(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 579 179**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04N 7/167 (2006.01)
H04L 29/06 (2006.01)
H04N 21/2347 (2011.01)
H04N 21/258 (2011.01)
H04N 21/266 (2011.01)
H04N 21/4405 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/6334 (2011.01)
H04N 21/835 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.04.2006 E 06727549 (5)**

(97) Fecha y número de publicación de la concesión europea: **25.05.2016 EP 1880505**

(54) Título: **Método y aparato para gestión de derechos de grano fino de contenido de flujo continuo**

(30) Prioridad:

12.05.2005 US 127780

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.08.2016

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

LAHTINEN, PEKKA, LLMANI y
ALVE, JUKKA, ANTERO

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y aparato para gestión de derechos de grano fino de contenido de flujo continuo

Campo de la invención

Esta invención se refiere a entregar contenido multimedia protegido. En particular, la invención proporciona aparatos y métodos para uso en proporcionar control mejorado sobre derechos de usuario a porciones del contenido protegido.

Antecedentes de la invención

El flujo continuo de vídeo, el flujo continuo de datos y la programación de difusión digital de banda ancha están creciendo en popularidad en las aplicaciones de red inalámbrica, por ejemplo, servicios de multidifusión de Protocolo de Internet (IP). Para soportar estas aplicaciones inalámbricas, los sistemas de difusión inalámbrica transmiten contenido de datos que soporta servicios de datos a muchos terminales inalámbricos simultáneamente. El contenido de medio digital u otros datos se difunden usando diversos protocolos de aplicación, protocolos de transporte y protocolos de red. Por ejemplo, un sistema de difusión proporciona difusión de datos de IP donde se transmite el servicio audio-visual de modo que puede empaquetarse y encapsularse vídeo MPEG4-AVC, audio MPEG4-AAC y componentes de datos auxiliares a RTP y/o ALC. Los paquetes se formatean posteriormente a UDP e IP y se transmiten a través de MPE en MPEG2-TS (por ejemplo DVB-H). En un dominio de conmutación de paquetes, el concepto de sesión multi-media puede requerir que uno o más componentes de sesión (audio, vídeo y datos auxiliares en el caso anterior) se unan lógicamente juntos. Las porciones de la sesión multi-media se envían entre un tiempo de inicio y un tiempo de fin comunes. Sin embargo, con un entorno de difusión todos los receptores que pueden recibir la señal de difusión pueden recibir los datos llevados mediante la señal de difusión. Es importante que el vendedor de contenido limite acceso al contenido multi-media de modo que únicamente los receptores autorizados puedan presentar el contenido multi-media a los usuarios.

Los sistemas de Gestión de Derechos Digitales (DRM), como el sistema de DRM de la Alianza Móvil Abierta (OMA), se están usando para vender acceso a ficheros discretos, como Ficheros de Contenido Digital (DCF) de DRM de OMA. Como una posible solución, un dispositivo (según se pide por su usuario humano) desde un Proveedor de Contenido obtiene el DCF (por ejemplo un fichero de música de MP3), que está encriptado mediante una clave de contenido. El dispositivo obtiene por separado (es decir compra) desde un Emisor de Derechos (RI) un Objeto de Derechos (RO) que puede incluir (entre otras cosas) dos partes: la clave de contenido para desencriptar el DCF, y los derechos de uso para el DCF. Los derechos de uso controlan la manera en la que el dispositivo (y por lo tanto su usuario humano) pueden usar el contenido de DCF desencriptado; por ejemplo, límites de tiempo para usar el contenido, si el contenido puede copiarse, etcétera. Diferentes RI pueden vender RO para el mismo DCF a diferentes precios y con diferentes derechos de uso.

A menudo, por ejemplo en el caso de DRM de OMA, los derechos de uso se expresan en un Lenguaje de Expresión de Derechos (REL) que puede contener condicionalidad basándose en variables como días de la semana, hora del día, periodos de días, etc.... Por ejemplo, puede establecerse que un derecho de uso particular se extienda durante un periodo de tiempo. Ejemplos de REL incluyen el Lenguaje de Derechos Digitales Abierto (ODRL) y Lenguaje de Marcas de Derechos Extensible (XrML).

Recientemente, se están desarrollando sistemas de DRM para vender servicios de flujo continuo, también, además de ficheros de DCF discretos. Un caso especial de tales servicios de flujo continuo son los verdaderos servicios de flujo continuo de difusión de radio (servicios de difusión en lo sucesivo), donde múltiples dispositivos reciben el mismo flujo de difusión. Por ejemplo DRM de OMA ha sugerido para vender y comprar servicios de difusión de datos de IP (IPDC), y la solución se está normalizando por la organización de la Difusión de Vídeo Digital (DVB), para (entre otras cosas) soportar receptores de televisión portátiles en la parte superior de la tecnología de difusión de radio de DVB-H (portátil).

Los papales de organización típicos en servicios de difusión incluyen: 1) un difusor que obtiene el contenido de flujo continuo desde proveedores y lo difunde encriptado a través de la trayectoria de radio, y 2) múltiples RI, que venden RO para desencriptar el contenido y establecer los derechos de uso para ellos en los dispositivos que reciben la difusión. Los RO pueden entregarse a través de la misma trayectoria de radio de difusión como el propio contenido encriptado, o mediante canales de interacción separados tales como operadoras de datos celulares (por ejemplo GSM GPRS, Servicio General de Paquetes de Radio).

En un escenario de este tipo, normalmente no es factible que la clave en cada RO desencripte el contenido de flujo continuo directamente, puesto que el contenido de flujo continuo es continuo (a diferencia de los ficheros de DCF discretos). Una técnica conocida para desencriptación de contenido es una jerarquía de clave como se usa en un acceso condicional de DVB. El difusor envía secuencias de contenido de flujo continuo encriptadas cada una mediante una clave de tráfico (TK), cambiando periódicamente la clave de tráfico. Al menos cada vez que la clave de tráfico cambia, se envía un Mensaje de Flujo de Clave (KSM), que contiene la clave de tráfico encriptada mediante

una clave de servicio (SK). Los RO contienen la clave de servicio. Por lo tanto, los dispositivos de recepción pueden usar la clave de servicio en los RO para desencriptar las claves de tráfico en los KSM. Los dispositivos de recepción pueden usar a continuación las claves de tráfico para desencriptar el contenido de flujo continuo. En la práctica, los KSM deben difundirse con mucha frecuencia para posibilitar el "cambio de canal" rápido desde un servicio a otro.

La clave de servicio también cambia periódicamente, aunque la frecuencia de cambio normalmente es muy inferior. Una nueva clave de servicio se requiere a continuación para que el dispositivo continúe desencriptando el contenido de flujo continuo. Por lo tanto, puede obtenerse un nuevo RO con la nueva clave de servicio mediante los dispositivos para sustituir los antiguos. Por consiguiente, los RO tienen un cierto periodo de validez, que equivale al tiempo durante el cual puede usarse la clave de servicio para desencriptar las claves de tráfico para desencriptar el contenido de flujo continuo.

Como se ha especificado anteriormente, un RO para un servicio de difusión sirve para desencriptar y hacer accesible contenido de flujo continuo, para el periodo de validez del RO. Como en el caso de DCF, el RO puede usarse también para establecer derechos de uso expresados en el REL para el mismo periodo de validez. Como un ejemplo, considérese el servicio de difusión de televisión portátil basado en DVB-H. Se permite a los dispositivos típicos presentar en una pantalla (de modo que un usuario humano pueda ver) el servicio de televisión, tal como un programa en un canal, a medida que se recibe. Los derechos de uso pueden establecer lo que el dispositivo/usuario puede hacer con el contenido de flujo continuo, que puede ser el servicio de televisión. Por ejemplo, los derechos de uso pueden proporcionar que el contenido pueda grabarse, pueda reproducirse en un momento más tarde, pueda copiarse a otro dispositivo, pueda verse únicamente o cualesquiera derechos se deseen proporcionar.

Aunque esta metodología proporciona un cierto nivel de funcionalidad, existe un problema. Cada RO puede establecer únicamente un conjunto de derechos de uso para el periodo de validez. Este nivel de control puede ser insuficiente. Por ejemplo, puede haber diferentes tipos de programas de televisión en un servicio de difusión de televisión portátil que los RI pueden desear proporcionar diferentes niveles de control con respecto al uso. Los RI pueden desear permitir unos derechos de uso "haz cualquier cosa" liberales para ciertos tipos o porciones de contenido tales como noticias, anuncios o concursos pero restringir los derechos de uso para otros tipos o porciones de contenido tales como eventos deportivos de gran calidad o largometrajes. Por lo tanto, aunque los RO con periodos de validez relativamente largos son buenos para acceso de contenido de flujo continuo (es decir desencriptación), sería útil proporcionar unos medios de grano más fino para proporcionar derechos de uso con frecuencia aumentada y/o precisión en el periodo de validez del RO de modo que el uso del tipo o porción del contenido esté de acuerdo con los derechos de uso que se pretenden conceder para el tipo o porción de contenido.

Adicionalmente, los derechos para cierto contenido pueden variar dependiendo de la hora del día o del día de la semana. Además, un usuario puede tener diferentes derechos para diferentes porciones del contenido. Por ejemplo, para mejorar la recaudación de ingresos, a menudo se permite a un usuario acceder a servicios multi-media de gran calidad únicamente si el usuario se abona al servicio o pide el servicio (por ejemplo, pago por visión). Sin embargo, el contenido puede separarse también en periodos de tiempo. Por lo tanto, por ejemplo, un usuario puede decidir abonarse a una edición de fin de semana en lugar de una suscripción de semana completa. Los RI pueden desear permitir que se grabe algo del contenido disponible en la suscripción de edición de fin de semana y se reenvíe libremente a otros mientras se limita otras porciones del contenido a un único uso o a un conjunto de distribución más controlado.

Se hace referencia a "Service y Content Protection for Mobile Broadcast Services, N.º 1.0 11 de marzo de 2005 pág. 1-34; Alexander Medvinsky et al "Use of Triggers for Broadcast Services", 27 de enero de 2005, pág. 1-5; y Open Mobile Alliance Ltd: "Service/Content Protection Architecture", Change Request, 15 de marzo de 2005. Se hace referencia también a "Digital Vídeo Broadcasting (DVB): DVB Specification for data broadcasting" ETSI EN 301 192 v1.4.1 (06-2004).

Breve sumario de la invención

De acuerdo con un primer aspecto de la memoria descriptiva, se proporciona un método que comprende: (A) recibir un flujo de datos encriptados (2001), que corresponde a una única sesión multi-media, desde un sistema de comunicación (2000), comprendiendo el flujo de datos una pluralidad de porciones encriptadas, respectivamente, mediante una pluralidad de claves de tráfico (2205); (B) recibir un mensaje de flujo de clave encriptada, incluyendo el mensaje de flujo de clave encriptada la pluralidad de claves de tráfico; y (C) usar la pluralidad de claves de tráfico para desencriptar las respectivas porciones del flujo de datos encriptados, en el que el mensaje de flujo de clave encriptada se separa del flujo de datos encriptados, y en el que cada porción del flujo de datos encriptados está incluida en el mismo segmento de tiempo de ráfaga de datos como el respectivo mensaje de flujo de clave encriptada.

De acuerdo con un segundo aspecto de la memoria descriptiva, se proporciona un aparato (2026) que comprende: un receptor para recibir: un flujo de datos encriptados, que corresponden a una única sesión multi-media, desde un sistema de comunicación (2000), comprendiendo el flujo de datos encriptados una pluralidad de porciones encriptadas, respectivamente, mediante una pluralidad de claves de tráfico (2005); y un mensaje de flujo de clave

encriptada, incluyendo el mensaje de flujo de clave encriptada la pluralidad de claves de tráfico; y un procesador para usar la pluralidad de claves de tráfico para desencriptar las respectivas porciones del flujo de datos encriptados, en el que el mensaje de flujo de clave encriptada está separado del flujo de datos encriptados, y en el que cada porción del flujo de datos encriptados está incluida en el mismo segmento de tiempo de ráfaga de datos como el respectivo mensaje de flujo de clave encriptada.

Breve descripción de los dibujos

Se obtendrá un entendimiento más completo de la presente invención y de las ventajas de la misma haciendo referencia a la siguiente descripción en consideración de los dibujos adjuntos, en los que números de referencia similares indican características similares y en los que:

La Figura 1 muestra la transmisión de servicios de Protocolo de Internet (IP) utilizando transmisión de segmento de tiempo de acuerdo con una realización de la invención;

La Figura 2 muestra una pila de protocolo que soporta transmisión de datos multi-media de acuerdo con una realización de la invención;

La Figura 3 muestra una configuración de componente para una sesión multi-media de acuerdo con una realización de la invención;

La Figura 4 muestra una configuración de componente para una sesión multi-media mostrada de acuerdo con una realización de la invención;

La Figura 5 muestra una variación de la configuración de componente mostrada en la Figura 4 de acuerdo con una realización de la invención;

La Figura 6 muestra una variación de la configuración de componente mostrada en la Figura 4 de acuerdo con una realización de la invención;

La Figura 7 muestra una variación de la configuración de componente mostrada en la Figura 4 de acuerdo con una realización de la invención;

La Figura 8 muestra una variación de la configuración de componente mostrada en la Figura 4 de acuerdo con una realización de la invención;

La Figura 9 muestra una variación de la configuración de componente mostrada en la Figura 4 de acuerdo con una realización de la invención;

La Figura 10 muestra una configuración de componente para una sesión multi-media de acuerdo con un ejemplo no de acuerdo con las reivindicaciones;

La Figura 11 muestra una variación de la configuración de componente mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones;

La Figura 12 muestra una variación de la configuración de componente mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones;

La Figura 13 muestra una variación de la configuración de componente mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones;

La Figura 14 muestra una variación de la configuración de componente mostrada en la Figura 10 de acuerdo con

La Figura 15 muestra una variación de la configuración de componente mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones;

La Figura 16 muestra una variación de la configuración de componente mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones;

La Figura 17 muestra un procedimiento para recibir una sesión multi-media de acuerdo con una realización de la invención;

La Figura 18 muestra un diagrama de flujo para la arquitectura mostrada en la Figura 17 de acuerdo con una realización de la invención;

La Figura 19 muestra un sistema para transferencia de contenido protegido que soporta servicios de IPDC (difusión de datos de IP) de DVB-H de acuerdo con la técnica anterior;

La Figura 20 muestra un sistema que soporta servicios de IPDC de DVB-H de acuerdo con una realización de la invención;

La Figura 21 muestra un diagrama de flujo para transmitir datos para los servicios de IPDC de DVB-H en el sistema mostrado en la Figura 20 de acuerdo con una realización de la invención;

La Figura 22 muestra un sistema que soporta servicios de IPDC de DVB-H de acuerdo con una realización de la invención;

La Figura 23 muestra un sistema que soporta servicios de IPDC de DVB-H de acuerdo con una realización de la invención;

La Figura 24 muestra un aparato que soporta un módulo de transmisión como se muestra en la Figuras 20, 22, y 23 de acuerdo con una realización de la invención;

La Figura 25 muestra un aparato que recibe una difusión multimedia y que aplica claves de IPSec de acuerdo con una realización de la invención;

La Figura 26 muestra un aparato que recibe una difusión multimedia y que desencripta las claves de IPSec de acuerdo con una realización de la invención;

La Figura 27 muestra un sistema para desplegar un módulo de software de extensión de seguridad de acuerdo con una realización de la invención;

La Figura 28 muestra y ejemplifica un método de la técnica anterior para proporcionar contenido encriptado;

La Figura 29 muestra un método para proporcionar contenido de flujo continuo encriptado de acuerdo con una realización de la invención;

La Figura 30 muestra un método para difundir contenido de flujo continuo de acuerdo con una realización de la invención;

La Figura 31 muestra una línea de tiempo de cambios a claves de tráfico de acuerdo con una realización de la invención;

La Figura 32 muestra una división de segmentos de programa de acuerdo con una realización de la invención; y

La Figura 33 muestra un sistema de provisión que usa una pluralidad de objetos de derecho de acuerdo con una realización de la invención.

Descripción detallada de la invención

En la siguiente descripción de las diversas realizaciones, se hace referencia a los dibujos adjuntos que forman una parte de la misma, y en los que se muestra a modo de ilustración diversas realizaciones en las que puede ponerse en práctica la invención. Se ha de entender que pueden utilizarse otras realizaciones y que pueden realizarse modificaciones estructurales y funcionales sin alejarse del alcance de la presente invención como se define mediante las reivindicaciones.

Para ayudar en la organización y para facilidad del lector, se proporciona la descripción detallada en dos secciones. En primer lugar, en las Figuras 1-27, se proporcionan detalles con respecto a métodos para enviar y recibir contenido de acuerdo con aspectos de la presente invención. A continuación en la Figuras 28-33, se desvelan detalles con respecto a métodos y aparatos para controlar derechos de uso para porciones de contenido.

Métodos y aparatos para proporcionar contenido de flujo continuo

La Figura 1 muestra la transmisión de servicios del Protocolo de Internet (IP) que utilizan transmisión de segmento de tiempo de acuerdo con una realización de la invención. Una estación base difunde paquetes de datos para una pluralidad de servicios de IP usando los flujos de datos 101, 103, 105, y 107. (Cada flujo de datos se asigna a una porción de una capacidad de velocidad de datos). En la realización, la estación base puede soportar funcionalidad que se asume normalmente mediante una estación base transceptora (BTS), un controlador de estación base (BSC), una combinación de una BTS y un BSC, y un nodo B, que es una designación de la tercera Generación (3G) de una estación base transceptora. La transmisión de datos es esencialmente continua de manera que los paquetes de datos para un servicio de IP se están transportando continuamente a través de un flujo de datos.

Para mitigar la pérdida de paquetes de datos, los flujos de datos 101, 103, 105, y 107 se mapean mediante las estaciones base en ráfagas de paquetes de datos 109, 111, 113, y 115, respectivamente, en las que se transmiten las ráfagas a través de canales de radio en lugar de los flujos de datos 101, 103, 105, y 107. Cada flujo de datos (101, 103, 105, y 107), y en consecuencia cada ráfaga (109, 111, 113, y 115), soporta al menos un servicio de datos. Por lo tanto, cada ráfaga puede soportar una pluralidad de servicios de datos (por ejemplo, un grupo de servicio de datos relacionados).

Las velocidades de datos asociadas con las ráfagas 109, 111, 113, y 115 son normalmente mayores que las velocidades de datos que están asociadas con los flujos de datos 101, 103, 105, y 107 de modo que puede enviarse un número correspondiente de paquetes de datos en una cantidad de tiempo más corta. En la realización, los flujos de datos 101, 103, 105, y 107 corresponden a velocidades de datos continuas de aproximadamente 100 Kbit/s. Las ráfagas 109, 111, 113, y 115 corresponden normalmente a aproximadamente 4 Mbit/s (pero pueden estar por encima de 10 Mbit/s) con una duración de un segundo aproximadamente. Sin embargo, otras realizaciones pueden usar diferentes velocidades de datos para los flujos de datos 101-107 y para las ráfagas 109-115.

En la realización, toda la capacidad de velocidad de datos se asigna a una ráfaga en un tiempo dado. Como se muestra en la Figura 1, las ráfagas 109, 111, 113, y 115 están intercaladas en tiempo. Una duración de tiempo en espera (durante el que no se transmiten paquetes de datos para el servicio de datos particular) tiene lugar entre transmisiones consecutivas de una ráfaga (por ejemplo, la ráfaga 109). Un sistema de difusión inalámbrico puede utilizar la duración de tiempo en espera durante la cual puede ordenarse al terminal inalámbrico que se transfiera a otra estación base para completar un traspaso. La otra estación base puede transmitir los mismos datos como la estación base que servía previamente al terminal inalámbrico usando una frecuencia central diferente y una cantidad diferente de desplazamiento de fase. La utilización de segmentación de tiempo posibilita que un terminal reduzca el consumo de potencia eléctrica que se proporciona mediante un origen de alimentación (normalmente una batería).

Las ráfagas se transmiten normalmente de manera periódica mediante una estación base. Por ejemplo, una ráfaga siguiente puede tener lugar T segundos después de la ráfaga 109, en la que se transmite una ráfaga cada T segundos. El terminal inalámbrico puede mantener temporización precisa, como con el Sistema de Posicionamiento Global (GPS), para determinar un tiempo absoluto en el que tiene lugar cada ráfaga. En otra realización, se proporciona al terminal inalámbrico información acerca de un periodo de tiempo en cada ráfaga, que informa al terminal inalámbrico acerca de la ráfaga posterior. Con una realización de la invención, la información de periodo de tiempo incluye un parámetro de tiempo real (que corresponde a “delta-t” con DVB-H) que indica un intervalo de tiempo desde el comienzo de un ráfaga de segmento de tiempo al comienzo del siguiente ráfaga de segmento de tiempo del mismo servicio y que se señaliza en un encabezamiento de sección de MPE. El periodo de tiempo puede incluirse en un paquete de IP, una trama encapsulada multiprotocolo, cualquier otra trama de paquete, y un canal de la tercera generación (3G) o del Servicio General de Paquetes de Radio (GPRS) o datos de modulación, tales como señalización de parámetros de transmisor. Como alternativa, el terminal inalámbrico puede detectar una aparición de una ráfaga recibiendo un preámbulo de señal, que puede ser una secuencia de datos que es conocida a priori para el terminal inalámbrico. En otra realización, el terminal inalámbrico puede recibir un mensaje de tara en un canal de tara desde una estación base. El mensaje de tara puede contener información de temporización con respecto a la aparición de ráfagas. El canal de tara puede ser lógica o físicamente distinto del canal de radio de enlace descendente que soporta la trasmisión de ráfagas.

Las ráfagas 109, 111, 113, y 115 pueden formatearse usando una encapsulación multi-protocolo de acuerdo con la Sección 7 de la Norma Europea EN 301 192 “Digital Vídeo Broadcasting (DVB), DVB specification for data broadcasting”. La encapsulación puede ajustarse a las normas del Protocolo de Internet (IP).

En una realización de la invención, una Difusión de Vídeo Digital (DVB-H) proporciona servicios de medios móviles a terminales inalámbricos, por ejemplo, unidades inalámbricas portátiles. En la realización, el sistema de DVB-H es compatible con DVB-T (de difusión de vídeo digital para operación terrestre) y soporta mejoras para soportar mejor la operación de terminales portátiles inalámbricos. El sistema de DVB-H soporta servicios de datos basados en el Protocolo de Internet (IP) en los que la información puede transmitirse como datagramas de IP. El sistema de DVB-H incorpora mejoras (con respecto a un sistema de DVB-T) que facilitan el acceso a servicios de DVB basados en IP en terminales inalámbricos portátiles inalámbricos. (Realizaciones alternativas de la invención soportan variaciones de sistemas de difusión de vídeo digital incluyendo DVB-T, ATSC, y ISDB-T.) Las mejoras de DVB-H están basadas en la capa física de la capa física de DVB-T con un número de mejoras de capa de servicio que tienen por objeto mejorar la vida de la batería y la recepción en el entorno portátil. Por lo tanto, las mejoras de DVB-H complementan servicios terrestres digitales existentes, ofreciendo a los proveedores de servicio la posibilidad de extender el mercado al mercado portátil inalámbrico.

La Figura 2 muestra una pila de protocolo de internet (IP) 200 que soporta transmisión de datos multi-media de acuerdo con una realización de la invención. El contenido de medios digital u otros datos se difunden usando diversos protocolos de aplicación, protocolos de transporte y protocolos de red. Con la pila de IP 200, una difusión de datos de IP soporta un servicio audio-visual que tiene componentes de vídeo MPEG4-AVC 201, audio MPEG4-AAC 203 y datos auxiliares 205. Cada componente (201, 203, o 205) se procesa mediante el codificador 207, codificador 209, o codificador 211 para obtener paquetes que están formateados para la capa de Protocolo de

Tiempo Real (RTP) 213. Los paquetes (datagramas) se procesan posteriormente mediante la capa de UDP (protocolo de datagramas de usuario) 215 y la capa del Protocolo de Internet (IP) 217. Los datagramas están asociados con ráfagas de segmentos de tiempo formateando los datagramas usando una encapsulación multi-protocolo (que corresponde normalmente a una capa de enlace en el modelo OSI) tal como, por ejemplo, de acuerdo con la Sección 7 de la Norma Europea EN 301 192 “Digital Vídeo Broadcasting (DVB), DVB specification for data broadcasting”. La encapsulación puede ajustarse a las normas del Protocolo de Internet (IP).

Una sesión multi-media está asociada normalmente con uno o más componentes de sesión (audio, vídeo y datos auxiliares en el caso anterior) que están unidos lógicamente juntos. Las partes de la sesión se envían entre un tiempo de inicio y tiempo de fin común. Tanto el tiempo de inicio y/o el tiempo de fin pueden estar definidos o no definidos.

