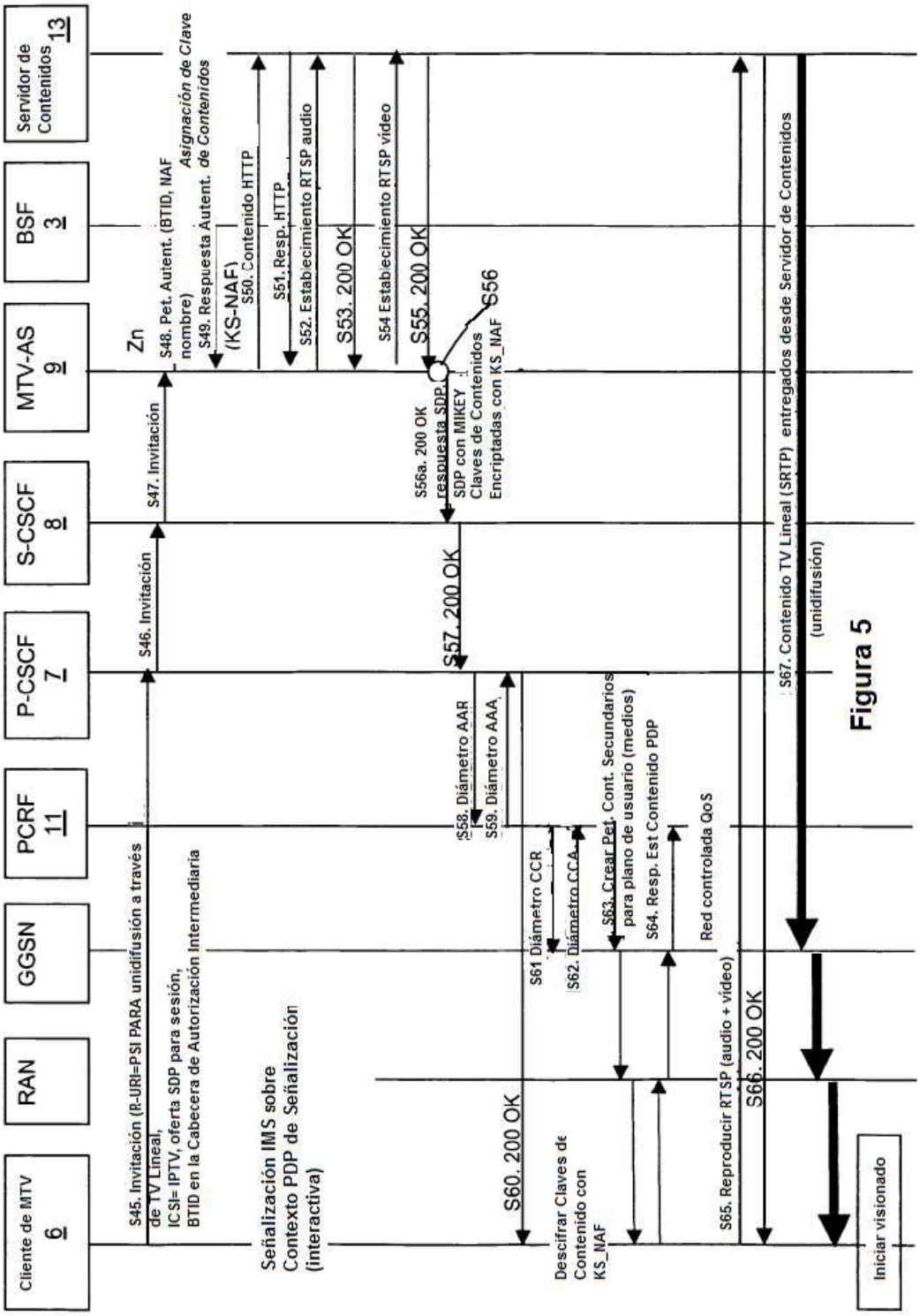
Cliente de MTV 6
RAN
GGSN
PCRF 11
P-CSCF 7
S-CSCF 8
MTV-AS 9
BSF 3
Servidor de Contenidos 13
S45. Invitación (R-URI=PSI PARA unidifusión a través de TV Lineal, ICSI= IPTV, oferta SDP para sesión, BTID en la Cabecera de Autorización Intermediaria
Señalización IMS sobre Contexto PDP de Señalización (interactiva)
S46. Invitación
S47. Invitación
Zn
S48. Pet. Autent. (BTID, NAF nombre)
S49. Respuesta Autent. de Contenidos
Asignación de Clave
(KS-NAF)
S50. Contenido HTTP
S51. Resp. HTTP
S52. Establecimiento RTSP audio
S53. 200 OK
S54 Establecimiento RTSP video
S55. 200 OK
S56
S56a. 200 OK respuesta SDP
SDP con MIKEY
Claves de Contenidos
Encriptadas con KS_NAF
S57. 200 OK
S58. Diámetro AAR
S59. Diámetro AAA
S60. 200 OK
Descifrar Claves de Contenido con KS_NAF
S61 Diámetro CCR
S62. Diámetro CCA
S63. Crear Pet. Cont. Secundarios para plano de usuario (medios)
S64. Resp. Est Contenido PDP
Red controlada QoS
S65. Reproducir RTSP (audio + video)
S66. 200 OK
S67. Contenido TV Lineal (SRTP) entregados desde Servidor de Contenidos (unidifusión)
Iniciar visionado