La Figura 3 muestra una configuración de componente 300 para una sesión multi-media 301 de acuerdo con una realización de la invención. El componente 303 corresponde a una pluralidad de datagramas (incluyendo los datagramas 309 y 315); el componente 305 corresponde a una pluralidad de datagramas (incluyendo los datagramas 311 y 317); y el componente 307 corresponde a una pluralidad de datagramas (incluyendo los datagramas 313 y 319). Los componentes 303, 305, y 307 se transmiten en paquetes de IP que están encapsulados a mensajería de una capa de portadora subyacente. Cada componente 303, 305, y 307 tiene una dirección de IP de origen definida, dirección de IP de destino y puerto usado en los paquetes de IP que llevan datos asociados con el componente. Diferentes componentes pueden tener una dirección de IP de origen definida independientemente, una dirección de IP de destino y un puerto. En variaciones de la realización, una sesión multi-media puede tener un número diferente de componentes.

Aunque la configuración de componentes ejemplar 300 muestra alineación de datagramas entre los componentes 303, 305, 307, la realización soporta configuraciones en las que los datagramas no están alineados y el número de datagramas para cada componente es diferente de el de los otros componentes. Por ejemplo, el número de datagramas para un componente de audio es normalmente menor que el número de datagramas para un componente de vídeo durante un intervalo de tiempo dado.

La Figura 4 muestra una configuración de componentes 400 para una sesión multi-media 401 de acuerdo con una realización de la invención. Los componentes 403, 405, y 407 están encriptados con la misma clave que cambia periódicamente en el flujo de clave 409 durante la sesión multi-media 401. (En las Figuras 4-16, un datagrama que está encriptado con la clave k_i se indica como E_i. (El flujo de clave 409 es un canal lógico que contiene información de clave y que está separado de los componentes de medios). De manera similar, un datagrama asociado con el j-ésimo componente y que está encriptado con la i-ésima clave asociada con el j-ésimo componente se indica como E_{ji}). La realización soporta diferentes métodos de encriptación que se aplican a los componentes 403, 405, o 407, incluyendo:

- IPSEC-ESP (denominado encriptación de nivel de IP; véase RFC en IPSEC-ESP)
- Cabida útil del paquete de sesión de aplicación encriptado (por ejemplo SRTP o DCF de DRM de OMA 1.0 o 2.0)
- Encriptación

Los métodos de encriptación anteriores pueden aplicarse por separado o en combinación durante la sesión multi-media 401. Los componentes 403, 405, y 407 corresponden a una pluralidad diferente de datagramas de contenido. El flujo de clave 409 incluye una pluralidad de datagramas asociados, correspondiendo cada datagrama asociado a una clave de encriptación. La encriptación se realiza normalmente en una base de datagrama individual (por ejemplo, paquete). Por ejemplo, los datagramas de contenido 415, 425, 427, 435, y 437 se encriptan con la clave k_1 (que corresponde al datagrama asociado 411) y el datagrama de contenido 417 se encripta con k_2 (que corresponde al datagrama asociado 413).

El flujo de clave 409 utiliza un protocolo de entrega tal como RTP, ALC/FLUTE, UHTTP, DVBSTP, IP con una cabida útil, y UDP con una cabida útil. Las claves entregadas en el flujo de clave 409 están normalmente protegidas mediante otra clave que el receptor autorizado tiene para acceder a los contenidos del flujo de clave 409 que lleva las claves, posibilitando por lo tanto el acceso a los componentes 403, 405, y 407. La entrega del flujo de clave 409 está opcionalmente sincronizada con los componentes 403, 405, y 407, por ejemplo, las indicaciones de tiempo de RTP con el uso del Protocolo de Control de RTP).

La Figura 5 muestra una variación de la configuración de componentes mostrada en la Figura 4 de acuerdo con una realización de la invención. La configuración de componentes 500 es similar a la configuración de componentes 400. La sesión multi-media 501 incluye los componentes 503, 505, y 507 y el flujo de clave 509. El componente 505 se encripta con las claves desde el flujo de clave 509, mientras los componentes 503 y 507 no.

La Figura 6 muestra una variación de la configuración de componentes mostrada en la Figura 4 de acuerdo con una realización de la invención. La configuración de componentes 600 es similar a la configuración de componentes 400. Sin embargo, el flujo de clave 609 incluye tres series de claves 611, 613, y 615 que corresponden a los componentes 603, 605, y 607, respectivamente. Las claves pueden cambiar periódicamente pero de manera

independiente durante la sesión multi-media 601 pero pueden sincronizarse entre sí.

La Figura 7 muestra una variación de la configuración de componentes mostrada en la Figura 4 de acuerdo con una realización de la invención. La configuración de componentes 700 es similar a la configuración de componentes 600 excepto que las claves para cada componente se llevan en diferentes el flujo de claves que cambian durante la sesión multi-media 701. En lugar de tener un flujo de clave, la configuración de componentes 700 utiliza tres flujos de claves 709, 711, y 713. Los flujos de claves 709, 711, y 713 corresponden a los componentes 703, 705, y 707, respectivamente.

La Figura 8 muestra una variación de la configuración de componentes mostrada en la Figura 4 de acuerdo con una realización de la invención. Con la configuración de componentes 800, el componente 805 se encripta con claves desde el flujo de clave 809. Sin embargo, el flujo de clave 809 proporciona claves que son actualmente aplicables para desencriptar el componente 805 así como claves que se usarán posteriormente al desencriptar el componente 805. En el ejemplo mostrado en la Figura 8, se aplica actualmente la clave k_1 (que corresponde al datagrama 811) mientras que se aplican posteriormente las claves k_2 (que corresponde al datagrama 813) y k_3 (que corresponde al datagrama 815). Aunque los componentes 803 y 807 no se encriptan durante la sesión multi-media 801, los componentes 803 y 807 pueden encriptarse con otras variaciones de la realización. Tener las claves que se aplicarán posteriormente posibilita a un dispositivo receptor suavizar las transiciones de clave durante la sesión multi-media 801. Por ejemplo, el dispositivo receptor puede configurar la pila de IP con una nueva clave para reducir las interrupciones al desencriptar datagramas de contenido.

La Figura 9 muestra una variación de la configuración de componentes mostrada en la Figura 4 de acuerdo con una realización de la invención. El flujo de clave 909 incluye la clave que se aplica actualmente al componente 905 para encriptación así como las claves que se aplicarán posteriormente cuando la transición de clave esté en un tiempo incremental predeterminado del tiempo actual. Por ejemplo, antes de la transición de clave 951, el flujo de clave 909 incluye tanto la clave k_1 (que corresponde al datagrama 911) como k_2 (que corresponde al datagrama 913) e incluye únicamente k_2 (que corresponde al datagrama 915) después de la transición de clave 951. Como con la configuración de componentes 800, la configuración de componentes 900 ayuda al dispositivo receptor a suavizar los efectos de las transiciones de clave.

La Figura 10 muestra una configuración de componentes 1000 para una sesión multi-media 1001 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones. Sin embargo, en comparación con las configuraciones de componentes 400-900, las claves se llevan en uno o más de los componentes en lugar de tener un flujo de clave separado para transmitir las claves. Con la configuración de componentes 100, el componente 1005 incluye datagramas de contenido (por ejemplo, el datagrama de contenido 1011) así como el datagrama 1009 que proporciona la clave k_1 que se ha usado para encriptar los componentes 1003, 1005, y 1007.

La Figura 11 muestra una variación de la configuración de componentes mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones. Con la configuración de componentes 1100, el componente 1107 proporciona la clave k_1 (que corresponde al datagrama 1109) y la clave k_2 (que corresponde al datagrama 1111) que se aplican al componente 1105 durante la sesión multi-media 1101. En el ejemplo mostrado en la Figura 11, los componentes 1103 y 1107 no están encriptados con las claves proporcionadas mediante el componente 1107.

La Figura 12 muestra una variación de la configuración de componentes mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones. La configuración de componentes 1200 es similar a la configuración de componentes 1100. Sin embargo, las calves se aplican tanto al componente que lleva la información de clave (componente 1205) así como otro componente (componente 1203) durante la sesión multi-media 1201. Sin embargo, en el ejemplo mostrado en la Figura 12, el componente 1207 no está encriptado.

La Figura 13 muestra una variación de la configuración de componentes mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones. Con la configuración de componentes 1300, cada componente 1303, 1305, y 1307 lleva llaves que se aplican al mismo componente durante la sesión multi-media 1301. Por ejemplo, las claves k_{11} (que corresponden al datagrama 1309) y k_{12} (que corresponden al datagrama 1311) se aplican al componente 1303. Las claves k_{21} (que corresponden al datagrama 1313) y k_{22} (que corresponden al datagrama 1315) se aplican al componente 1305. Las claves k_{31} (que corresponden al datagrama 1317) y k_{32} (que corresponden al datagrama 1319) se aplican al componente 1307.

La Figura 14 muestra una variación de la configuración de componentes mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones. Con la configuración de componentes 1400, cada componente 1403, 1405, y 1407 lleva llaves que se aplican un componente diferente durante la sesión multi-media 1401. Por ejemplo, las claves k_{11} (que corresponden al datagrama 1413 y se llevan mediante componente 1405) y k_{12} (que corresponden al datagrama 1419 y se llevan mediante el componente 1407) se aplican al componente 1403. Las claves k_{21} (que corresponden al datagrama 1417 y se llevan mediante el componente 1407) y k_{22} (que corresponden al datagrama 1411 y se llevan mediante el componente 1403) se aplican al componente 1405. Las claves k_{31} (que corresponden al datagrama 1409 y se llevan mediante el componente 1403) y k_{32} (que corresponden al datagrama 1415 y se llevan mediante el componente 1405) se aplican al componente 1407.

La Figura 15 muestra una variación de la configuración de componentes mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones. Con la configuración de componentes 1500, la información de clave se lleva en un datagrama de contenido en lugar de en un datagrama separado. Por ejemplo, la clave k_1 está incluida en el datagrama de contenido 1509 en una porción concatenada (o con un encabezamiento especial) 1511 y k_2 está incluida en el datagrama de contenido 1513 en una porción concatenada (o con un encabezamiento especial) 1515. Las claves k_1 y k_2 se aplican a los datagramas en los componentes 1503, 1505, y 1507.

La Figura 16 muestra una variación de la configuración de componentes mostrada en la Figura 10 de acuerdo con un ejemplo no de acuerdo con las reivindicaciones. La configuración de componentes 1600 es similar a la configuración de componentes 800, en que se proporciona tanto la clave actual así como las claves posteriores. Por ejemplo, el componente 1605 lleva la clave k_1 (que corresponde al datagrama 1609) y la clave k_2 (que corresponde al datagrama 1611), donde la clave k_1 se aplica actualmente a los componentes 1603 y 1607 y la clave k_2 se aplica posteriormente durante la sesión multi-media 1601. De manera similar, la clave k_2 (que corresponde al datagrama 1613) y la clave k_3 (que corresponde al datagrama 1615) se llevan posteriormente en el componente 1605. Como con la configuración de componentes 800, la configuración de componentes 1600 ayuda al dispositivo receptor a suavizar las transiciones de clave.

La Figura 17 muestra una arquitectura 1700 para recibir una sesión multi-media de acuerdo con una realización de la invención. Con la arquitectura 1700, un dispositivo de recepción recibe la ráfaga de datos de segmento de tiempo 1701 que contiene tanto los componentes de sesión de IP como el flujo de clave relacionado con los componentes de sesión. Pluralidades de datagramas de contenido 1705, 1707, y 1709 corresponden al componente 1, componente 2, y componente 3, respectivamente. Una pluralidad de datagramas 1711 corresponden al flujo de clave. La ráfaga de segmento de tiempo 1701 se almacena en la memoria intermedia provisional 1713 antes de reenviar los datagramas (paquetes) a la pila de IP 1721. El dispositivo de recepción extrae en primer lugar las claves (que corresponden al datagrama 1717) para la ráfaga de segmento de tiempo recibida 1701 desde la memoria intermedia provisional 1713. En segundo lugar, el dispositivo de recepción instala las claves extraídas a la base de datos de Asociación de Seguridad (SA) de IPSec 1719. También, el dispositivo de recepción extrae los restantes datagramas 1715 desde la memoria intermedia provisional y los reenvía a la pila de IP 1721. Después de la desencriptación, los datagramas procesados se pasan a las aplicaciones 1723 para la presentación del contenido multi-media. En consecuencia, la pila de IP 1721 no rechaza los datagramas de contenido (a menos que haya datagramas de contenido que el dispositivo de recepción no tuviera una clave correspondiente como entregada en el segmento de tiempo actual o una ráfaga de segmento de tiempo anterior). El proceso se repite para una siguiente ráfaga de segmento de tiempo recibida 1703.

La Figura 18 muestra el diagrama de flujo 1800 para la arquitectura mostrada en la Figura 17 de acuerdo con una realización de la invención. En la etapa 1801, un dispositivo de recepción recibe una ráfaga de segmento de tiempo a través de un canal de comunicaciones, por ejemplo, un canal inalámbrico. En la etapa 1803, el dispositivo de recepción separa componentes (por ejemplo, un componente de audio y un componente de vídeo) de la ráfaga de segmento de tiempo recibida. En la etapa 1805, el dispositivo de recepción extrae el conjunto de claves asociado desde el flujo de clave. Las claves extraídas pueden aplicarse a datagramas de contenido contenidos en la ráfaga de segmento de tiempo o en ráfagas de segmento de tiempo posteriores. También, la realización soporta configuraciones en las que se usan diferentes claves para diferentes datagramas en la ráfaga de segmento de tiempo. Las claves extraídas se aplican a la base de datos de Asociación de Seguridad (SA) de IPSec (por ejemplo, la DB de SA 1719 mostrada en la Figura 17) en la etapa 1807. En la etapa 1809, los datagramas de contenido se extraen desde una memoria intermedia (por ejemplo, la memoria intermedia provisional 1713) y se envían a una pila de IP (por ejemplo, la pila 1721) en la etapa 1811. Los datagramas de contenido se desencriptan posteriormente y se envían a la aplicación correspondiente.

La Figura 19 muestra un sistema 1900 para transferencia de contenido protegido que soporta servicios de IPDC (difusión de datos de IP) de DVB-H de acuerdo con la técnica anterior. El sistema 1900 proporciona transferencia de contenido protegido para servicios de DVB-H usando IPDC como se especifica en “Interim DVB-H IP Datacast Specifications: IP Datacast Baseline Specification: Specification of Interface I_MT”, documento de DVB A080, abril de 2004. De acuerdo con esta memoria descriptiva, las porciones de datos asociados de seguridad se transmiten en un directorio de servicio electrónico (ESG) en el carrusel de SA 1921 como el fichero de SA protegido de DRM 1919 (que se proporciona mediante el gestor de derechos digitales (DRM) 1909 realizando la función de protección) y el fichero de política de IPSec 1911. Como los datos de carrusel normalmente se actualizan con poca frecuencia (por ejemplo, una vez al día) el sistema 1900 no proporciona una solución eficaz para entrega de clave, especialmente si se actualiza una o más de las claves o cambian con frecuencia.

El contenido multi-media 1901 (que corresponde a datagramas de IP) se encripta mediante el módulo de encriptación 1903 con las claves de IPSec 1905 y se transmite (como se realiza mediante el sistema de transmisión 1925) como paquetes de segmento de tiempo (después de la encapsulación multi-protocolo, codificación de FEC, y la formación de ráfaga de segmento de tiempo) al dispositivo de recepción 1926. El objeto de derechos (RO) 1923 (que se proporciona mediante la generación del objeto de derechos 1922) se transmite al dispositivo de recepción 1926 a través de un canal de interacción, en el que se proporciona el dispositivo de recepción 1926 con un medio para comunicaciones bidireccional, por ejemplo, funcionalidad de teléfono móvil. Un usuario del dispositivo de

recepción 1926 puede ordenar el servicio (contenido) y recibir en consecuencia el correspondiente objeto de derechos (RO) 1933, que permite al usuario desencriptar el contenido del servicio ordenado. En la realización, el objeto de derechos 1933 normalmente no contiene claves de IPSec 1905.

El dispositivo de recepción 1926 procesa las ráfagas de segmento de tiempo con el módulo de procesamiento de ráfagas 1927. Los paquetes recibidos se desencriptan mediante el módulo de desencriptación 1929 con una clave proporcionada mediante el módulo de extracción de clave 1931 para obtener el contenido 1935. Las claves se determinan desde el objeto de derechos 1933. Las claves normalmente se entregan en un carrusel de SA como ficheros de SA protegidos de DRM. El objeto de derechos 1933 permite al dispositivo de recepción 1926 extraer las claves.

La Figura 20 muestra un sistema 2000 que soporta servicios de IPDC de DVB-H de acuerdo con una realización de la invención. El contenido multi-media 2001 (que corresponde a los datagramas de contenido) se encripta mediante el módulo de encriptación 2003 aplicando claves de IPSec 2005. El sistema de transmisión 2025 obtiene tanto datagramas de contenido encriptados desde el módulo de encriptación 2003 como las correspondientes claves desde el DRM 2009. El sistema de transmisión 2025 forma datagramas correspondientes que contienen las claves que corresponden a encriptar los datagramas de contenido. El sistema de transmisión 2025 inserta tanto los datagramas de contenido encriptados como los datagramas correspondientes en una ráfaga de segmento de tiempo, que se transmite al dispositivo de recepción 2026 a través de un canal de comunicaciones. Aunque la Figura 20 no muestra explícitamente un módulo de radio, la realización puede proporcionar capacidad de señal inalámbrica para transmitir la ráfaga de segmento de tiempo al dispositivo de recepción 2026 a través de un canal inalámbrico.

El dispositivo de recepción 2026 procesa una ráfaga de segmento de tiempo recibida, en la que los datagramas de contenido encriptados y los correspondientes datagramas (que contienen las correspondientes claves que se usan para encriptar los datagramas de contenido recibidos) se separan (demultiplexan) mediante el módulo de procesamiento de ráfagas 2027. En la realización, el dispositivo de recepción 2026 comprende un receptor de banda ancha para recibir señales de DVB que incluyen ráfagas de segmentos de tiempo y un transceptor para comunicaciones bidireccionales en una red inalámbrica. Las comunicaciones bidireccionales soportan pedido de servicio por un usuario, mensajería de OMA, e instalación de módulo de extensión de seguridad. La realización soporta diferentes configuraciones de señal, en las que se incluyen las claves en un flujo de clave separado o en las que se incluyen las claves en componentes multi-media como se ha analizado anteriormente con las Figuras 4-16. El módulo de extracción de claves 2031 extrae las claves desde los datagramas correspondientes para desencriptar los datagramas de contenido, como se realiza mediante el módulo de desencriptación 2029. El módulo de desencriptación proporciona el contenido desencriptado 2035 a una aplicación (no mostrada) de modo que el contenido pueda presentarse.

Adicionalmente, el objeto de gestión de derechos 2023 (como se determina mediante el generador de objetos de derechos 2022) se transmite por separado al dispositivo de recepción 2026 en respuesta a un pedido de compra. En consecuencia, el dispositivo de recepción 2026 recibe el objeto de derechos 2033 para determinar si se permite procesar al dispositivo de recepción 2026 el contenido recibido.

La Figura 21 muestra un diagrama de flujo 2100 para transmitir datos para los servicios de IPDC de DVB-H en el sistema 2000 de acuerdo con una realización de la invención. En la etapa 2101, el aparato de transmisión (por ejemplo, el sistema de transmisión 2025) determina si un datagrama de contenido obtenido debería incluirse en la ráfaga de segmento de tiempo actual. Si no, se envía la ráfaga de segmento de tiempo (con datagramas de contenido previamente obtenidos y claves asociadas) al dispositivo de recepción en la etapa 2109.

Si el datagrama de contenido obtenido debiera incluirse en la ráfaga de segmento de tiempo actual, la etapa 2103 determina la clave correspondiente y encripta el datagrama de contenido con la clave en la etapa 2105. En la etapa 2107 el datagrama de contenido encriptado y la correspondiente información de clave (que corresponde a un datagrama correspondiente que puede incluirse en el componente multi-media o en un flujo de clave) se inserta en la ráfaga de segmento de tiempo actual.

La Figura 22 muestra un sistema 2200 que soporta servicios de IPDC de DVB-H de acuerdo con una realización de la invención. En la Figura 22, los elementos 2201, 2203, 2205, 2222, 2223, 2227, 2229, 2231, 2233, y 2235 corresponden a los elementos 2001, 2003, 2005, 2022, 2023, 2027, 2029, 2031, 2033, y 2035 como se muestra en la Figura 20. Como con el sistema 2000, el sistema 2200 transmite datagramas de contenido y la información de clave correspondiente en la misma ráfaga de segmento de tiempo. La información de clave se proporciona al sistema de transmisión 2225 mediante el generador de mensaje de clave 2206. El generador de mensaje de clave puede encriptar adicionalmente las claves de modo que se transmita la información de clave encriptada al dispositivo de recepción 2226 mediante el sistema de transmisión 2225. El DRM 2209, en conjunto con el generador de objetos de derechos 2222, proporciona el objeto de derechos 2233 que corresponde al servicio de IPDC de DVB-H al dispositivo de recepción 2226.

Los ficheros de política de IPSec 2211 (que pueden contener información de asociación de seguridad) se transmiten por separado en el carrusel de SA 2221 desde el servicio (contenido) y los mensajes de clave que se multiplexan y

transmiten usando segmentación de tiempo de IPDC. En la realización, el carrusel de SA 2221 se transmite como parte de la guía electrónica de servicio (ESG).

La Figura 23 muestra un sistema 2300 que soporta servicios de IPDC de DVB-H de acuerdo con una realización de la invención. El sistema 2300 soporta el acceso condicional (CA) que puede proporcionar un segundo nivel de encriptación usando una clave privada correspondiente. (Como se analizará con la Figura 26, las claves de IPSec pueden encriptarse mediante gestión de derechos digital (DRM) así como mediante un módulo de CA). El dispositivo de recepción 2326 comprende una sección de receptor y una sección de terminal. La sección de receptor realiza procesamiento de ráfagas, demultiplexación y gestión de claves. La sección de receptor incluye también la instalación de la extensión de CA y la desencriptación de clave. El DRM 2351 envía el paquete de instalación de complemento de CA 2353 al DRM 2314 de modo que se instala un nuevo módulo de extensión de CA en el dispositivo de recepción 2326 como se analizará adicionalmente con la Figura 27. La desencriptación de la clave se realiza en un entorno de procesamiento seguro. La sección de terminal realiza la gestión de clave y la desencriptación de clave además de la desencriptación (que corresponde al módulo de desencriptación 2329) y la presentación de contenido (que corresponde al contenido 2335).

La encriptación de las claves 2305 (que se usan para encriptar el contenido 2301 mediante el módulo de encriptación 2303) se realiza mediante el módulo de encriptación de clave 2311. El módulo de encriptación de clave 2311 comprende el módulo de CA 2308 y el DRM 2309. Por lo tanto, el módulo de encriptación de clave 2311 puede proporcionar dos niveles de encriptación. Tanto la información de clave encriptada como los datagramas de contenido están incluidos en la misma ráfaga de segmento de tiempo mediante el sistema de transmisión 2325.

En correspondencia, la desencriptación de la información de clave recibida se realiza mediante el módulo de desencriptación de clave 2317. El módulo de desencriptación de clave 2317 comprende el DRM 2314 y el módulo de CA 2315. El módulo de desencriptación de clave 2317 realiza dos niveles de desencriptación que corresponden a los dos niveles de encriptación. El módulo de procesamiento de ráfagas 2327 desencripta los datagramas de contenido recibidos usando las claves desencriptadas proporcionadas mediante el gestor de claves 2313. Los datagramas de contenido recibidos se desencriptan mediante el módulo de desencriptación 2329 de la sección de terminal. El gestor de claves 2313 recibe la información de clave que se demultiplexa mediante el módulo 2327 y reenvía la información de clave al módulo de desencriptación de clave 2317 (que está asociado con un entorno confiable) para desencriptación de DRM y de CA.

En la realización, el objeto de derechos (RO) se transmite como un mensaje de DRM de OMA 2 (de acuerdo con la Versión 2.0 de la Gestión de Derechos Digitales de la Alianza Móvil Abierta) desde el DRM 2309 al DRM 2314. El objeto de derechos se transmite normalmente por separado desde las ráfagas de segmento de tiempo.

La Figura 24 muestra el aparato 2400 que soporta un sistema de transmisión (por ejemplo, 2025, 2225, y 2325) como se muestra en la Figuras 20, 22, y 23 de acuerdo con una realización de la invención. En la realización, el aparato 2400 realiza funciones normalmente asociadas con una capa de enlace (la segunda capa del modelo de protocolo de OSI). El procesador 2405 obtiene datagramas encriptados desde un módulo de encriptación (no mostrado) a través de la interfaz de encriptación 2401 y la información de clave correspondiente desde un generador de claves (no mostrado) a través de la interfaz de claves 2403. La interfaz de transmisión 2407 codifica los datagramas para corrección de errores hacia delante en el dispositivo de recepción, realiza encapsulación multi-protocolo, y formatea la ráfaga de segmento de tiempo con los datagramas codificados. (En la realización, los datagramas incluyen tanto datagramas de contenido como los correspondientes datagramas que contienen las claves).

La Figura 25 muestra el aparato 2500 para un dispositivo de recepción (por ejemplo, los dispositivos de recepción 1926, 2026, 2226, y 2326 como se muestra en la Figura 19, 20, 22, y 23, respectivamente) que recibe una difusión multi-media y que aplica claves de IPSec de acuerdo con una realización de la invención. El aparato 2500 procesa una ráfaga de segmento de tiempo (por ejemplo, ráfagas de segmento de tiempo 2501 y 2503) para extraer los datagramas de contenido y flujo de clave asociado. En la realización mostrada en la Figura 25, la ráfaga de segmento de tiempo 2501 o la ráfaga de segmento de tiempo 2503 tiene datagramas de contenido (por ejemplo, datagramas de contenido 2505, 2507, y 2509) con paquetes de IP encapsulados de ESP que contienen contenido de servicio y correspondientes datagramas de clave (por ejemplo, el datagrama correspondiente 2511) que comprende mensajes de clave de UDP. Las claves en un mensaje de clave de UDP pueden protegerse con DRM.

El aparato 2500 puede distinguir entre contenido de servicio y mensajes de clave. En consecuencia, el módulo receptor 2551 separa datagramas de contenido de datagramas de clave. En la realización, a los datagramas de clave se les proporciona un nivel de prioridad superior que a los datagramas de contenido mediante el aparato de transmisión (no mostrado). En la realización, el nivel de prioridad asociado con un datagrama se indica mediante un campo, por ejemplo, un campo de tipo de servicio (ToS) o un campo de servicios diferenciados. Por lo tanto, los datagramas de clave se envían a la pila de IP 2553 antes de los correspondientes datagramas de contenido de modo que pueda permitirse más tiempo para procesamiento de clave mediante el módulo de desencriptación de clave 2555. El módulo de desencriptación de clave presenta claves encriptadas desde la pila de IP 2553 a través del gestor de claves 2559.

Las realizaciones mostradas en las Figuras 17 y 25 incluyen las claves en la misma ráfaga de segmento de tiempo como el datagrama de contenido asociado. Sin embargo, en otro ejemplo no de acuerdo con las reivindicaciones, las claves en una ráfaga de segmento de tiempo están asociadas con datagramas de contenido de desencriptación que están contenidos en la siguiente ráfaga de segmento de tiempo, permitiendo por lo tanto más tiempo para procesamiento de claves. Son posibles otras variaciones. Por ejemplo, puede proporcionarse un número de claves para uso al desencriptar contenido en una única ráfaga de segmento de tiempo y las claves pueden a continuación usarse para una pluralidad de posteriores ráfagas de segmento de tiempo.

Las claves desencriptadas se presentan al módulo de IPSec 2557 de modo que los datagramas de contenido asociados en la pila de IP 2553 pueden desencriptarse y presentarse al cliente 2561.

La Figura 26 muestra el aparato 2600 que recibe una difusión multi-media y desencripta claves de IPSec recibidas 2601 de acuerdo con una realización de la invención. El gestor de claves 2653 encamina la clave de IPSec encriptada al servidor de DRM 2655 para desencriptar un segundo nivel de encriptación usando un algoritmo de desencriptación público y clave privada 2603. El servidor de DRM 2655 devuelve la clave desencriptada de segundo nivel 2607 al gestor de claves 2653. Si el gestor de claves 2653 determina que la clave está encriptada con un primer nivel de encriptación, el gestor de claves 2653 encamina la clave de encriptación de segundo nivel al módulo de software de extensión de CA 2657. El módulo de extensión de CA 2657 utiliza un algoritmo de desencriptación secreto y clave privada 2605 para desencriptar la clave desencriptada de segundo nivel 2607. En una realización de la invención, el algoritmo de desencriptación secreto corresponde a un algoritmo de aleatorización común (CSA) de DVB, que está disponible a partir del Instituto Europeo de Normas de Telecomunicación (ETSI). El módulo de software de extensión de CA 2657 devuelve la clave desencriptada 2609 al gestor de claves 2653, que reenvía la clave desencriptada 2609 a la pila de IP 2651.

En la realización, el módulo de extensión de CA 2657 realiza un primer nivel de desencriptación que es opcional y está basado en un método de CA específico de operador que incluye una clave privada asociada y un algoritmo de desencriptación asociado. El segundo nivel de encriptación está basado en una norma abierta, por ejemplo, DRM2 de OMA. Debido a que el primer nivel de encriptación es opcional, el gestor de claves 2653 determina si se ha de aplicar un primer nivel de encriptación a la clave desencriptada de segundo nivel 2607. Si es así, el gestor de claves 2653 encamina la clave desencriptada de segundo nivel 2607 a un módulo de software de extensión de CA 2657. Si no, el gestor de claves 2653 encamina la clave desencriptada de segundo nivel 2607 directamente a la pila de IP 2651 puesto que la clave desencriptada de segundo nivel 2607 está completamente desencriptada.

En la realización, el gestor de claves 2653 determina si la clave desencriptada de segundo nivel 2607 se ha encriptado en el primer nivel examinando un indicador de encriptación asociado (no mostrado), por ejemplo, un encabezamiento o un campo de mensaje. El indicador de encriptación asociado indica 'SÍ' si se ha encriptado en primer nivel la clave desencriptada de segundo nivel 2607 y 'NO' si no se ha encriptado en primer nivel la clave desencriptada de segundo nivel 2607. Si la clave desencriptada de segundo nivel 2607 se ha encriptado en primer nivel, el indicador de encriptación asociado no está encriptado en primer nivel.

La Figura 27 muestra el sistema 2700 para desplegar un nuevo módulo de software de extensión de seguridad 2701 en el dispositivo de recepción 2750 de acuerdo con una realización de la invención. El módulo de software de extensión de seguridad 2701 está formateado como un paquete de instalación 2705 (por ejemplo, un fichero de SIS como se soporta por Symbian). El paquete de instalación 2705 está protegido (por ejemplo, con OMA-DRM2) para formar el paquete protegido 2707 y se entrega a un dispositivo de recepción usando un mecanismo de entrega. La realización soporta diferentes canales de comunicaciones en un mecanismo de entrega, incluyendo un canal de comunicaciones inalámbricas en el que el dispositivo de recepción es un terminal inalámbrico. El paquete protegido recibido 2707 se dirige al instalador de aplicación 2751, que es una aplicación confiable. El instalador de aplicación 2751 extrae el nuevo módulo de software de extensión de seguridad 2701 desde el paquete protegido 2707 y sustituye el módulo de software de extensión de seguridad actual 2755 que está actualmente instalado en el dispositivo de recepción 2750 con el nuevo módulo de software de extensión de seguridad 2701. Para extraer el nuevo módulo de software de extensión de seguridad 2701, el dispositivo de recepción 2750 recibe el objeto de derechos 2703 que se procesa mediante el DRM 2753. En consecuencia, el DRM 2753 indica al instalador de aplicación 2751 que se permite la sustitución del módulo de software de extensión de seguridad.

En las realizaciones de la invención, las configuraciones de componentes como se muestra en la Figuras 3-16 pueden incorporarse en sistemas como se muestra en la Figuras 20, 22, y 23.

Métodos y aparatos para proporcionar derechos de uso de grano fino

Aunque el análisis anterior proporciona detalles con respecto a realizaciones de métodos y aparatos para uso al proporcionar contenido de flujo continuo que puede usarse con los métodos y aparatos analizados a continuación, pueden usarse también otros métodos y aparatos.

El control de derechos para el contenido de flujo continuo es algo difícil puesto que hay una cantidad limitada de ancho de banda disponible. Una solución natural al problema es crear y entregar de la manera normal los RO con

periodos de validez muy cortos, conteniendo posiblemente la misma clave de servicio pero con diferentes derechos de uso. Esto puede ser complicado en la práctica aunque, ya que las claves de servicio cambian mucho menos frecuentemente que, por ejemplo, los programas de televisión en un canal de televisión. Como otra solución, los RO o simplemente expresiones de derechos pueden entregarse en KSM. Enviar RO completas con frecuencia en el KSM consumiría un poco de ancho de banda, sin embargo, ya que deben dirigirse a cada abonado (o un grupo de abonados) individualmente, de modo que únicamente aquellos que han pagado obtengan los derechos. Incluso si los derechos son los mismos para todos los abonados, y el acceso al KSM está limitado por otros medios de modo que el KSM necesita contener únicamente la parte de expresión de derechos de un RO, la propia expresión de derechos puede requerir un número considerable de bits, particularmente si se usa un Lenguaje de Expresión de Derechos de tipo XML. Las soluciones típicas a este problema implican diversos métodos de compresión para pasar a binario la expresión de derechos, o para limitar los posibles derechos a unos pocos casos predeterminados ("estados de uso"). Sin embargo, estas soluciones potenciales fallan al proporcionar adecuadamente RI con un control suficientemente de grano fino de una manera amigable para el ancho de banda para que sea práctico para su adopción.

Mirando en primer lugar a la Figura 28, se proporciona un ejemplo de la técnica anterior. El contenido está encriptado (E) con una clave de contenido (CK) y proporcionado a un receptor (no mostrado). El receptor obtiene por separado una RO 2860 que incluye la CK junto con un conjunto de derechos de uso. El contenido encriptado recibido puede a continuación verse o usarse de otra manera como se proporciona en el RO de acuerdo con los derechos de uso obtenidos. Sin embargo, este método de la técnica anterior no es particularmente adecuado para contenido de flujo continuo.

Volviendo a la Figura 29, se muestra un aspecto ilustrativo de la presente invención. El contenido de flujo continuo 2910 se proporciona a un difusor y se encripta en una encriptación 2915 usando la TK 2925. El receptor (no mostrado) se proporciona con la TK 2925 mediante un KSM 2940, estando formado el KSM 2940 mediante la encriptación 2930 usando la SK 2950 junto con la TK 2925. El flujo de clave, que proporciona el KSM, se anuncia a los usuarios con dirección de IP y número de puerto. Como la TK 2925 se encripta con SK 2950, el dispositivo usa el RO 2960, que contiene la SK 2950, para desencriptar el KSM 2940 para poder desencriptar el contenido de flujo continuo 2910. Además de proporcionar la SK 2950, el RO 2960 proporciona también los derechos de uso 2965.

Normalmente, la TK cambiará periódicamente. La Figura 31 proporciona un ejemplo de esto. Como se indica, la TK cambia varias veces mientras la SK es válida. En la práctica, el número de cambios en la TK puede ser mucho más alto. Cuando la TK cambia, se proporciona un nuevo KSM 2940 (Figura 29) al receptor con la nueva TK encriptada mediante la misma SK 2950. Por lo tanto, mientras la SK 2950 permanece igual, el RO 2960 permitirá al receptor desencriptar el contenido de flujo continuo. Cuando la SK cambia, sin embargo, es necesario un nuevo RO de modo que los KSM enviados al dispositivo pueda desencriptarse y el contenido de flujo continuo usado como permitido. En general, los RO comprados desde los RI deben tener periodos de validez relativamente largos para hacer al mecanismo de DRM factible. En una realización, una vez que se obtiene el RO padre, los RO hijos pueden obtenerse también. Como se ha analizado anteriormente con referencia a las claves en las Figuras 4-16, en una realización de la invención las TK se entregan en el KSM antes de su periodo de validez de modo que el usuario (dispositivo) puede desencriptar la clave o claves y la combinación de bits antes de que se reciba el contenido de flujo continuo real (o segmento de él). De manera similar, el RO puede obtenerse antes del periodo de validez.

Como se ha indicado anteriormente, los derechos normalmente se expresan en el REL. Para tratar el problema de uso de derechos en una solución amigable para el ancho de banda que proporcione suficiente precisión de control, puede usarse una nueva categoría de programa llamado variable de REL. La variable de categoría de programa puede ser pequeña, por ejemplo 2 bits, aunque aún proporciona suficientes derechos de uso para controlar algunas aplicaciones. Usar tres o más bits, sin embargo, proporciona control de grano más fino y por lo tanto puede ser deseable. El tamaño de la variable, sin embargo, es algo dependiente del método de entrega. En algunas realizaciones de la invención, en lugar de usar una variable separada, la información de categoría de programa está embebida en o concatenada con algún otro identificador, tal como el identificador de contenido, programa o identificador de servicio.

Mirando a la Figura 30, diversos proveedores de contenido (CP) proporcionan contenido a un difusor. Además, diversos RI comunican con el difusor, para determinar las categorías de programa o para proporcionar las categorías de programa, como se analizará a continuación. Debería indicarse que los RI y los CP pueden o pueden no ser las mismas entidades. El contenido se encripta y a continuación se difunde a los receptores. Debería indicarse que la encriptación de contenido puede hacerse mediante el proveedor de contenido o mediante el difusor y las claves de encriptación se entregan en consecuencia entre el encriptador y el emisor de derechos (RI).

Por ejemplo, considerando un servicio de difusión y un dispositivo. Desde un RI particular, el dispositivo obtiene un RO desde un RI particular para acceder a cierto contenido, y hay una descripción de REL de los derechos de uso para el contenido en el RO. Aunque la descripción es estática para el periodo de validez, el REL puede contener derechos de uso que son condicionales a la variable de REL de categoría de programa. Por lo tanto, a medida que el KSM cambia el valor de la variable de REL de categoría de programa, los derechos de uso (condicionales) actualmente de hecho pueden cambiar.

El valor de la variable de categoría de programa puede obtenerse desde los KSM del servicio de difusión en cuestión de dos maneras alternativas, analizadas a continuación. Puesto que los KSM se envían muy frecuentemente, los cambios del valor de variable de REL de categoría de programa y por lo tanto los cambios en derechos de uso actualmente efectivos pueden ser de grano muy fino en el tiempo. Para ahorrar ancho de banda de difusión, sin embargo, preferentemente se minimiza la cantidad de nuevos datos añadidos al KSM para indicar la variable de REL de categoría de programa.

Antes de analizar cómo pueden proporcionarse las categorías de programa al receptor, la Figura 32 muestra un ejemplo de diversas porciones de contenido. Por ejemplo, el contenido de flujo continuo 3210 puede incluir una categoría de noticias 3215, una categoría de deportes 3217, una categoría de documentales 3219 y una categoría de películas 3221. La categoría de noticias puede dividirse adicionalmente en n categorías 3215-1, 3215-2, ..., 3215-n. Estas categorías pueden representar, por ejemplo, pero sin limitación, titulares, noticias nacionales, noticias extranjeras, etc.... De manera similar, la categoría de deportes 3217 podría dividirse también adicionalmente en categorías tales como resúmenes, resultados, difusión en directo, etc... Como alternativa, las categorías pueden no tener nada que ver con el tipo de contenido, sino que simplemente se definen para cada conjunto diferente de diferentes derechos de uso. Por ejemplo, las categorías podrían estar 'altamente restringidas', 'algo restringidas', 'normal' y 'liberal', que reflejan los permisos dados al usuario.

A continuación se proporcionan dos posibles métodos para proporcionar KSM, la diferencia más significativa es la interacción necesaria entre el difusor y los RI. Debería observarse que podría usarse también alguna combinación de los dos métodos.

Mirando al primer método para determinar la categoría de programa para el REL, en un aspecto de la invención, el difusor "ordena" el contenido de flujo continuo en diferentes categorías. Por ejemplo, el número de categoría de programa puede ser relativamente pequeño, tal como 4 categorías diferentes, o puede ser relativamente grande, tal como 256 categorías de programa diferentes. Evidentemente, serán necesarios bits adicionales a medida que aumenta el número de categorías de programa, por lo tanto dos bits pueden proporcionar información con respecto a cuatro categorías de programa mientras que son necesarios 8 bits para proporcionar 256 categorías de programa. Por ejemplo, en un servicio de difusión de televisión portátil, cada programa de televisión está categorizado en una de un número de categorías de programa, que puede incluir noticias, programas de bajo valor (lv), programas de alto valor (hv), deportes lv, deportes hv, películas antiguas, películas nuevas, etc. Los RI no pueden influenciar las categorías (establecidas por el difusor y comunes a todos los RI), sino que pueden usar libremente el intervalo de valor de variable de REL de categoría de programa amplio (por ejemplo, desde 0...255) en sus derechos de uso expresados en el REL en el RO que proporcionan al dispositivo. Normalmente, sin embargo, será más práctico un número más pequeño, tal como 12-16 categorías de programa. No es necesaria comunicación extra entre el difusor y los RI. Cada uno de tales segmentos de programa puede asociarse a un conjunto de derechos (en el informe de invención: categoría de programa) incluyendo 'presentación en directo', 'almacenamiento y visualización durante 48 horas', 'almacenamiento y visualización indefinidamente', 'reenvío y copiado (reenvío) indefinidamente' o algún otro tipo similar.

Por lo tanto, el RO puede incluir derechos condicionales expresados en el REL que dependen del valor de la categoría de programa. Por lo tanto, un usuario puede comprar derechos completos de manera que el RO proporciona los máximos derechos disponibles para el contenido. Como alternativa, el usuario puede seleccionar un RO libre promocional que proporciona muchos más derechos limitados y puede permitir únicamente la visualización de porciones del contenido de flujo continuo. Periódicamente el RO se actualizará puesto que la SK cambia, por lo tanto los derechos de uso pueden variar de RO a RO. El usuario recibe el uno o más RO cuando ordena/compra/suscribe/renueva el servicio o partes de él. En una realización de la invención el usuario puede recibir en primer lugar un RO 'padre' y pueden obtenerse RO 'hijos' o crearse más tarde. Si el usuario no ha pedido (comprado/suscrito) el segmento de programa que está recibiendo, se informa al usuario de que ('No tiene los derechos para este programa/(segmento de programa)') y/o se le informa de cómo comprar los derechos.

En otro aspecto de la invención, como se muestra en la Figura 33, los RI establecen las categorías y las comunican al difusor, que a continuación pone las categorías en los KSM. Puesto que hay múltiples RI, puede ser útil limitar el número de bits que se permite por RI a dos bits. En un caso de este tipo, el intervalo de categoría de programa podría ser 0...3. Ese intervalo, sin embargo, sería específico de RI, y podría relacionar directamente por lo tanto los derechos de uso de una porción particular de contenido de flujo continuo (en lugar de tipo de contenido de flujo continuo en una forma más genérica). En un caso de este tipo, en lugar de proporcionar un RO único, pueden proporcionarse cuatro RO, cada uno con un conjunto de derechos de uso configurados por el RI.

En el mecanismo de RO que se está usando en la Figura 33, debe haber un medio para indicar qué valor de categoría se refiere a qué RI, preferentemente sin usar identidades de RI (que son mayores de dos bits). En una realización, cada KSM 3340 contiene un vector de N valores de categoría (para algún N) donde cada valor de categoría puede ser de dos bits. En otra realización de la invención, los valores de categoría pueden ser más de dos bits. Los RO proporcionados al receptor contienen un índice de RI en el intervalo 1...N de modo que el valor de categoría en cada uno del RI_1 a RI-N corresponde a un conjunto de RO. Aún en otras realizaciones de la invención uno o más bits o combinaciones de bits en el KSM pueden usarse para los valores de categoría. Mientras el KSM

puede incluir el vector, pueden usarse otros formatos y protocolos para proporcionar el valor de categoría asociado con el RI. Además, en una realización un número de bits y/o combinaciones de bits en el vector puede reservarse para uso futuro.

En otra realización de la invención, un número de bits y/o combinaciones de bits en el KSM, que pueden o pueden no haberse reservado para otros fines, pueden mapearse a los valores de categoría o interpretarse como los valores de categoría. Además, ciertas localizaciones en el KSM podrían usarse para proporcionar una indicación en cuanto a si un tipo de programa podría verse. Un RO podría determinar cuál valor de categoría basándose en el valor de categoría mediante el KSM y a continuación mirar en el lugar apropiado en el KSM para determinar qué derecho de uso existe, tal como si el contenido pudiera visualizarse. Como cada RO podría configurarse para mirar en diferentes localizaciones con el KSM para determinar los derechos de uso, el control individualizado que puede variar con cada KSM podría proporcionarse fácilmente.

Como se muestra, el usuario ha recibido en este caso cuatro RO desde el RI N.º I, cada uno con una clase de derechos de usuario. La ventaja de usar clases de derechos de uso es que el número total y tamaño de objetos de derechos puede ser menor que en el caso de un conjunto completo de RO si los derechos de uso se ofrecen para comprar en el nivel de segmentos de programa. Cuando el usuario recibe el KSM que lleva el TK real, la combinación de bits en la posición que corresponde a la posición RI N.º I permite al usuario seleccionar el RO que corresponde a esta compra. Por ejemplo un valor de 0 en el RI N.º I indicaría RO1, un valor de 1 indicaría RO2, un valor de 2 indicaría RO3 y un valor de 3 indicaría el RO4. A medida que los TK pueden cambiarse de segmento de programa a segmento de programa, el usuario puede usar sus derechos de la manera que ha pedido (comprado). Debería observarse que el usuario está 'escuchando' al KSM que se le ha anunciado (dirección de IP y número de puerto).

Por ejemplo, en un servicio de difusión de televisión portátil, basándose en programaciones de programas de televisión, los RI eligen una de las 4 categorías para cada programa, las comunican al difusor, y el difusor a continuación incluye las categorías en los KSM. Para un RI, las cuatro categorías pueden ser 1) únicamente permitida presentación en directo, 2) almacenamiento y reproducción permitidos durante 48 horas, 3) almacenamiento y reproducción permitidos indefinidamente y 4) almacenamiento, reproducción y copiado a otros dispositivos permitido indefinidamente. Este ejemplo, sin embargo, es meramente ilustrativo y pueden proporcionarse otras combinaciones de derechos de uso.

En la situación anterior todos los comparadores del conjunto de RO desde el RI pueden tener el mismo conjunto de derechos. Por ejemplo, un RI N.º J en el KSM 3340 puede corresponder a una oferta de paquete particular mientras un segundo RI N.º J+1 puede corresponder a una oferta de paquete diferente. Debería indicarse, sin embargo, que la categoría de programa para cada RI es particular a la TK, por lo tanto el mismo conjunto de RO puede proporcionar diferentes derechos de uso para diferentes TK, y adicionalmente, diferentes conjuntos de RO pueden proporcionar diferentes conjuntos y/o combinaciones de derechos de uso.

Por lo tanto, para un conjunto de RO el RO1 puede proporcionar derechos de uso de visión únicamente mientras que otro conjunto de RO el RO1 puede proporcionar desplazamiento en el tiempo.

Además, en ambas soluciones, debe recordarse que la condicionalidad basándose en las categorías únicamente complementa los derechos de uso globales en el RO, haciéndolo más dinámico: muchos derechos de uso es probable que sean incondicionales y por lo tanto no dependientes del valor de variable de REL de categoría de programa.

De manera similar, en ambas soluciones, en lugar de proporcionar condicionalidad en los derechos de uso de un único RO, la información de categoría de programa enviada en el KSM puede usarse como alternativa para seleccionar uno de un conjunto de RO complejos, o posiblemente uno de varios RO hijos relacionados al mismo RO padre.

Por lo tanto, los aspectos de la presente invención proporcionan una manera eficaz en ancho de banda de entregar derechos aplicables a todos los abonados, pero que pueden variar de programa a programa y de periodo de tiempo a periodo de tiempo, mientras aún permite la riqueza completa del REL para definir estos derechos para cada categoría de programa. La invención puede aplicarse a servicios de IPDC a través de DVB-T, DVB-H, MediaFLO, Difusión de OMA y otros sistemas.

Como puede apreciarse por un experto en la materia, un sistema informático con un medio legible por ordenador asociado que contiene instrucciones para controlar el sistema informático puede utilizarse para implementar las realizaciones ejemplares que se desvelan en el presente documento. El sistema informático puede incluir al menos un ordenador tal como un microprocesador, procesador de señales digitales y circuitería electrónica de periféricos asociada.

Aunque la invención se ha descrito con respecto a ejemplos específicos que incluyen actualmente modos preferidos para llevar a cabo la invención, los expertos en la materia apreciarán que hay numerosas variaciones y

permutaciones de los anteriores sistemas y técnicas descritos que caen dentro del alcance de la invención como se expone en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método que comprende:

(A) recibir un flujo de datos encriptados (2001), que corresponden a una única sesión multi-media, desde un sistema de comunicaciones (2000), comprendiendo el flujo de datos una pluralidad de porciones encriptadas, respectivamente, mediante una pluralidad de claves de tráfico (2205);
(B) recibir un mensaje de flujo de clave encriptada, incluyendo el mensaje de flujo de clave encriptada la pluralidad de claves de tráfico; y
(C) usar la pluralidad de claves de tráfico para desencriptar las respectivas porciones del flujo de datos encriptados,

en el que el mensaje de flujo de clave encriptada está separado del flujo de datos encriptados, y estando **caracterizado por que** cada porción del flujo de datos encriptados está incluida en la misma ráfaga de datos de segmento de tiempo como el respectivo mensaje de flujo de clave encriptada.

2. El método de la reivindicación 1, en el que (C) comprende:

(D) desencriptar el mensaje de flujo de clave con una clave de servicio.

3. El método de la reivindicación 2, que comprende adicionalmente:

(E) obtener un objeto de derechos, incluyendo el objeto de derechos la clave de servicio; y
(F) usar el flujo de datos.