Figura 5

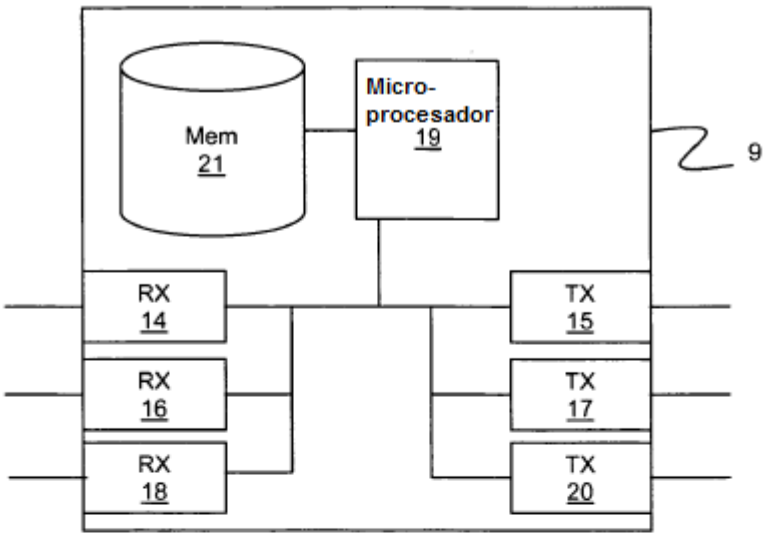

Figura 6

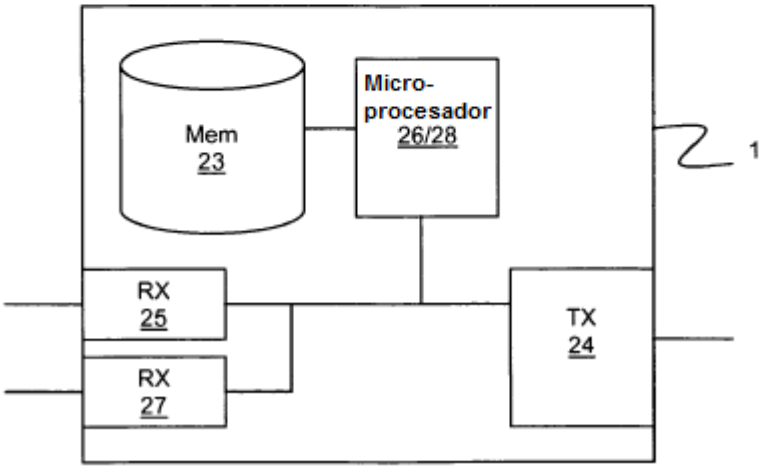

Figura 7