4. El método de la reivindicación 1, en el que (B) comprende:

(i) recibir un valor de variable de categoría de programa.

5. El método de la reivindicación 3, en el que (F) comprende:

(i) visualizar el flujo de datos.

6. El método de la reivindicación 3, en el que (F) comprende:

(i) almacenar el flujo de datos.

7. El método de la reivindicación 3, en el que el uso del flujo de datos se controla mediante un derecho de uso asociado al objeto de derechos.

8. El método de la reivindicación 2, que comprende adicionalmente:

(E) repetir (A), (B), (C) y (D) después de que cambie la clave de tráfico.

9. El método de la reivindicación 3, en el que el objeto de derechos incluye adicionalmente un valor de variable de categoría de programa asociado a derecho de uso incluido en el mensaje de flujo de clave y (F) está controlado por el derecho de uso.

10. Un medio de almacenamiento legible por ordenador que tiene instrucciones ejecutables por ordenador almacenadas en el mismo que, cuando se ejecutan mediante un ordenador, provocan que el ordenador realice el método indicado en cualquier reivindicación anterior.

11. Un aparato (2026) que comprende:

un receptor para recibir:

un flujo de datos encriptados, que corresponden a una única sesión multi-media, desde un sistema de comunicación (2000), comprendiendo el flujo de datos encriptados una pluralidad de porciones encriptadas, respectivamente, mediante una pluralidad de claves de tráfico (2005); y
un mensaje de flujo de clave encriptada, incluyendo el mensaje de flujo de clave encriptada la pluralidad de claves de tráfico; y

un procesador para usar la pluralidad de claves de tráfico para desencriptar las respectivas porciones del flujo de datos encriptados,

en donde el mensaje de flujo de clave encriptada está separado del flujo de datos encriptados, y estando **caracterizado por que** cada porción del flujo de datos encriptados está incluida en la misma ráfaga de datos de segmento de tiempo como el respectivo mensaje de flujo de clave encriptada.

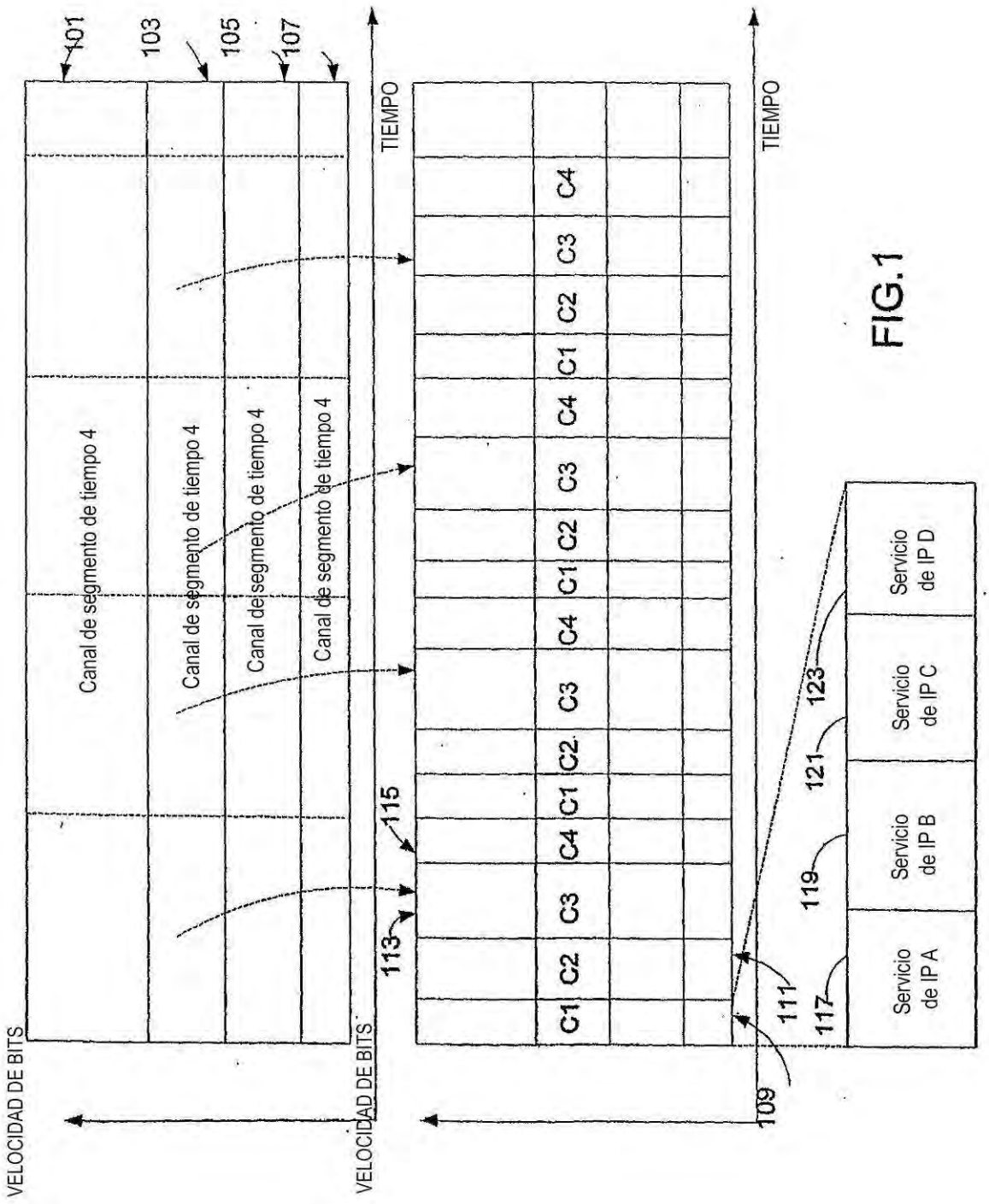
101
103
105
107
Canal de segmento de tiempo 4
Canal de segmento de tiempo 4
Canal de segmento de tiempo 4
Canal de segmento de tiempo 4
VELOCIDAD DE BITS
TIEMPO
113
115
C1 C2 C3 C4 C1 C2 C3 C4 C1 C2 C3 C4
VELOCIDAD DE BITS
TIEMPO
109
111
117
119
121
123
Servicio de IP A
Servicio de IP B
Servicio de IP C
Servicio de IP D

FIG.1

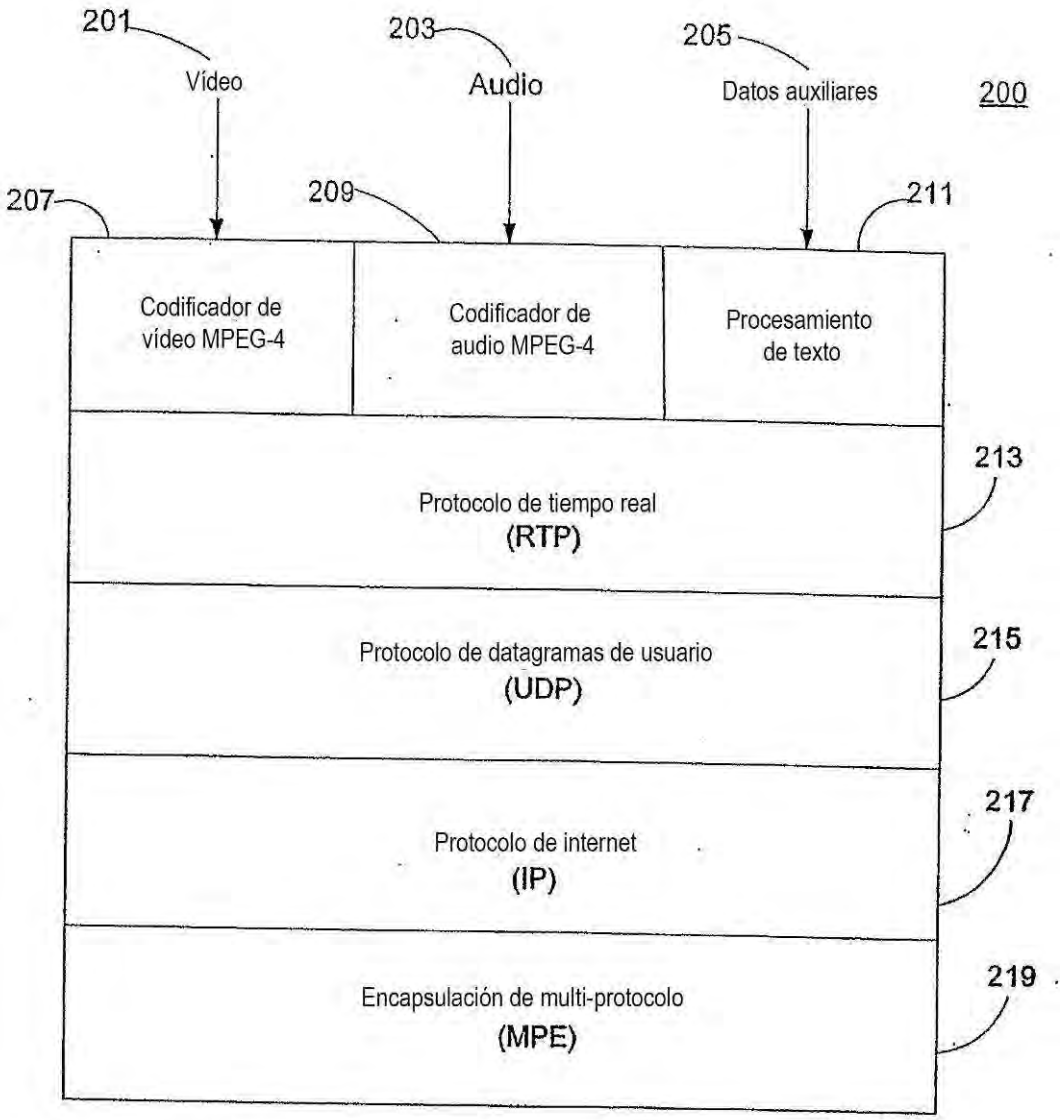
201
Vídeo
203
Audio
205
Datos auxiliares
200
207
209
211
Codificador de vídeo MPEG-4
Codificador de audio MPEG-4
Procesamiento de texto
213
Protocolo de tiempo real
(RTP)
215
Protocolo de datagramas de usuario
(UDP)
217
Protocolo de internet
(IP)
219
Encapsulación de multi-protocolo
(MPE)

FIG. 2

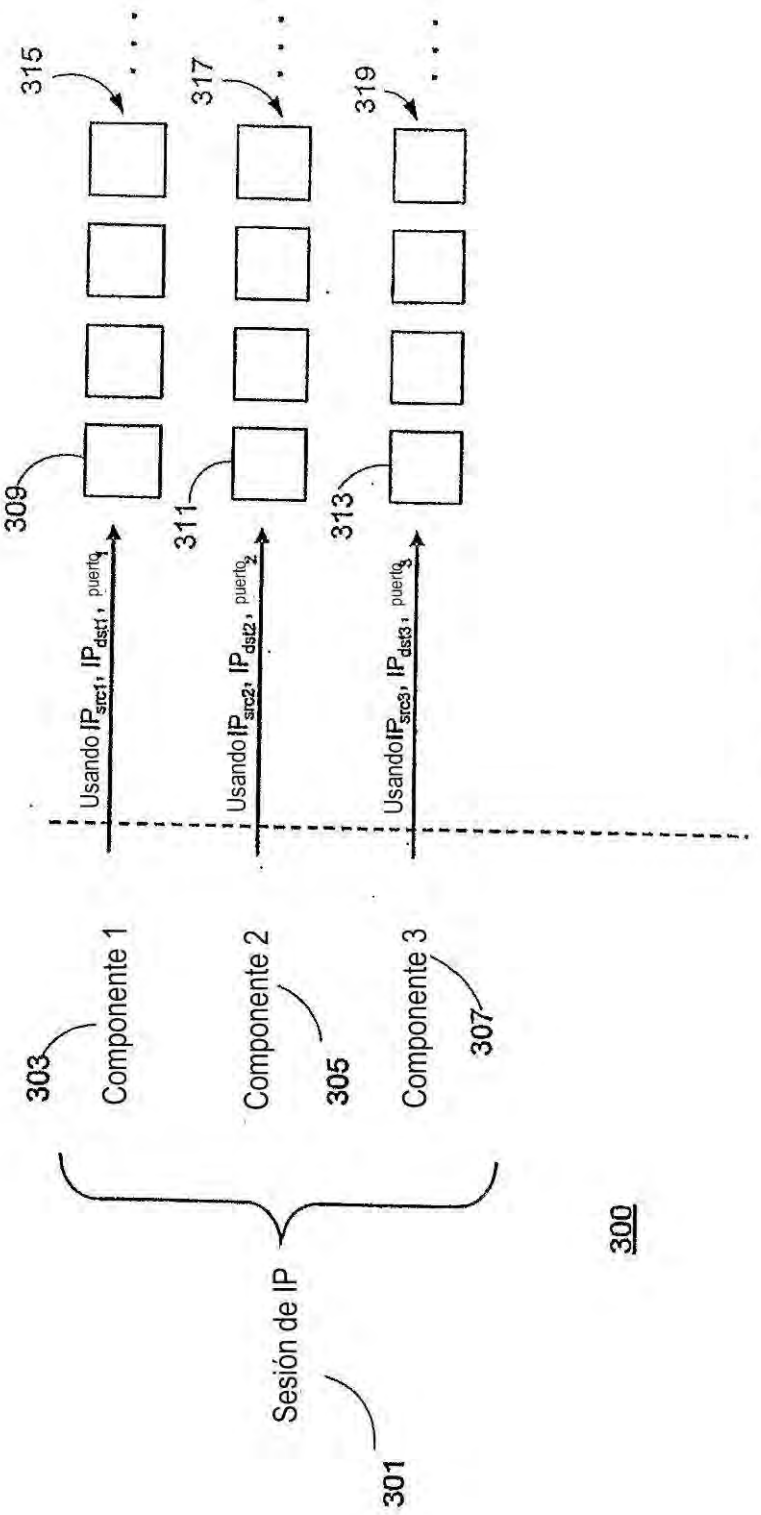
315
317
319
309
311
313
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
Componente 1
Componente 2
Componente 3
303
305
307
Sesión de IP
301
300
Transmitido como un flujo de paquetes de IP

FIG. 3

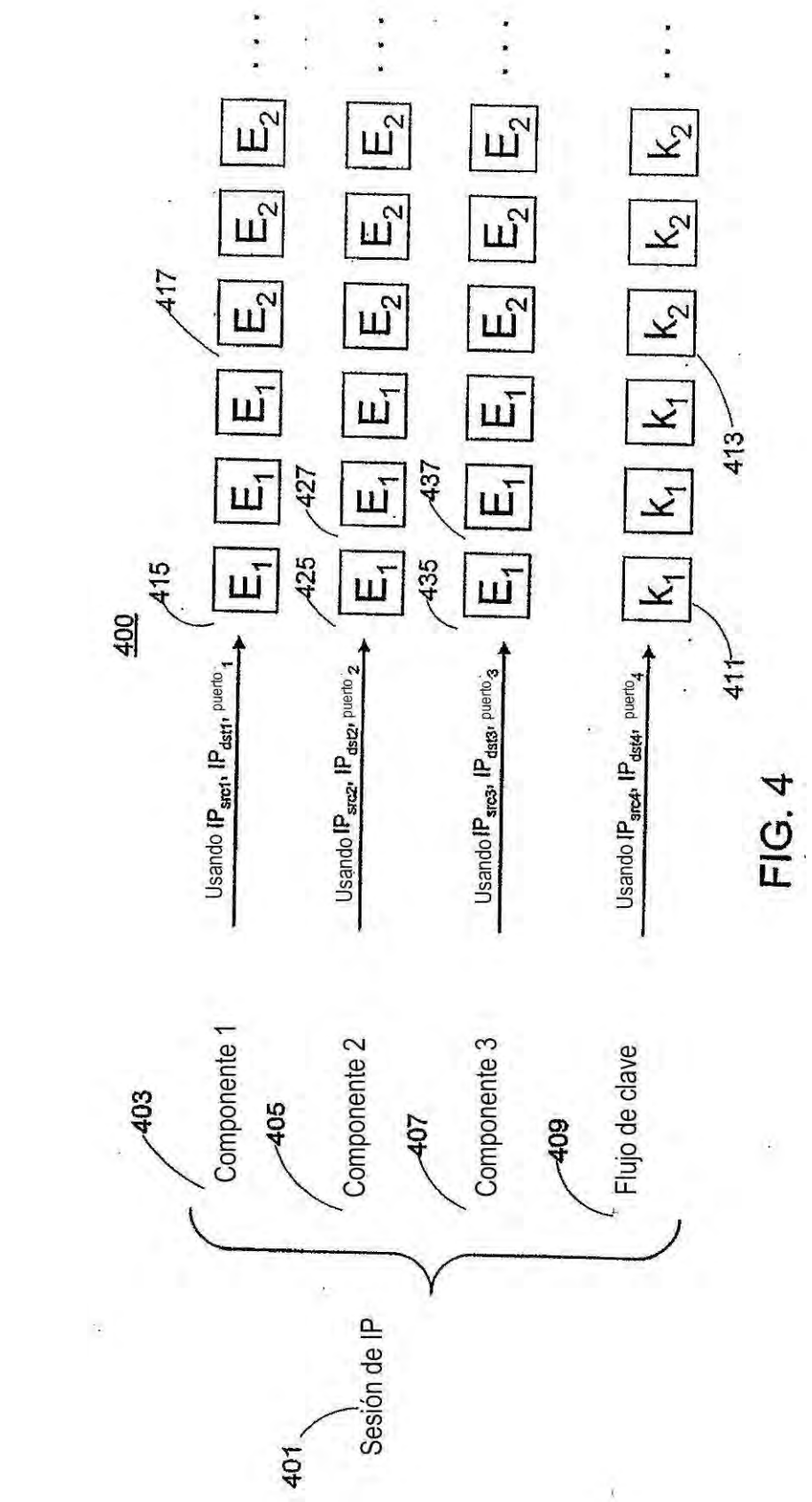
400
401
Sesión de IP
403
Componente 1
405
Componente 2
407
Componente 3
409
Flujo de clave
Usando IP_{src1}, IP_{dst1}, puerto 1
Usando IP_{src2}, IP_{dst2}, puerto 2
Usando IP_{src3}, IP_{dst3}, puerto 3
Usando IP_{src4}, IP_{dst4}, puerto 4
411
413
415
417
425
427
435
437
E_1
E_2
k_1
k_2

FIG. 4

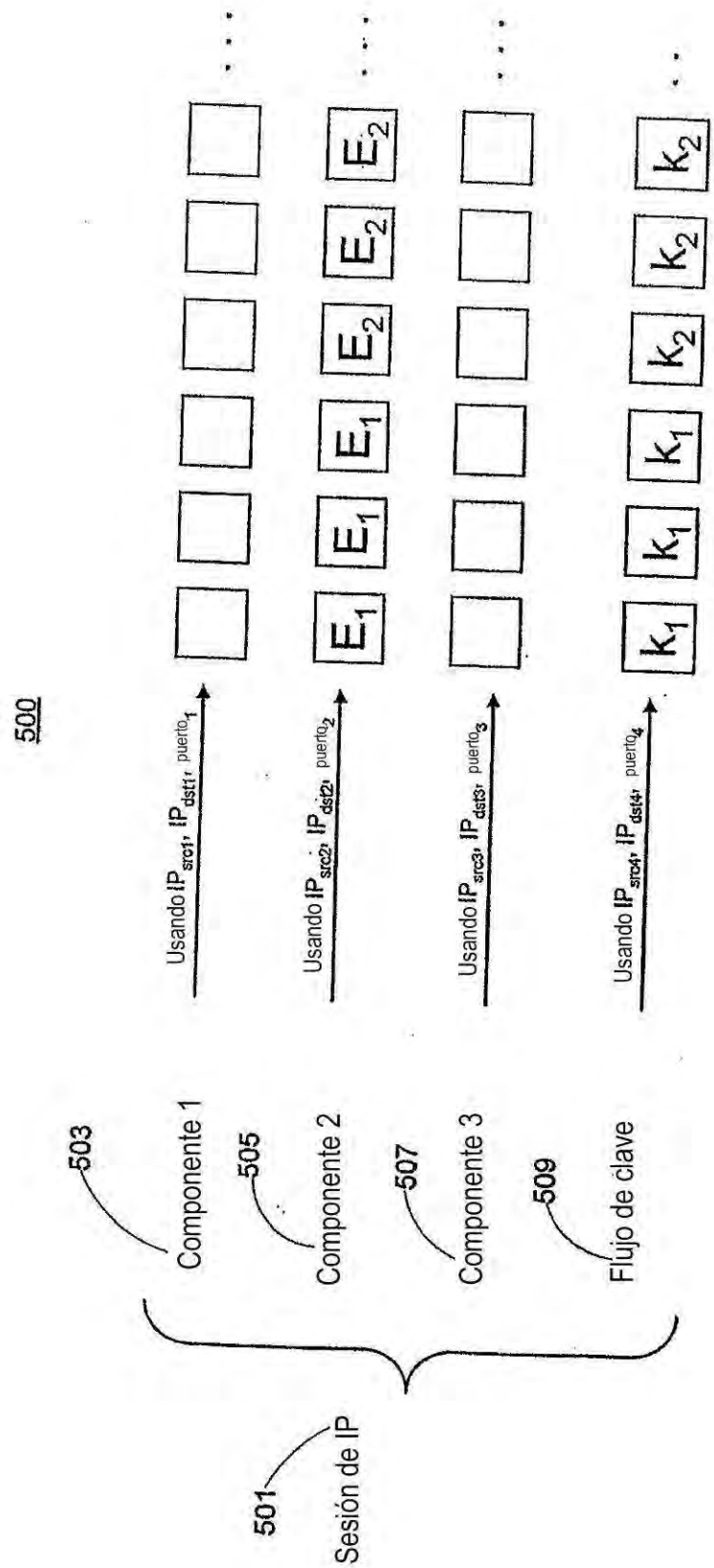
500
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
Usando IP_{src4}, IP_{dst4}, $puerto_4$
E_1
E_2
k_1
k_2
503
Componente 1
505
Componente 2
507
Componente 3
509
Flujo de clave
501
Sesión de IP

FIG. 5

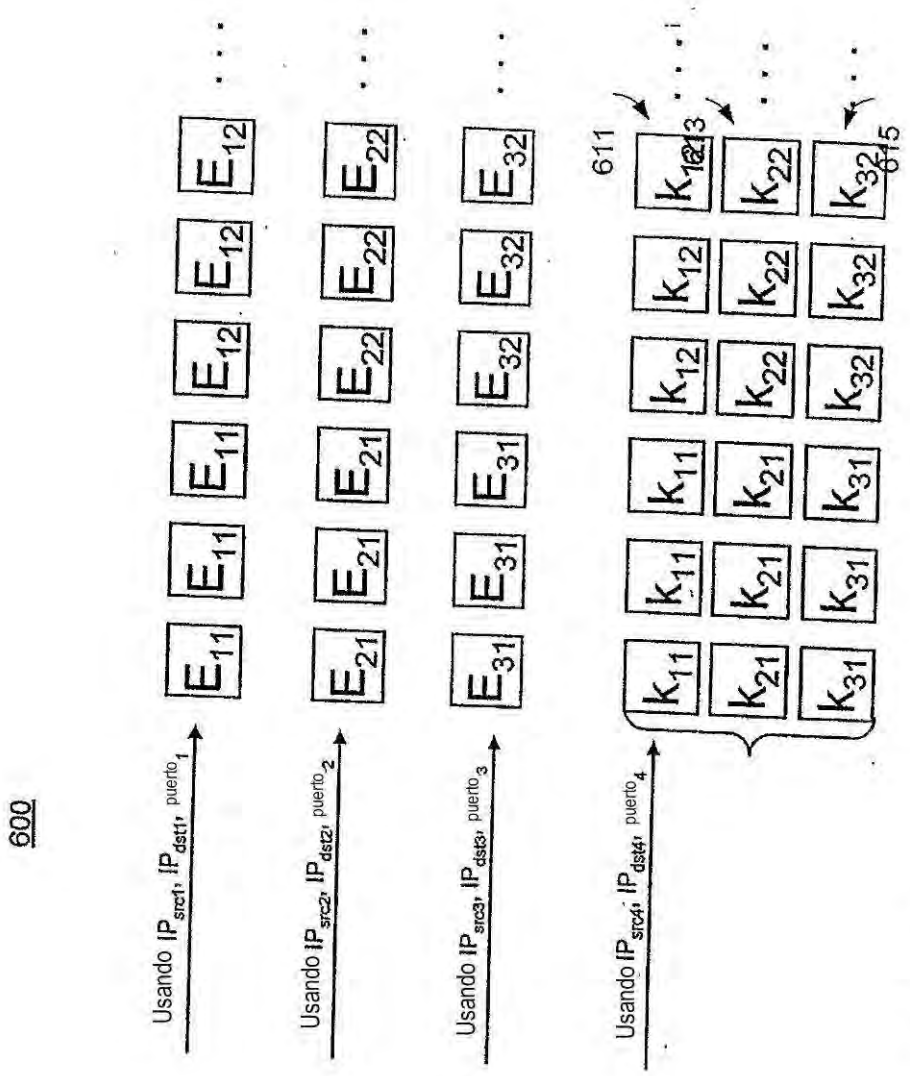
600
601
Sesión de IP
603
Componente 1
605
Componente 2
607
Componente 3
609
Flujo de clave
611
613
615
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
Usando IP_{src4}, IP_{dst4}, $puerto_4$
E_{11} E_{12} E_{21} E_{22} E_{31} E_{32}
K_{11} K_{12} K_{21} K_{22} K_{31} K_{32}

FIG. 6

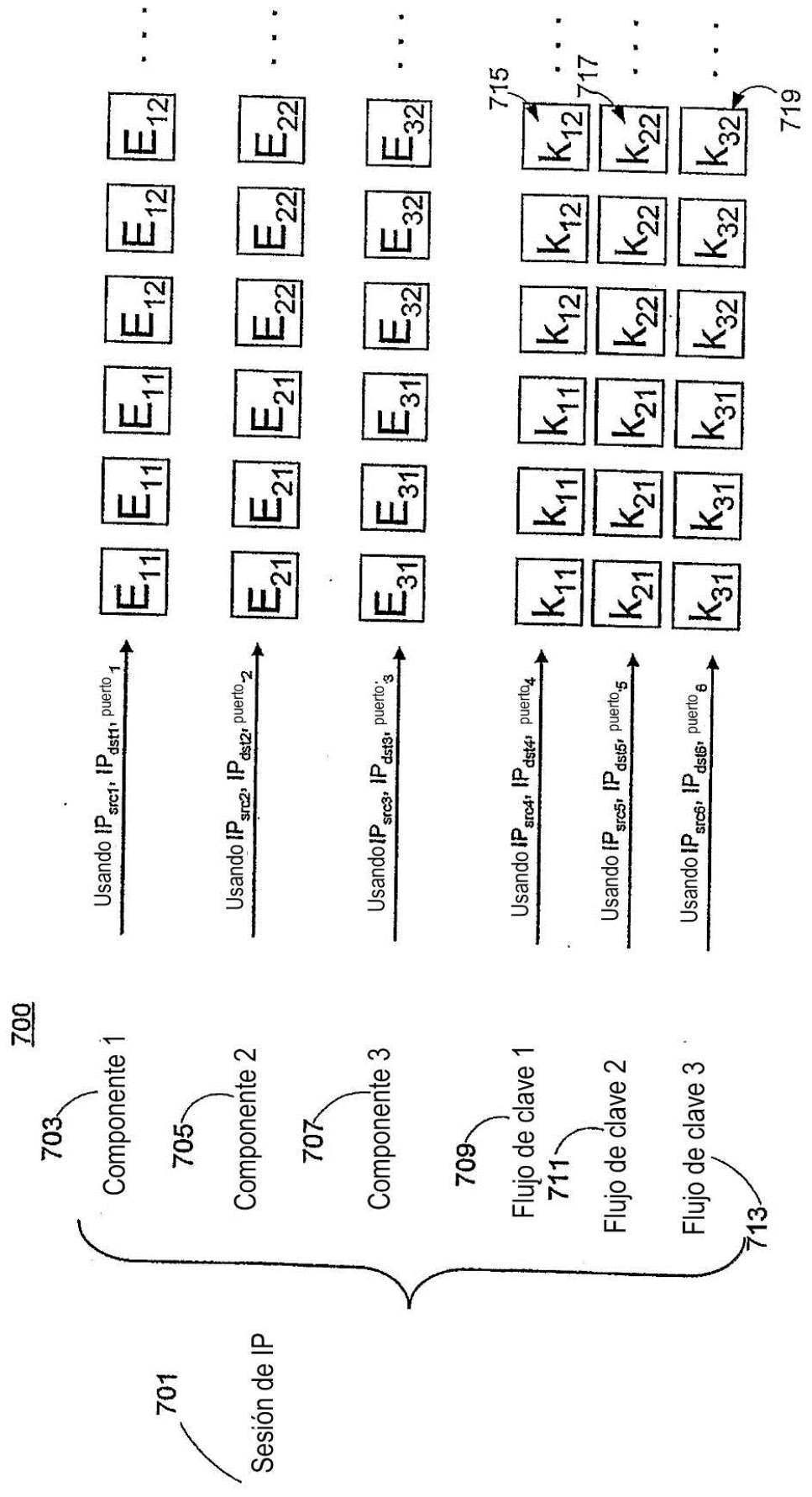
700
701
Sesión de IP
703
Componente 1
705
Componente 2
707
Componente 3
709
Flujo de clave 1
711
Flujo de clave 2
713
Flujo de clave 3
Usando IP_src1, IP_dst1, puerto_1
Usando IP_src2, IP_dst2, puerto_2
Usando IP_src3, IP_dst3, puerto_3
Usando IP_src4, IP_dst4, puerto_4
Usando IP_src5, IP_dst5, puerto_5
Usando IP_src6, IP_dst6, puerto_6
E11
E21
E31
E12
E22
E32
K11
K21
K31
K12
K22
K32
715
717
719

FIG. 7

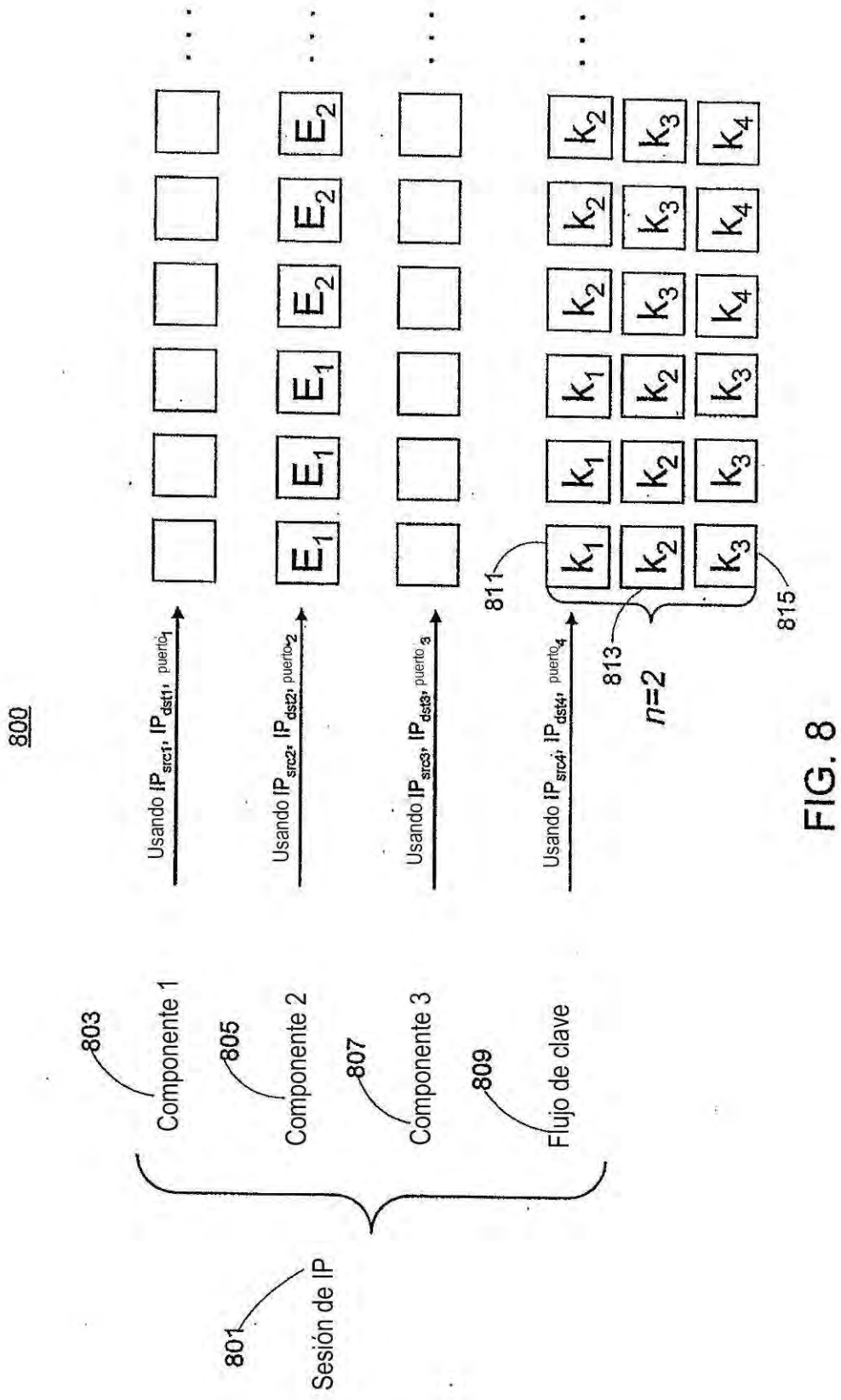
800
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
Usando IP_{src4}, IP_{dst4}, $puerto_4$
803
Componente 1
805
Componente 2
807
Componente 3
809
Flujo de clave
801
Sesión de IP
811
813
815
n=2

FIG. 8

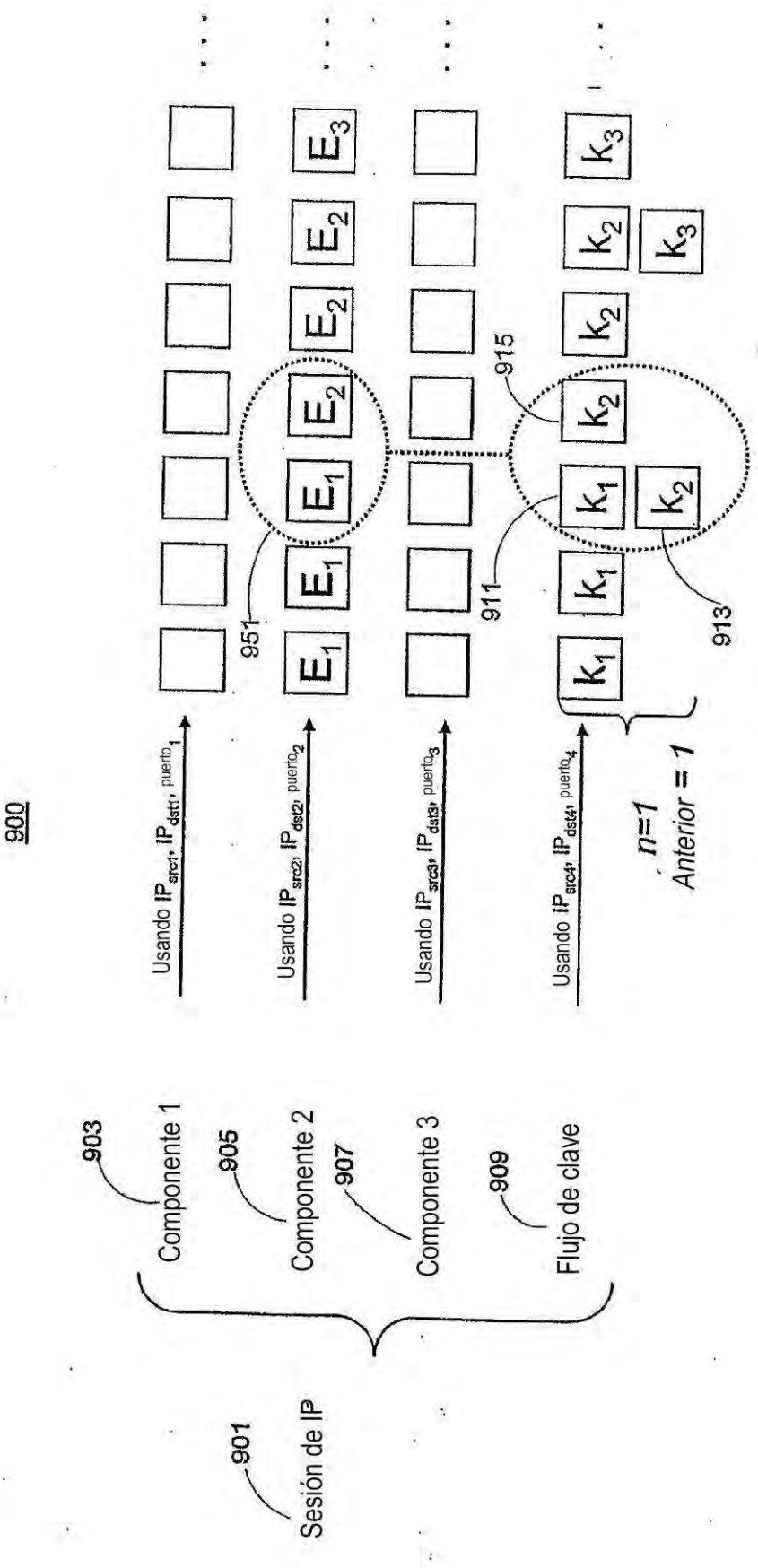
900
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
Usando IP_{src4}, IP_{dst4}, $puerto_4$
951
911
913
915
n=1
Anterior = 1
903
Componente 1
905
Componente 2
907
Componente 3
909
Flujo de clave
901
Sesión de IP

FIG. 9

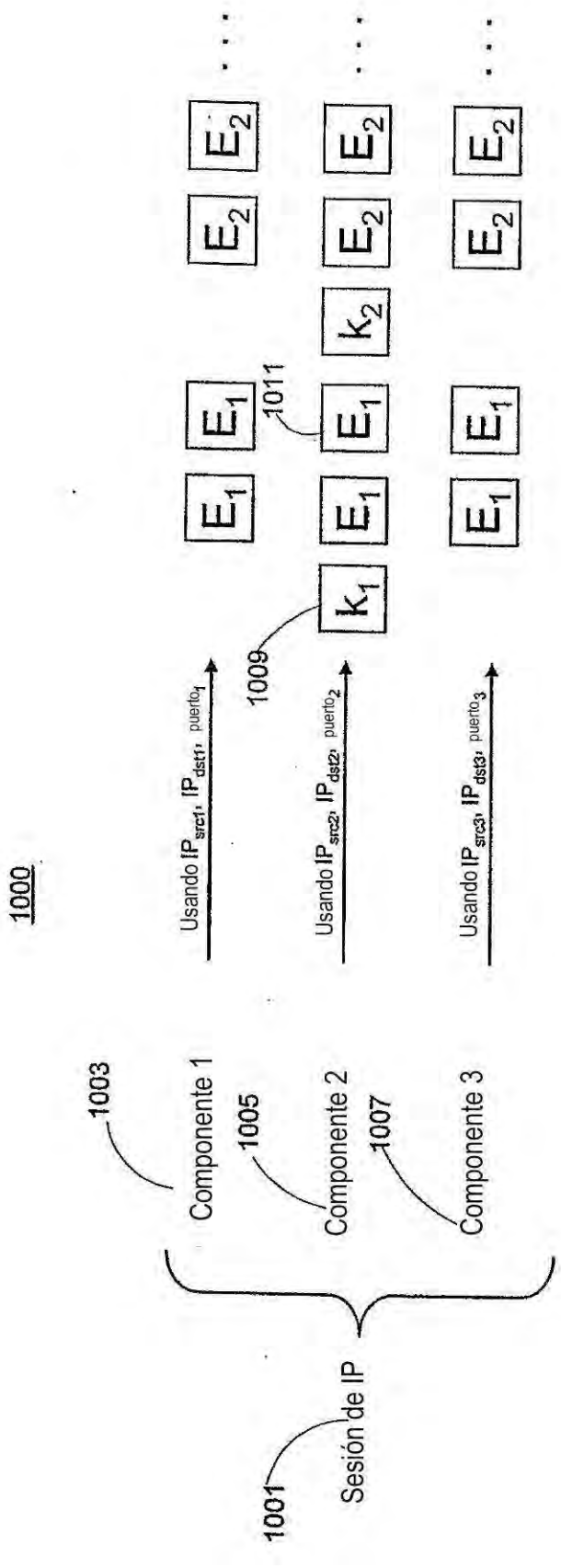
1000
1001
Sesión de IP
1003
Componente 1
1005
Componente 2
1007
Componente 3
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
1009
1011
k_1
k_2
E_1
E_2

FIG. 10

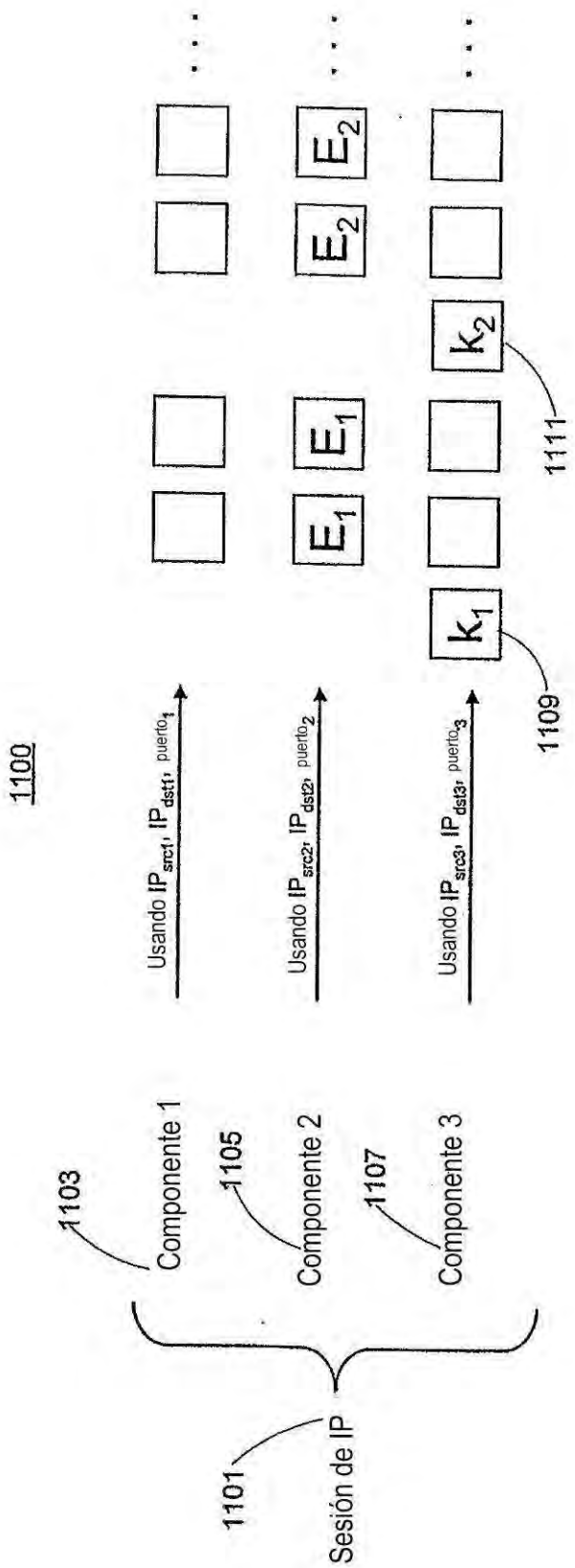
1100
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
1109
1111
1103
Componente 1
1105
Componente 2
1107
Componente 3
1101
Sesión de IP

FIG. 11

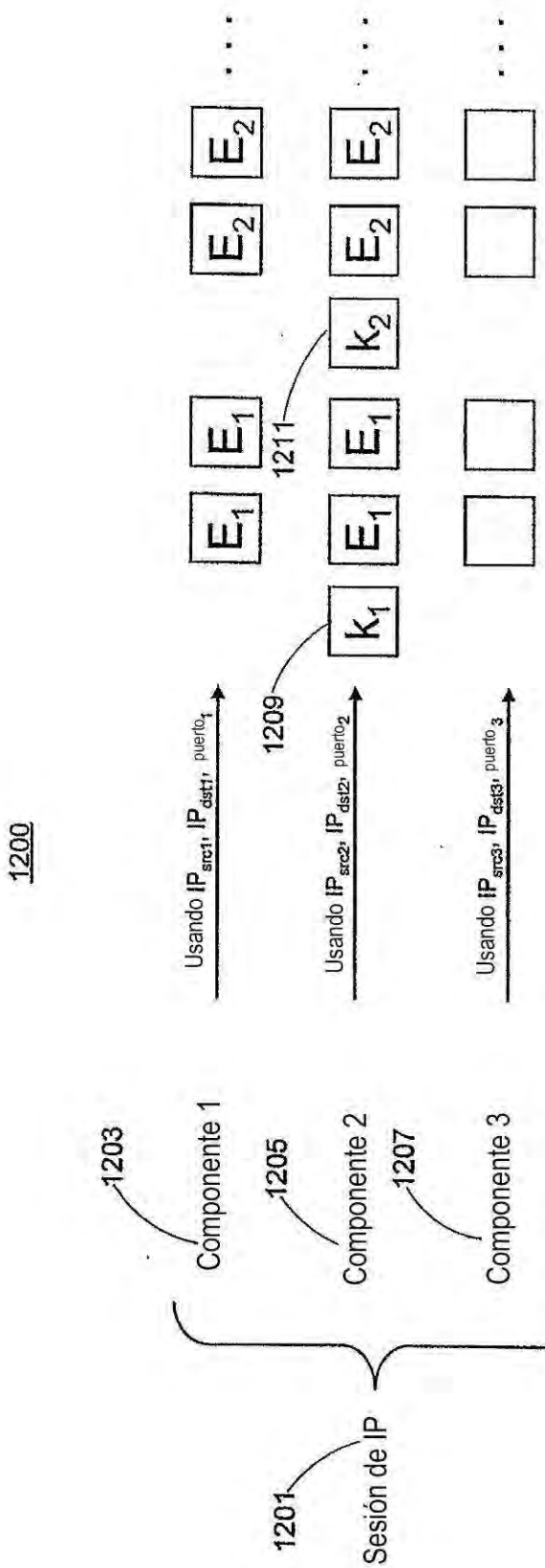
1200
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
1209
1211
E_1
E_2
k_1
k_2
1203
Componente 1
1205
Componente 2
1207
Componente 3
1201
Sesión de IP

FIG. 12

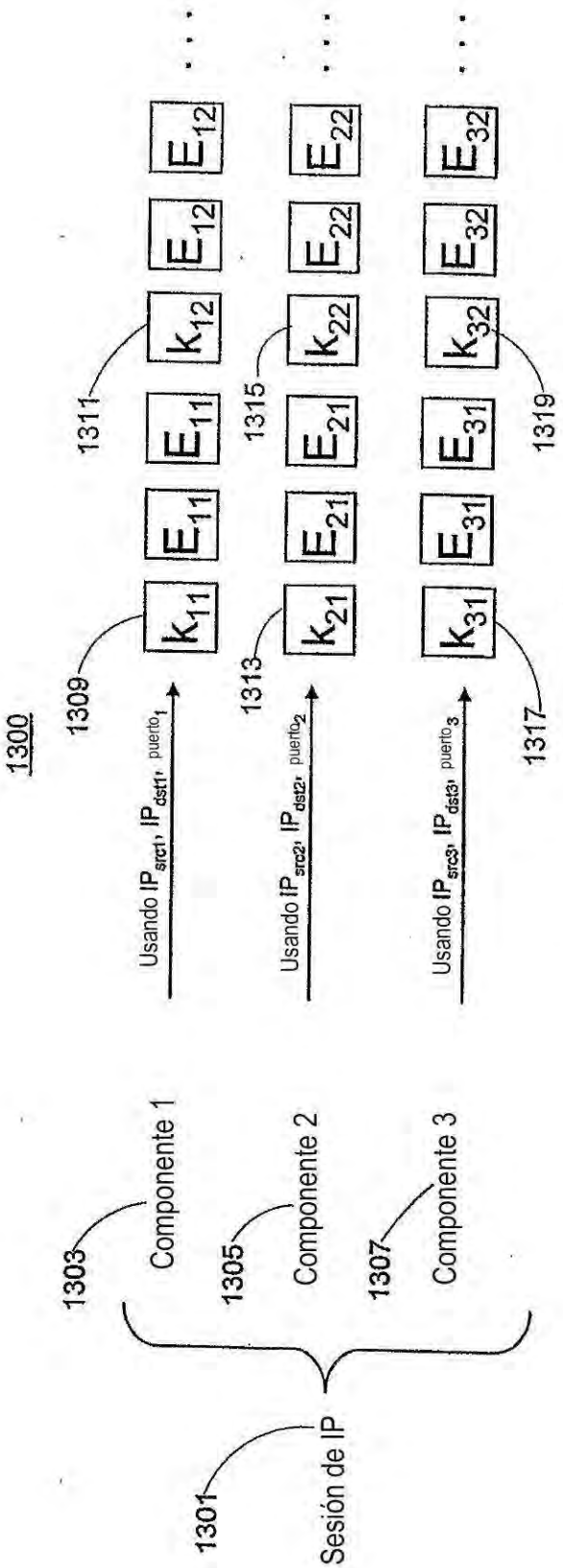
1300
1301
Sesión de IP
1303
Componente 1
1305
Componente 2
1307
Componente 3
1309
1311
1313
1315
1317
1319
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
k_{11} E_{11} E_{11} k_{12} E_{12} E_{12} . . .
k_{21} E_{21} E_{21} k_{22} E_{22} E_{22} . . .
k_{31} E_{31} E_{31} k_{32} E_{32} E_{32} . . .

FIG. 13

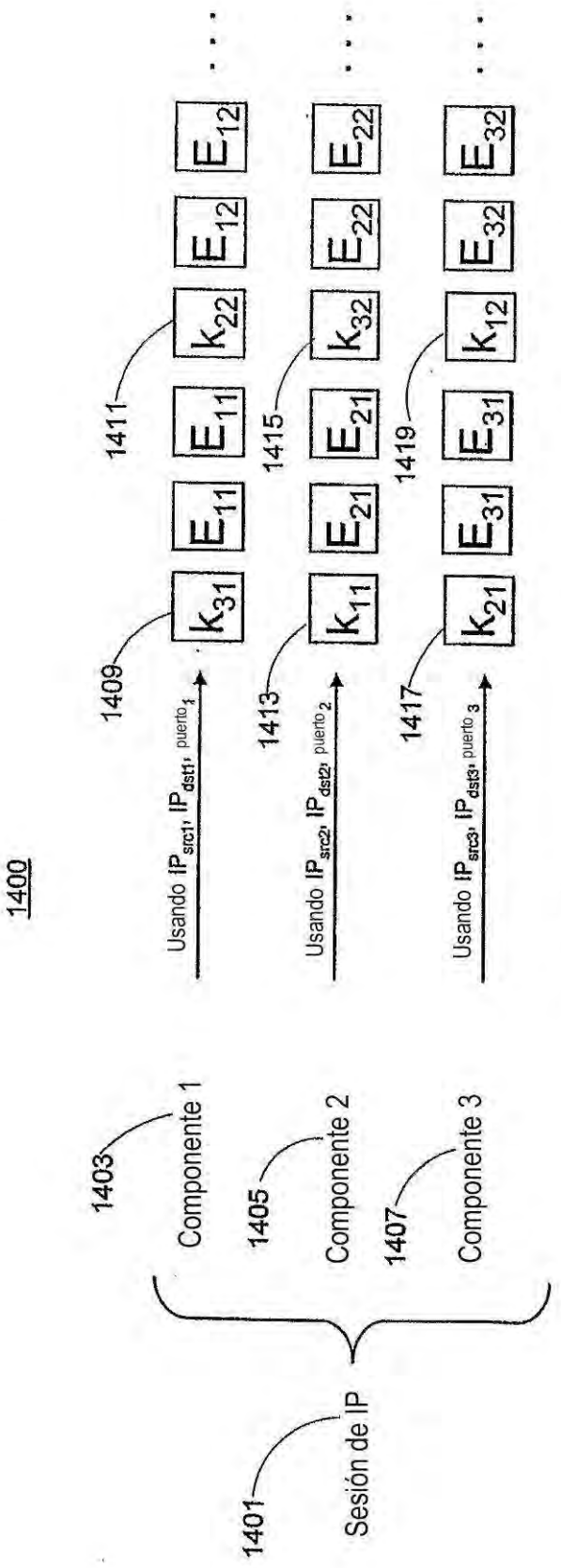
1400
1401
Sesión de IP
1403
Componente 1
1405
Componente 2
1407
Componente 3
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
1409
1411
1413
1415
1417
1419
k_{31} E_{11} k_{22} E_{12} . . .
k_{11} E_{21} k_{32} E_{22} . . .
k_{21} E_{31} k_{12} E_{32} . . .

FIG. 14

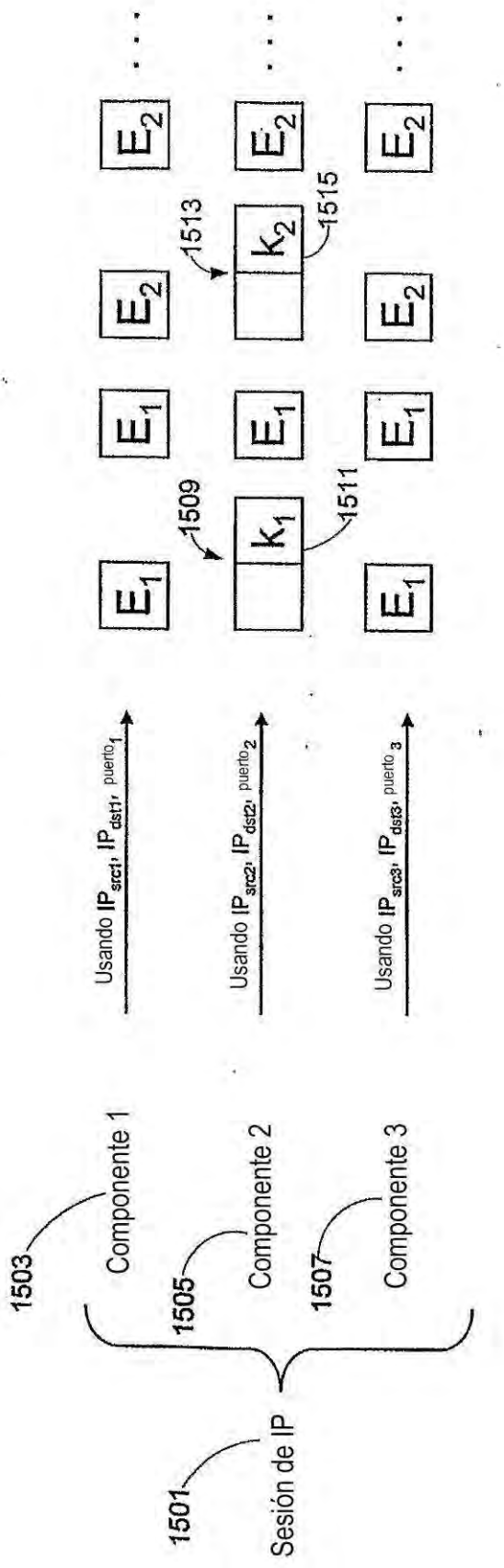
1500
1501
Sesión de IP
1503
Componente 1
1505
Componente 2
1507
Componente 3
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
1509
1511
1513
1515
E_1
E_2
k_1
k_2

FIG. 15

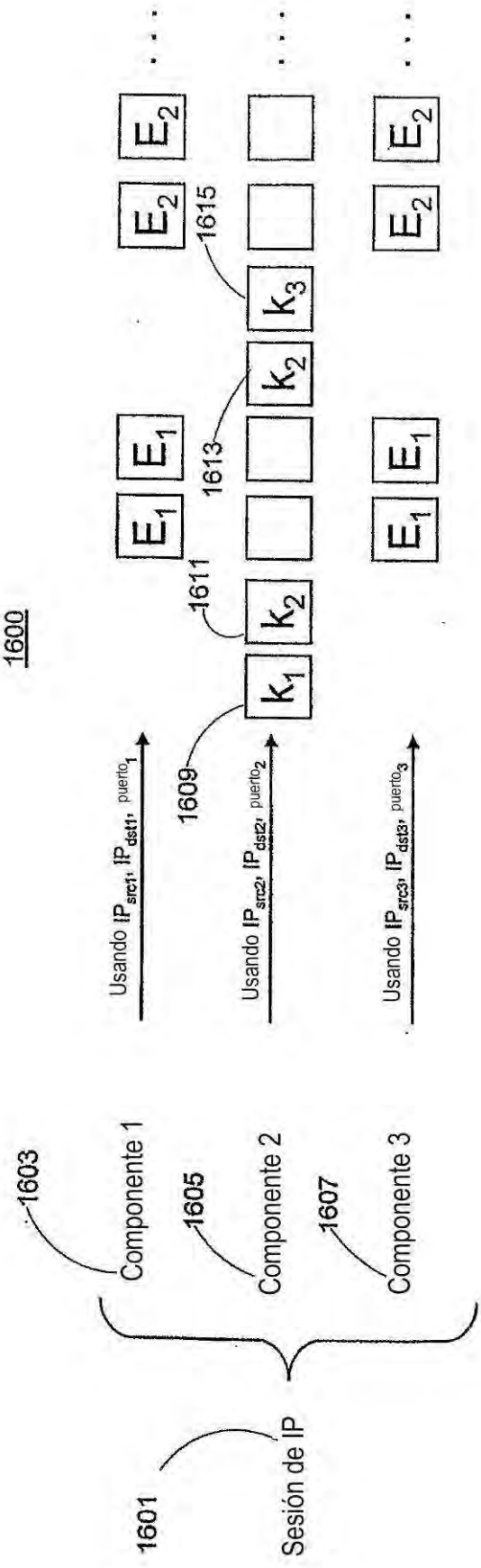
1600
1601
Sesión de IP
1603
Componente 1
1605
Componente 2
1607
Componente 3
Usando IP_{src1}, IP_{dst1}, $puerto_1$
Usando IP_{src2}, IP_{dst2}, $puerto_2$
Usando IP_{src3}, IP_{dst3}, $puerto_3$
1609
1611
1613
1615
k_1
k_2
k_2
k_3
E_1
E_1
E_1
E_1
E_2
E_2
E_2
E_2

FIG. 16

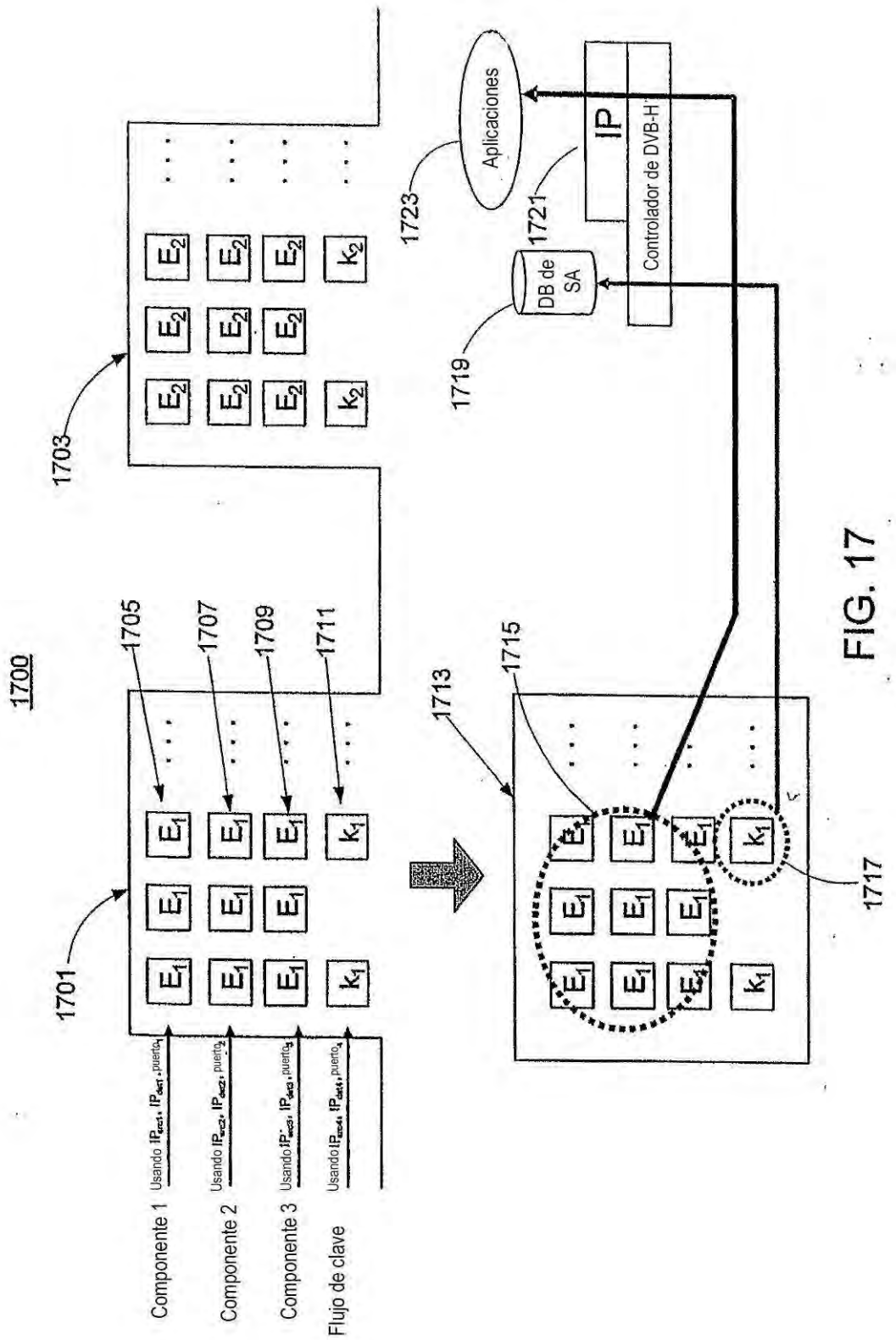
1700
1701
1703
1705
1707
1709
1711
1713
1715
1717
1719
1721
1723
Componente 1
Componente 2
Componente 3
Flujo de clave
Aplicaciones
IP
Controlador de DVB-H
DB de SA

FIG. 17

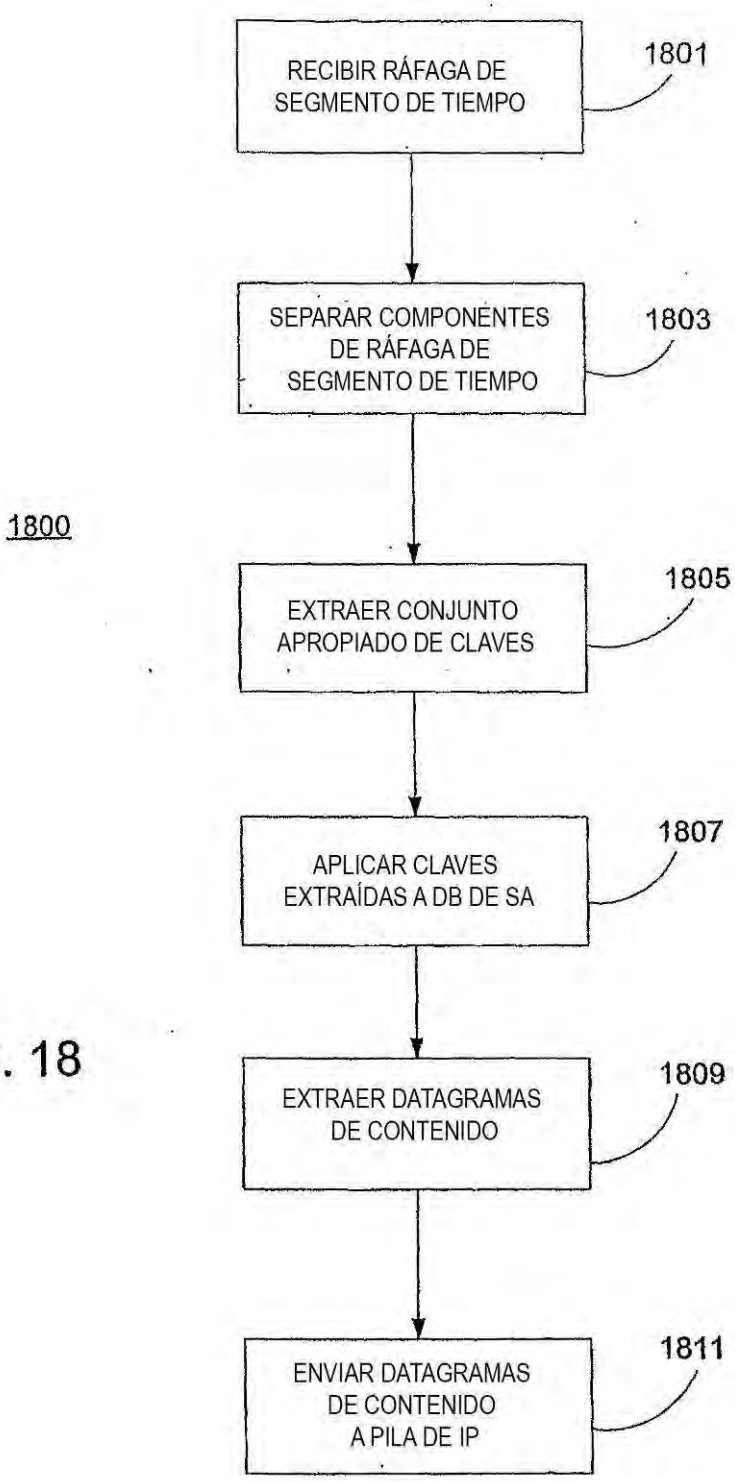
1800
RECIBIR RÁFAGA DE SEGMENTO DE TIEMPO
1801
SEPARAR COMPONENTES DE RÁFAGA DE SEGMENTO DE TIEMPO
1803
EXTRAER CONJUNTO APROPIADO DE CLAVES
1805
APLICAR CLAVES EXTRAÍDAS A DB DE SA
1807
EXTRAER DATAGRAMAS DE CONTENIDO
1809
ENVIAR DATAGRAMAS DE CONTENIDO A PILA DE IP
1811

FIG. 18

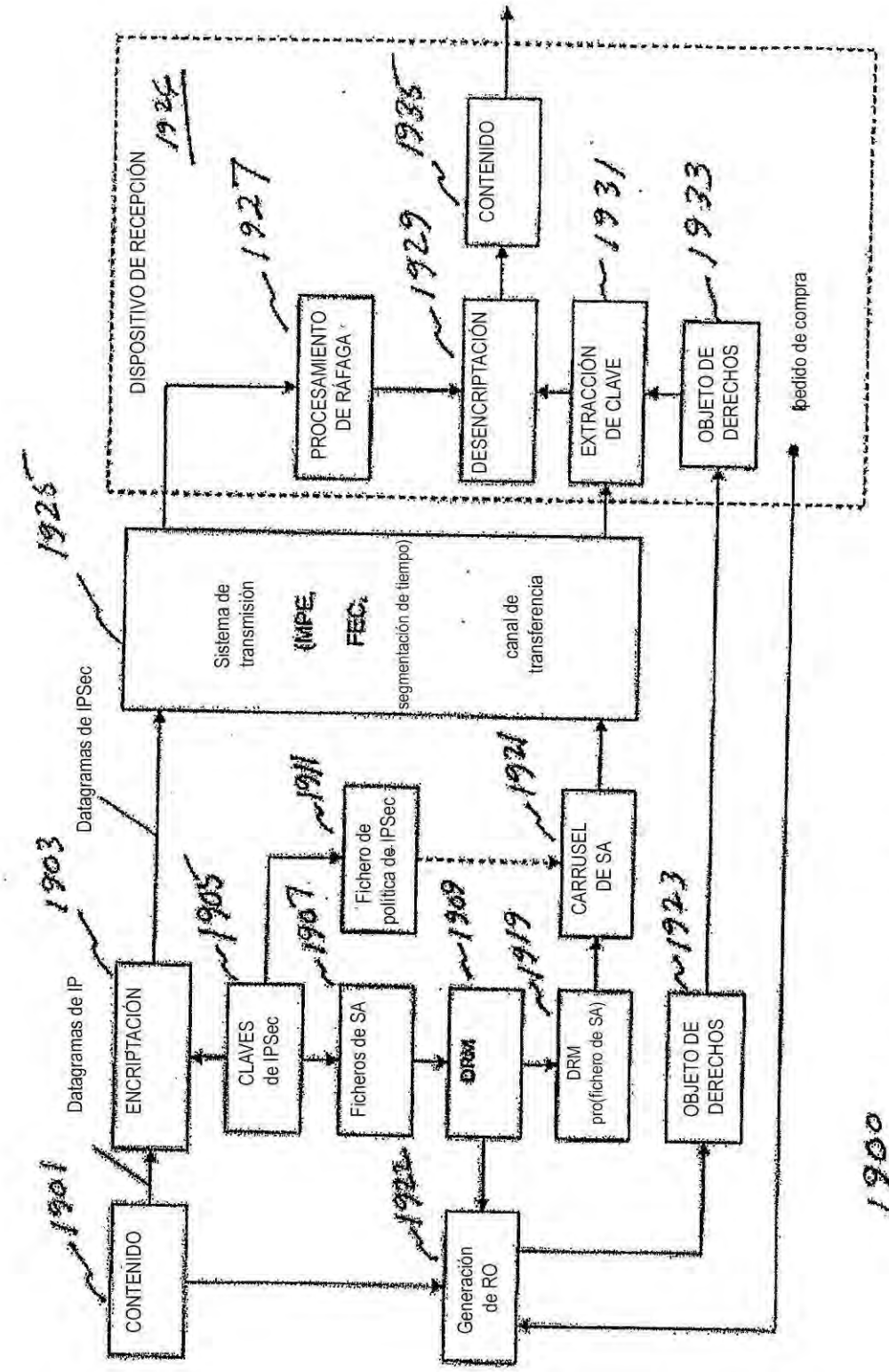

FIG. 19 (Técnica anterior)

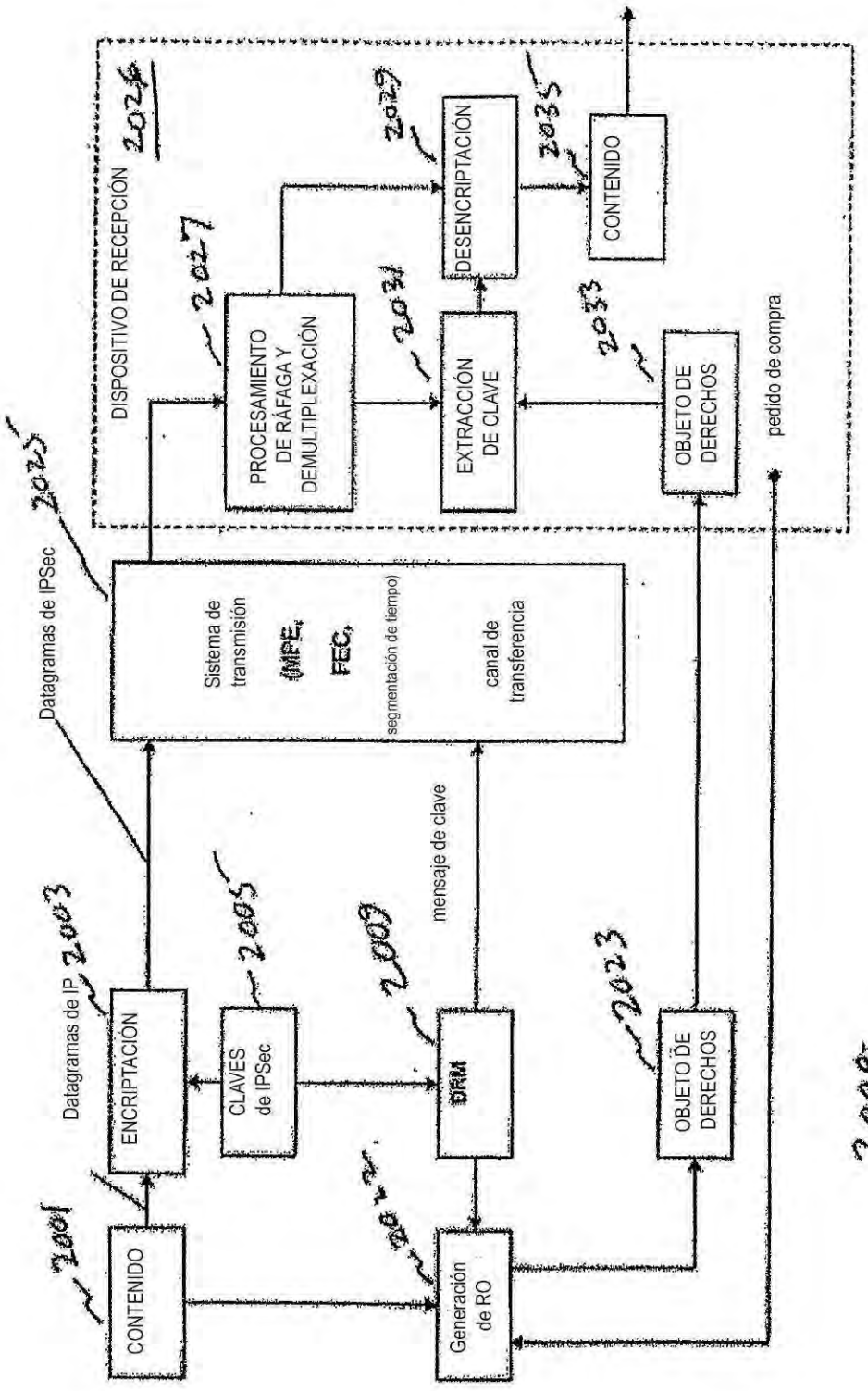
2000
2001
CONTENIDO
2003
ENCRIPTACIÓN
Datagramas de IP
Datagramas de IPSec
2005
CLAVES de IPSec
2007
Generación de RO
2009
DRM
mensaje de clave
2021
Sistema de transmisión
MPE,
FEC,
segmentación de tiempo)
canal de transferencia
2023
OBJETO DE DERECHOS
2025
DISPOSITIVO DE RECEPCIÓN
2027
PROCESAMIENTO DE RÁFAGA Y DEMULTIPLEXACIÓN
2029
DESENCRIPTACIÓN
2031
EXTRACCIÓN DE CLAVE
2033
OBJETO DE DERECHOS
2035
CONTENIDO
pedido de compra

FIG. 20

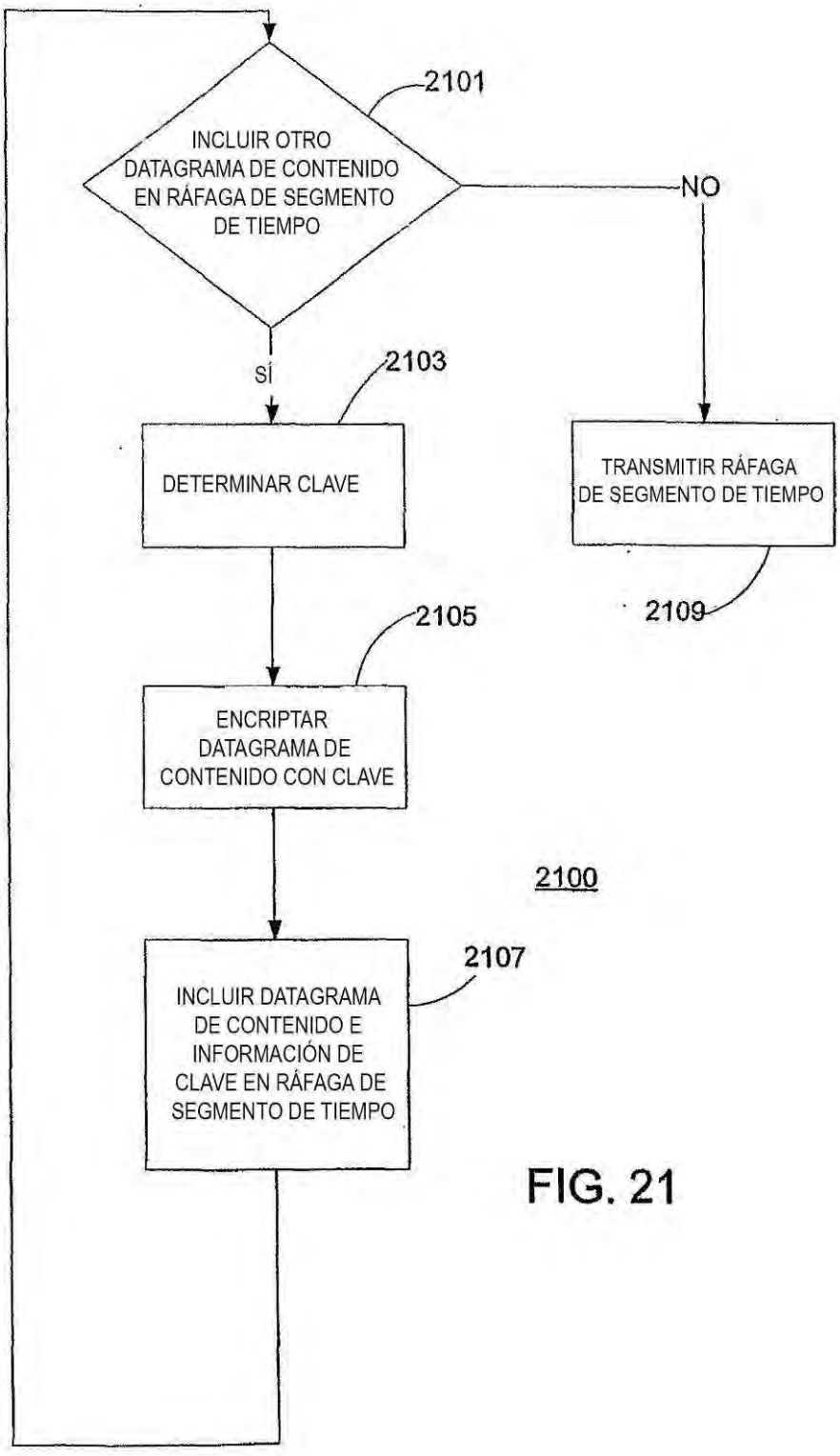
2101
INCLUIR OTRO DATAGRAMA DE CONTENIDO EN RÁFAGA DE SEGMENTO DE TIEMPO
NO
SÍ
2103
DETERMINAR CLAVE
TRANSMITIR RÁFAGA DE SEGMENTO DE TIEMPO
2109
2105
ENCRIPTAR DATAGRAMA DE CONTENIDO CON CLAVE
2100
2107
INCLUIR DATAGRAMA DE CONTENIDO E INFORMACIÓN DE CLAVE EN RÁFAGA DE SEGMENTO DE TIEMPO

FIG. 21

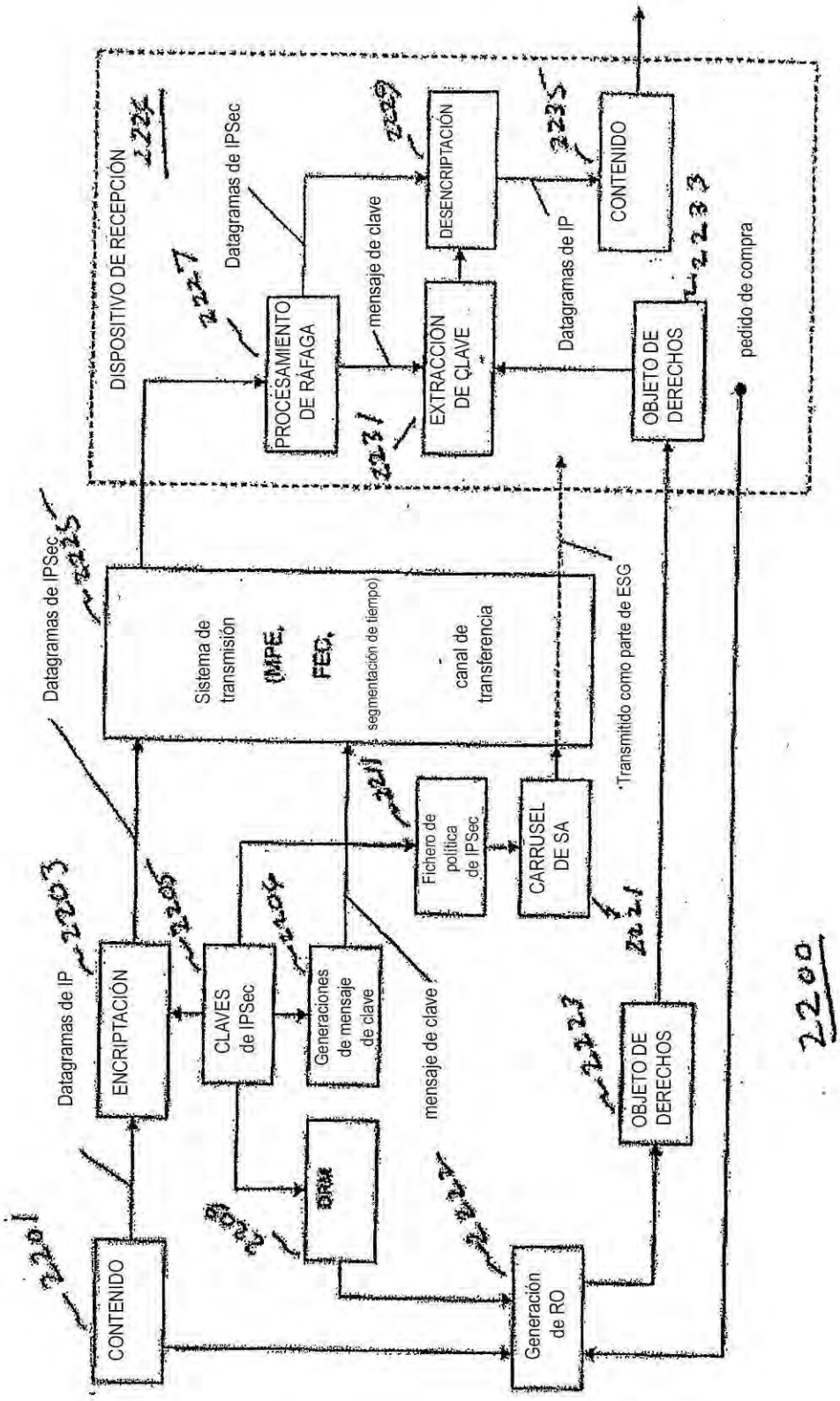
2200
2201
CONTENIDO
DRM
2203
Datagramas de IP
ENCRIPTACIÓN
2205
CLAVES de IPSec
2207
Generaciones de mensaje de clave
mensaje de clave
2209
Generación de RO
2211
Fichero de política de IPSec
CARRUSEL DE SA
2213
OBJETO DE DERECHOS
Datagramas de IPSec
2215
Sistema de transmisión
(MPE, FEC, segmentación de tiempo)
canal de transferencia
Transmitido como parte de ESG
DISPOSITIVO DE RECEPCIÓN
2224
2227
Datagramas de IPSec
PROCESAMIENTO DE RÁFAGA
mensaje de clave
2231
EXTRACCIÓN DE CLAVE
2229
DESENCRIPTACIÓN
Datagramas de IP
2225
CONTENIDO
2233
OBJETO DE DERECHOS
pedido de compra

FIG. 22

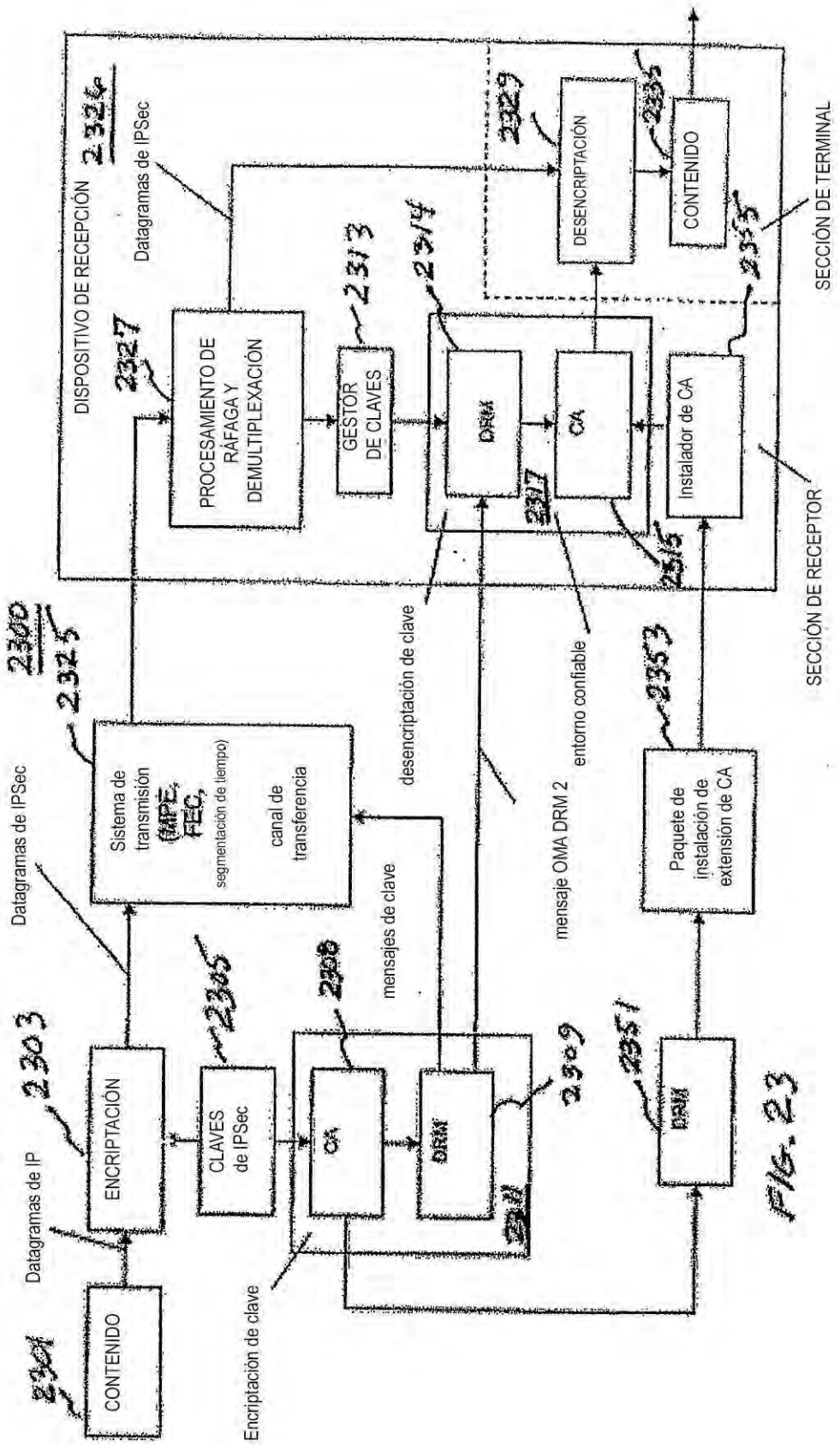
2301
CONTENIDO
Datagramas de IP
2303
ENCRIPTACIÓN
Datagramas de IPSec
2305
CLAVES de IPSec
2306
CA
DRM
2309
2311
Encriptación de clave
mensajes de clave
2300
2325
Sistema de transmisión (MPE, FEC, segmentación de tiempo)
canal de transferencia
Datagramas de IPSec
DISPOSITIVO DE RECEPCIÓN 2326
2327
PROCESAMIENTO DE RÁFAGA Y DEMULTIPLEXACIÓN
2313
GESTOR DE CLAVES
2314
DRM
CA
2317
2315
desencriptación de clave
mensaje OMA DRM 2
entorno confiable
2329
DESENCRIPTACIÓN
2335
CONTENIDO
2355
Instalador de CA
SECCIÓN DE RECEPTOR
SECCIÓN DE TERMINAL
2353
Paquete de instalación de extensión de CA
2351
DRM

FIG. 23

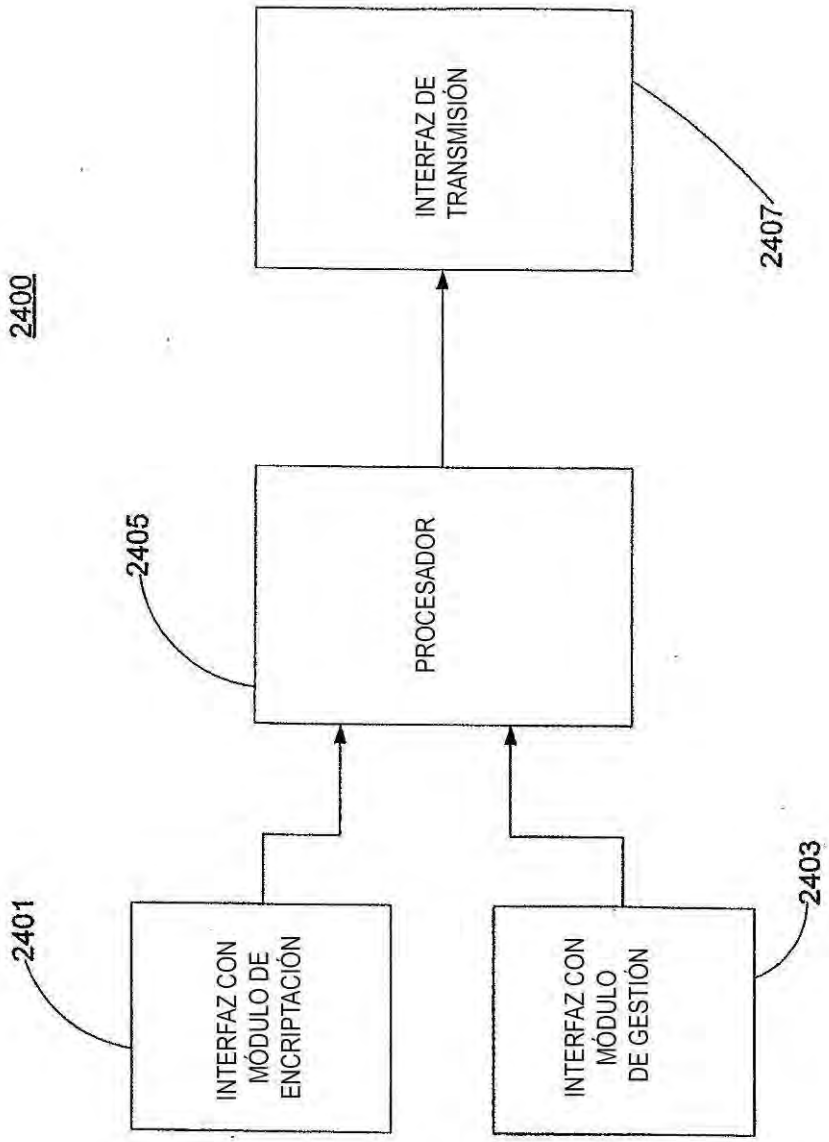
2400
2401
INTERFAZ CON MÓDULO DE ENCRIPTACIÓN
2403
INTERFAZ CON MÓDULO DE GESTIÓN
2405
PROCESADOR
2407
INTERFAZ DE TRANSMISIÓN

FIG. 24

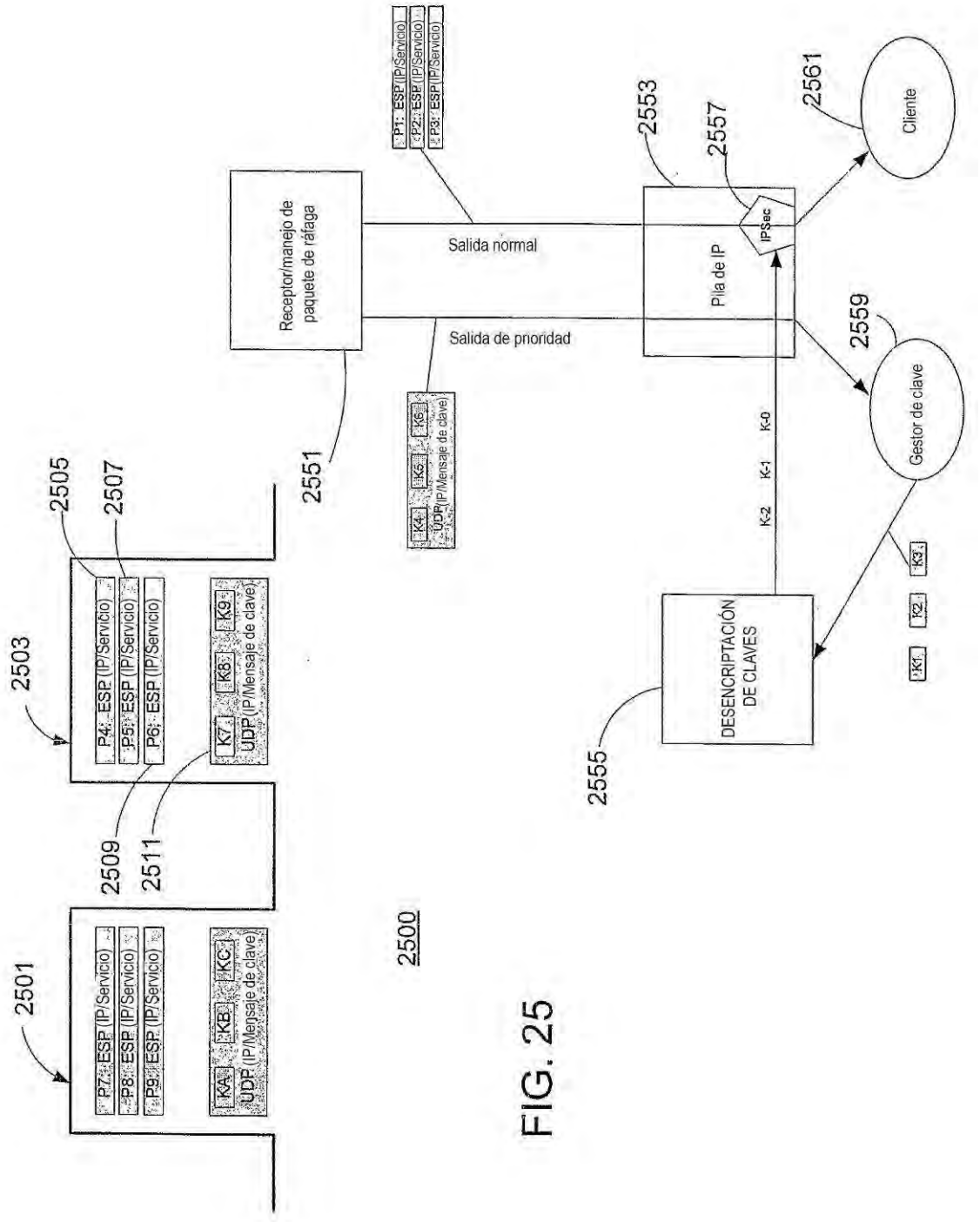
2500
2501
2503
2505
2507
2509
2511
2551
2553
2555
2557
2559
2561
P7: ESP (IP/Servicio)
P8: ESP (IP/Servicio)
P9: ESP (IP/Servicio)
KA
KB
KC
UDP (IP/Mensaje de clave)
P4: ESP (IP/Servicio)
P5: ESP (IP/Servicio)
P6: ESP (IP/Servicio)
K7
K8
K9
UDP (IP/Mensaje de clave)
Receptor/manejo de paquete de ráfaga
Salida normal
Salida de prioridad
P1: ESP (IP/Servicio)
P2: ESP (IP/Servicio)
P3: ESP (IP/Servicio)
K4
K5
K6
UDP (IP/Mensaje de clave)
Pila de IP
IPSec
Cliente
Gestor de clave
K-0
K-1
K-2
DESENCRIPTACIÓN DE CLAVES
K3
K2
K1

FIG. 25

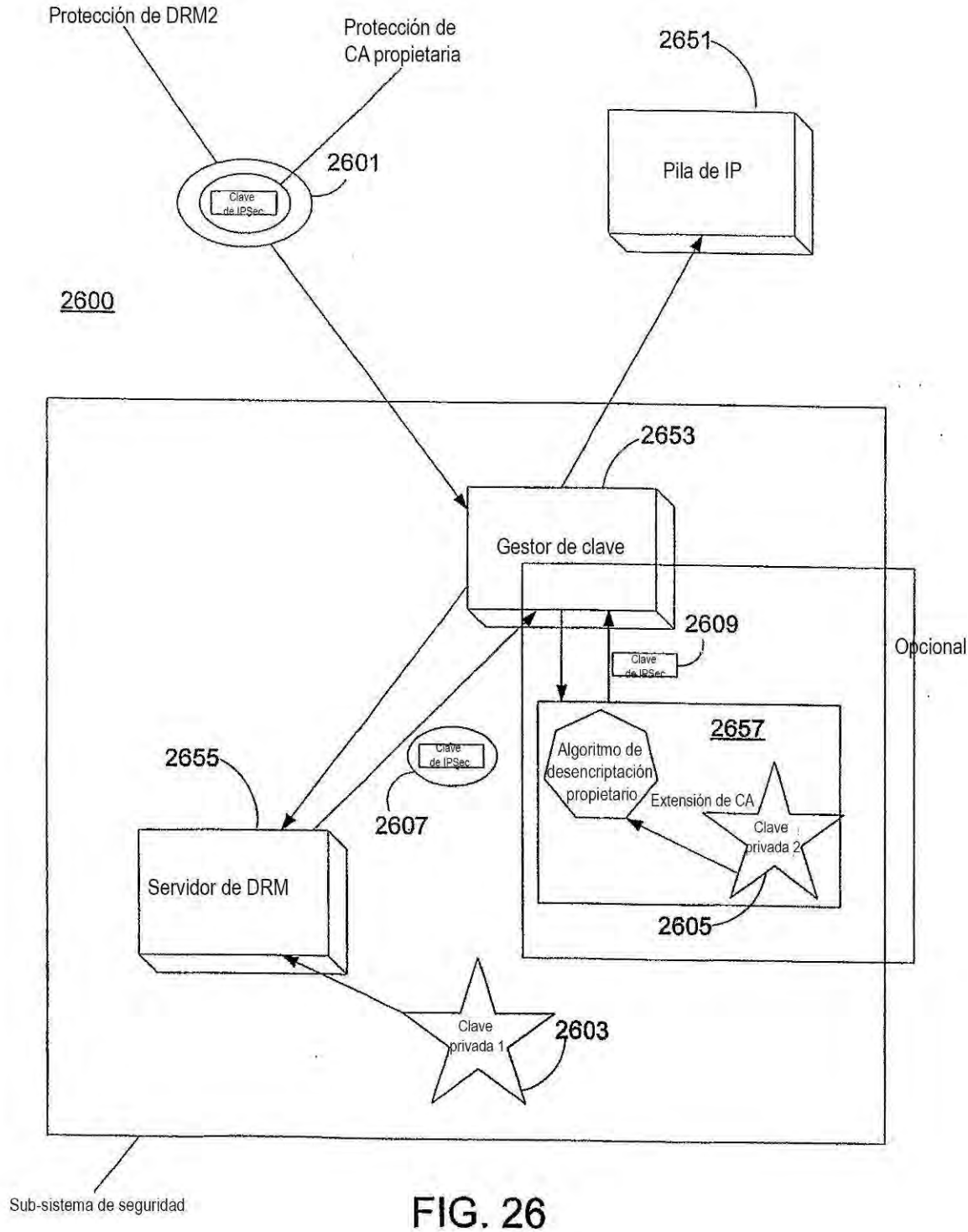
Protección de DRM2
Protección de CA propietaria
2651
2601
Clave de IPSec
Pila de IP
2600
2653
Gestor de clave
2609
Opcional
Clave de IPSec
2657
Algoritmo de desencriptación propietario
Extensión de CA
Clave privada 2
2655
Clave de IPSec
2607
Servidor de DRM
2605
Clave privada 1
2603
Sub-sistema de seguridad

FIG. 26

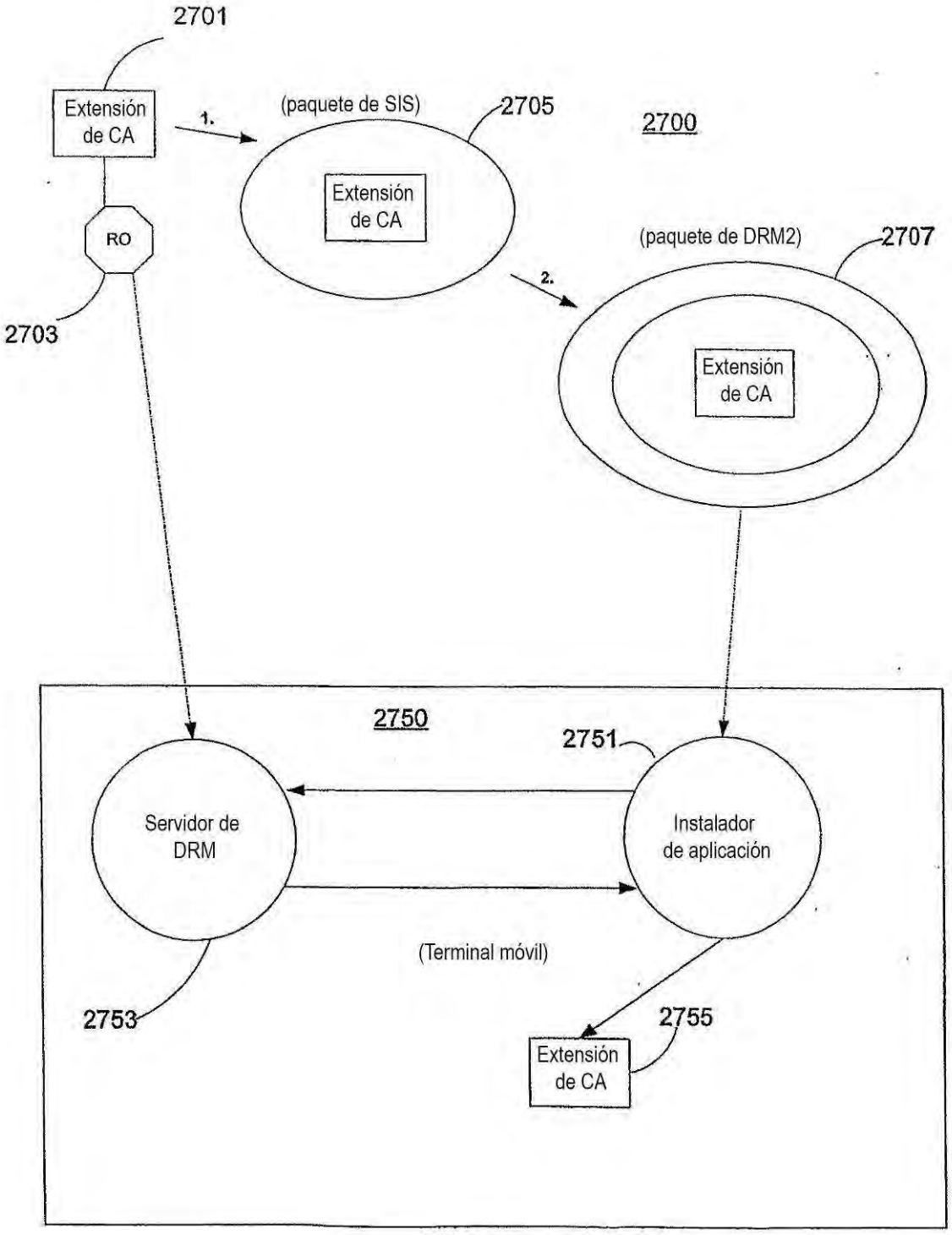
2701
Extensión de CA
1.
(paquete de SIS)
2705
2700
Extensión de CA
RO
2703
(paquete de DRM2)
2707
2.
Extensión de CA
2750
2751
Servidor de DRM
Instalador de aplicación
(Terminal móvil)
2753
2755
Extensión de CA

FIG. 27

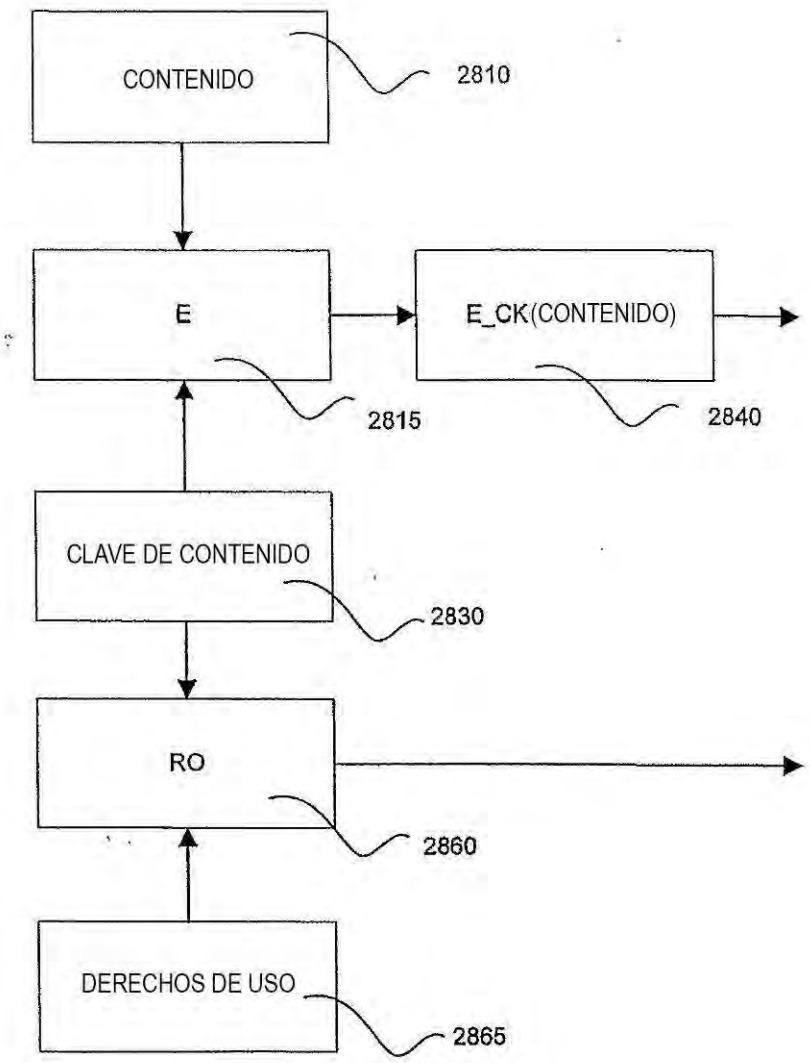
CONTENIDO
2810
E
E_CK(CONTENIDO)
2815
2840
CLAVE DE CONTENIDO
2830
RO
2860
DERECHOS DE USO
2865

FIG. 28

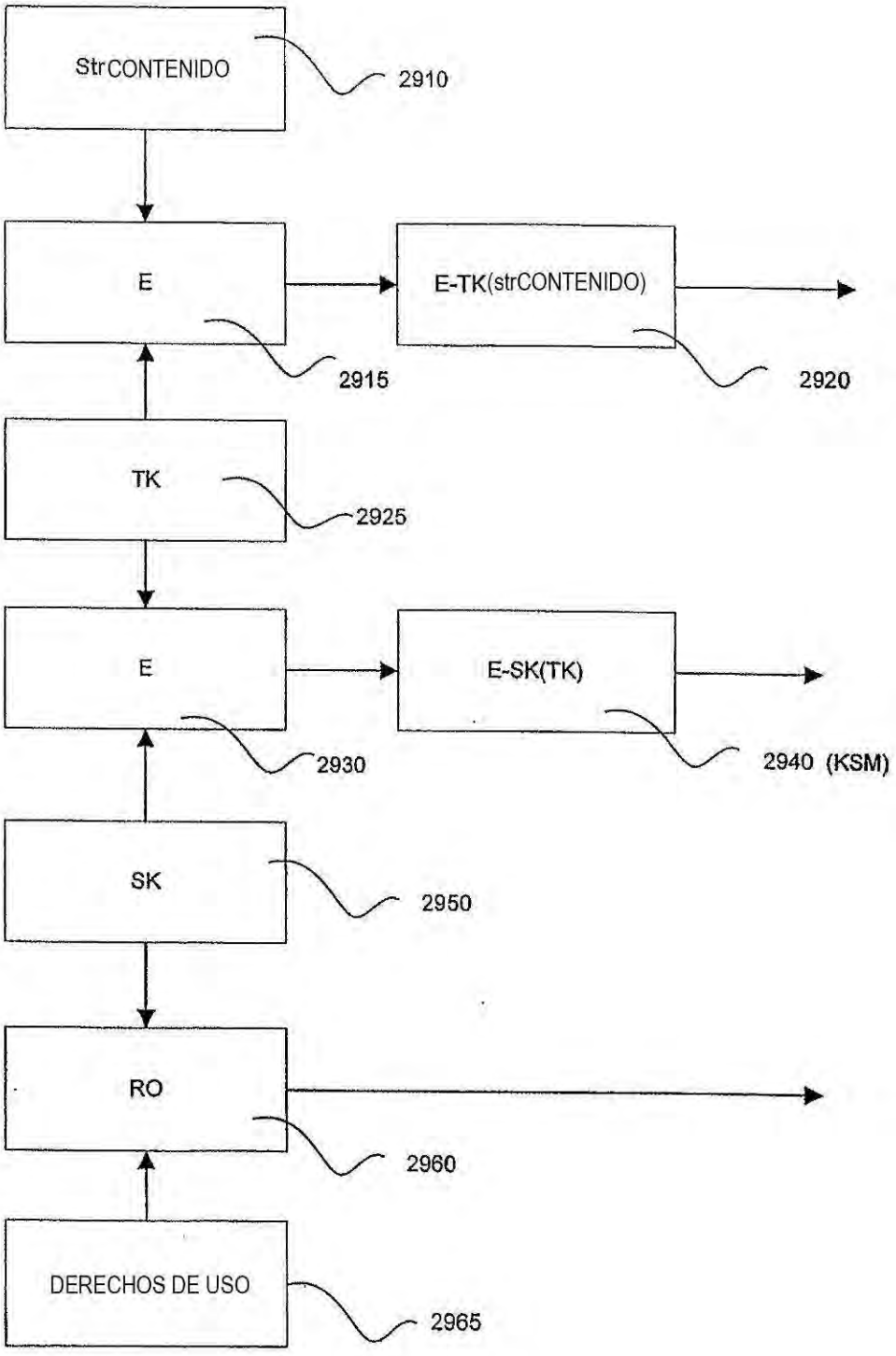
StrCONTENIDO
2910
E
E-TK(strCONTENIDO)
2915
2920
TK
2925
E
E-SK(TK)
2930
2940 (KSM)
SK
2950
RO
2960
DERECHOS DE USO
2965

FIG. 29

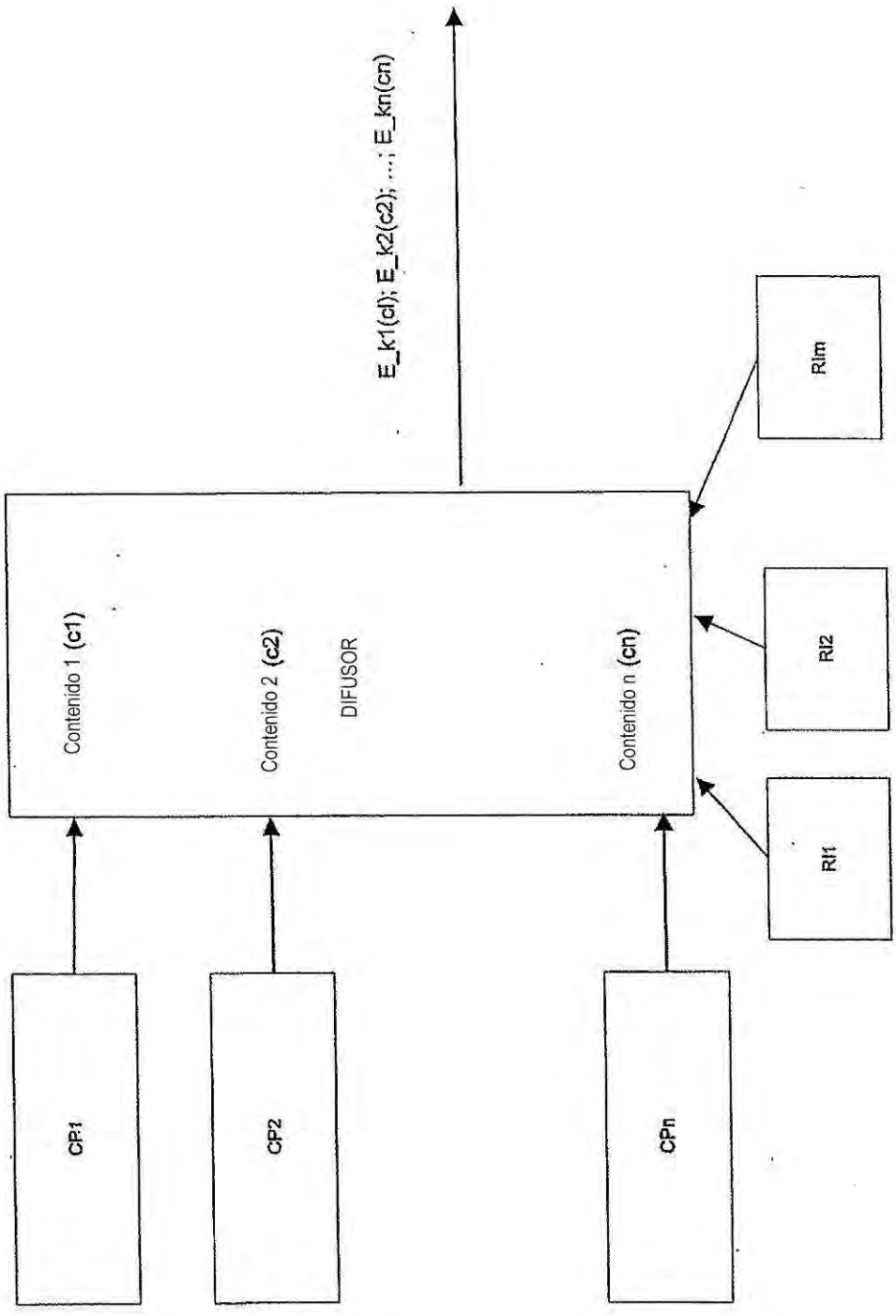
E_k1(c1); E_k2(c2); ...; E_kn(cn)
Rim
Ri2
Ri1
Contenido 1 (c1)
Contenido 2 (c2)
DIFUSOR
Contenido n (cn)
CP1
CP2
CPn

FIG. 30

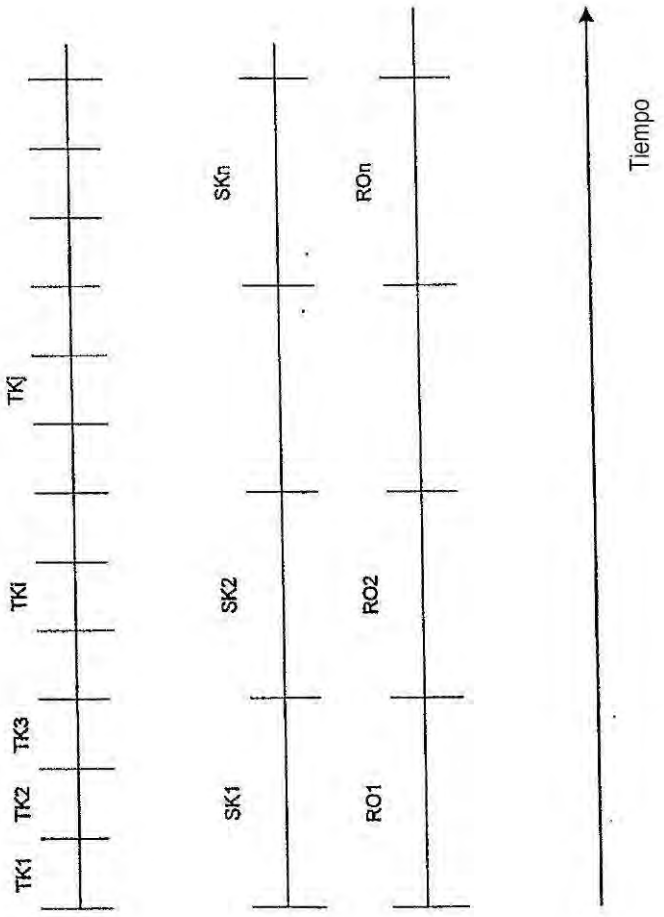

FIG. 31

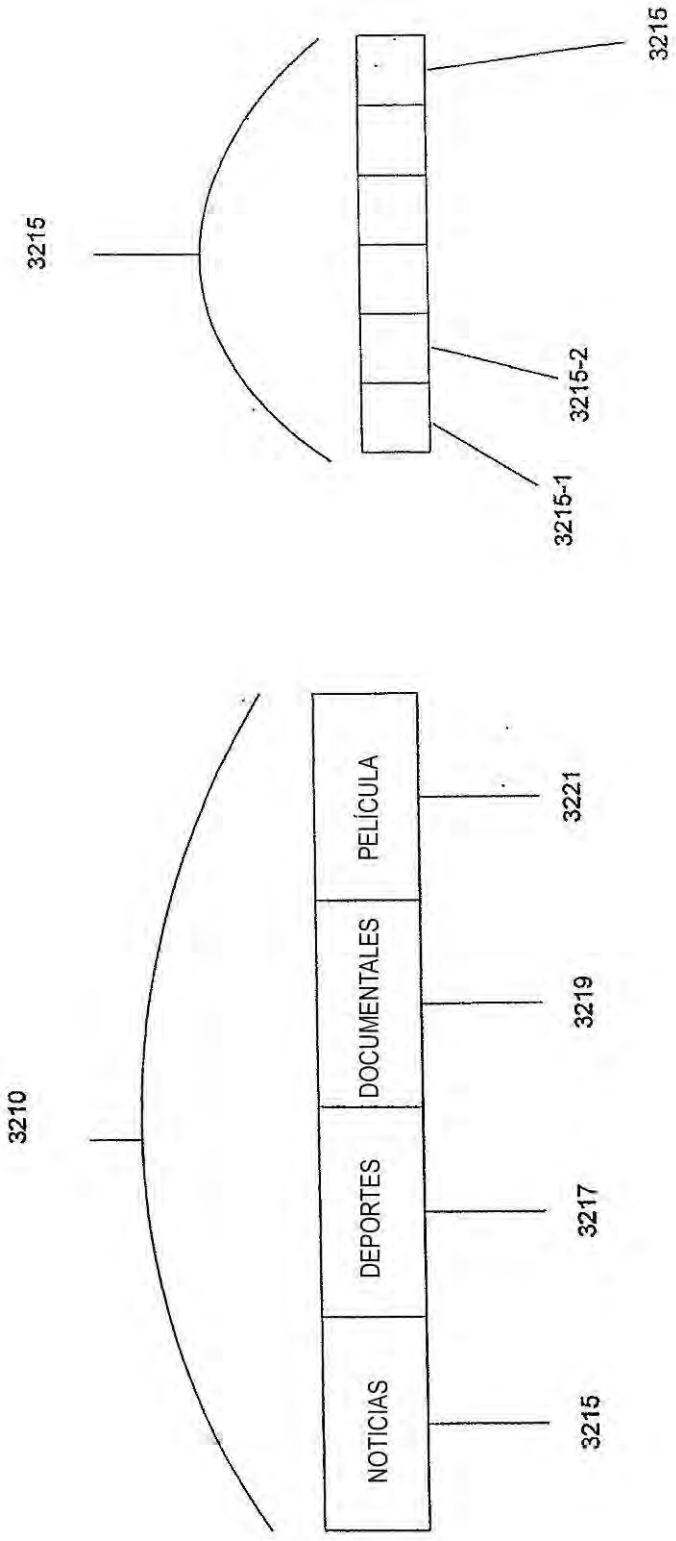
3210
NOTICIAS
DEPORTES
DOCUMENTALES
PELÍCULA
3215
3217
3219
3221
3215
3215-1
3215-2
3215

FIG. 32

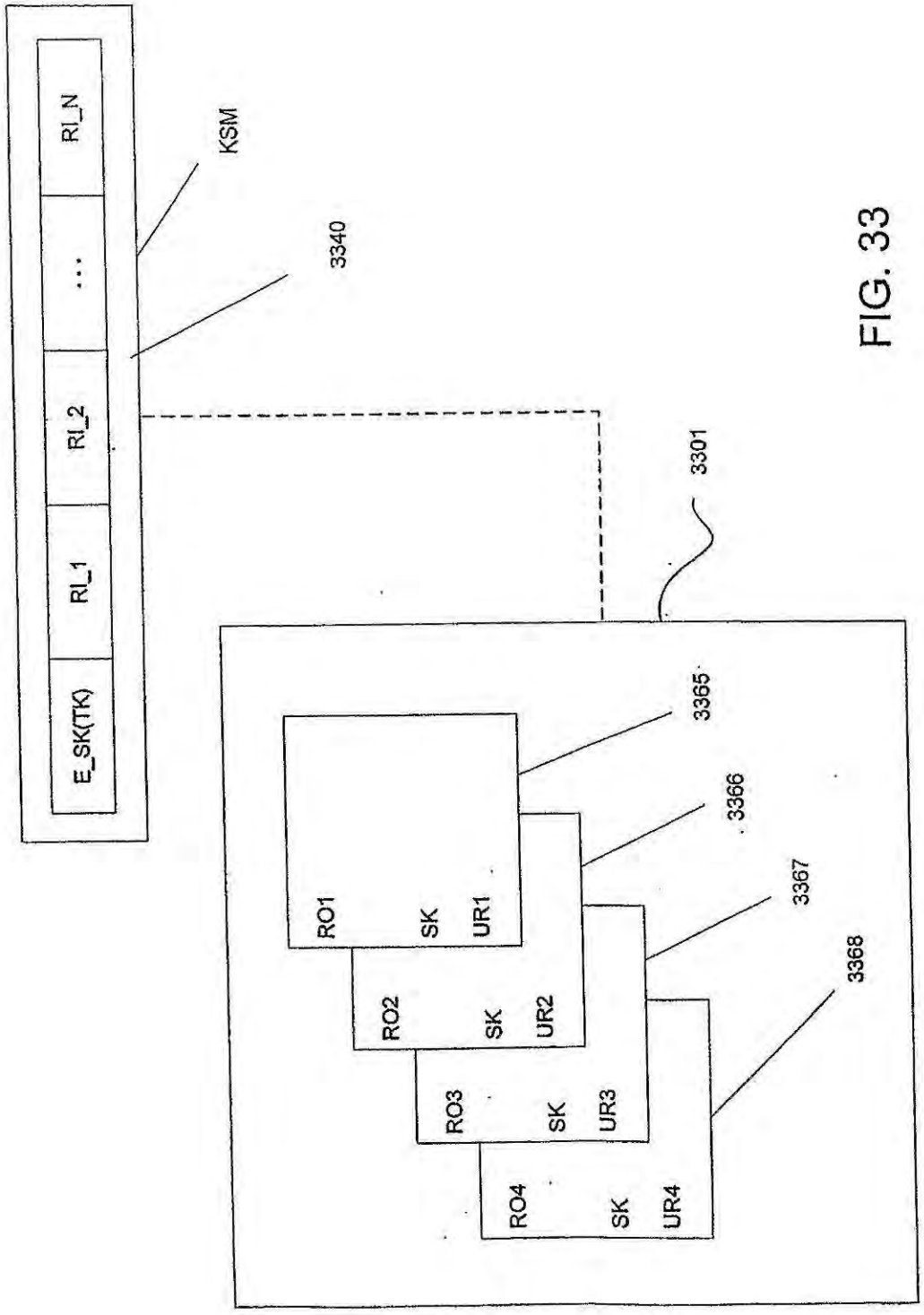
E_SK(TK)
RL_1
RL_2
...
RL_N
KSM
3340
3301
3365
3366
3367
3368
RO1
SK
UR1
RO2
SK
UR2
RO3
SK
UR3
RO4
SK
UR4

FIG. 33