(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 287 486**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03734739 .0**
(86) Fecha de presentación : **28.01.2003**
(87) Número de publicación de la solicitud: **1470690**
(87) Fecha de publicación de la solicitud: **27.10.2004**

(54) Título: **Procedimiento y dispositivo de transmisión de mensajes de gestión de titularidad.**

(30) Prioridad: **31.01.2002 FR 02 01146**

(45) Fecha de publicación de la mención BOPI:
16.12.2007

(45) Fecha de la publicación del folleto de la patente:
16.12.2007

(73) Titular/es: **VIACCESS**
Les Collines de l'Arche - Tour Opéra C
92057 Paris La Defense, FR

(72) Inventor/es: **Bons, Pascal y**
Hamou, Bernard

(74) Agente: **Justo Vázquez, Jorge Miguel de**

DESCRIPCIÓN

Procedimiento y dispositivo de transmisión de mensajes de gestión de titularidad.

Campo técnico

La invención se refiere al campo de las transmisiones de datos y/o de servicios codificados hacia una pluralidad de terminales unidas a una red de intercambio de datos y se refiere más particularmente a un procedimiento de transmisión de mensajes de gestión de titularidad (EMM) de estos datos y de estos servicios así como a un dispositivo para poner en práctica el procedimiento.

Estado de la técnica anterior

Con el desarrollo de los intercambios de datos a través de redes abiertas tales como la red Internet, la protección de los intercambios tiene una importancia creciente en las actividades de los operadores y de los proveedores de servicios. Esta protección tiene como fines principales:

- evitar que las transacciones realizadas a través de la red sean interceptadas;
- asegurar la integridad de los datos, es decir, determinar si los datos transmitidos han sido alterados durante la comunicación;
- permitir la autentificación, es decir, asegurar la identidad de los interlocutores de una transacción y la confidencialidad, que consiste en hacer la información incomprensible para personas distintas a las que realizan la transacción.

La autentificación se realiza mediante el control de acceso que solamente permite el acceso a los recursos a las personas autorizadas.

En el campo de la difusión de programas audiovisuales encriptados, el protocolo DVB define un algoritmo común de codificación (por Common Scrambling Algorithm), pero no prevé nada en lo que se refiere al control de acceso, dejando a los operadores y a los proveedores de servicios la libertad de definir sus propios sistemas.

Sin embargo, el protocolo DVB prevé el transporte de datos de control de acceso que se recuperan en la recepción por medio de desencriptadores de datos en una tabla de control de acceso (CAT, por Conditional Access Table) insertada en el multiplexor de transporte MPEG y por medio de otros paquetes de datos privados indicados por medio de desencriptadores de datos en una tabla de programa (PMT, por Program Map Table) que contiene números de identificación PID (por Packet Identifier) de cada componente de programa codificado en forma de conjunto elemental de PES (por Packetized Elementary Stream) de MPEG.

Generalmente, las informaciones necesarias para la decodificación se transmiten en mensajes de control de acceso específicos llamados mensajes de acceso condicional CAM (por Conditional Access Messages), que comprenden al menos un mensaje de control de la titularidad ECM (Entitlement Control Message) y un mensaje de gestión de la titularidad EMM (por Entitlement Management Message).

Estos mensajes de acceso condicional se generan a partir de al menos tres datos de entrada:

- una palabra de control CW (por Control Word) para inicializar la secuencia de decodificación,
- una clave de servicio (Service Key) utilizada para cifrar la palabra de control para un grupo de uno o varios usuarios;
- una clave de usuario (User Key) utilizada para cifrar la clave de servicio.

Los ECM están en función de la palabra de control y de la clave de servicio mientras que los EMM están en función de la clave de servicio y de la clave de usuario.

Los ECM y los EMM se transmiten periódica y permanentemente a los terminales para garantizar su recepción por los usuarios.

En la recepción, el principio de descifrado consiste en recuperar la clave de servicio a partir de los EMM y la clave de usuario contenida en un procesador de seguridad, por ejemplo una tarjeta con chip. La clave de servicio se utiliza a continuación para descifrar los ECM para recuperar la palabra de control, lo que permite iniciar el sistema de decodificación.

En los sistemas de control de acceso conocidos, la transmisión de los EMM se realiza de forma secuencial, sin prioridad ni programación independientemente de las funciones específicas de cada mensaje EMM transmitido. Ahora bien, los diferentes EMM no se refieren necesariamente a los mismos datos ni a los mismos servicios y por consiguiente no se someten a las mismas restricciones de transmisión. En efecto, los EMM pueden repartirse en tres grandes familias que se diferencian por sus respectivas funciones y por sus condiciones de transmisión. Como ejemplo pueden mencionarse:

- mensajes unidos a un contrato anterior entre el abonado y el operador, tal como por ejemplo un abono a un servicio durante un periodo determinado. En este caso, los mensajes EMM se transmiten permanentemente durante el periodo del abono. Esta transmisión representa un flujo de datos muy importante que sin embargo debe mantenerse para asegurar su recepción por el abonado.

- mensajes denominados dinámicos que corresponden a una necesidad inmediata de un abonado tal como por ejemplo la compra de una sesión o de un acontecimiento.

- mensajes de gestión técnica del procesador de seguridad decidida por el operador de acuerdo con el abonado.

La transmisión secuencial, sin prioridad ni programación de estos mensajes EMM genera un tiempo de ciclo importante, que varía de un sitio a otro y que provoca un tiempo de espera importante por parte del abonado. Además, la mezcla de mensajes que tienen caracteres y grados de prioridad diferentes conduce a una ocupación no optimizada de la banda de paso.

El objeto de la invención el paliar los inconvenientes descritos anteriormente.

El documento EP-A-1 111 923 describe un método de gestión de un sistema de control de acceso condicional que tiene una pluralidad de abonados equipado cada uno con un terminal provisto de un módulo de acceso condicional y de un circuido protegido para almacenar las titularidades, cada terminal recibe un ECM que comprende una primera clave CW cifrada con una clave de servicio P_T, cada circuito protegido recibe un mensaje EMM que comprende al menos la clave de servicio P_T necesaria para el descifrado de la CW.

Este método tiene por objeto rastrear un circuito protegido utilizado fraudulentamente enviando a los terminales diferentes claves para obtener las primeras claves CW y observando las informaciones de una clave suministrada por un pirata. A tal efecto, se envían mensajes EMM de búsqueda a una parte de los terminales. Estos mensajes comprenden al menos la clave P_T y una clave artificial (P_{D1} o P_{D2}) e identificadores de dichas claves P_T y P_{D1} o P_{D2}. De acuerdo con este método, se transmiten los primeros mensajes EMM que comprenden P_T y P_{D1} a una primera parte de los terminales y se transmiten los segundos mensajes EMM que comprenden P_T y P_{D2} a una segunda parte de los terminales, a continuación se transmite un mensaje ECM que identifica la clave P_T que debe utilizarse para desencriptar CW, a todos los terminales inmediatamente antes de que se solicite dicha clave CW para descifrar el contenido.

De este modo, el pirata está obligado a hacer públicas todas las claves, comprendidas entre P_{D1} y P_{D2}, mucho antes de que se solicite la clave CW. Esto permite rastrear al pirata que distribuye P_{D1} y P_{D2}.

El documento EP 0 866 615 A2 describe un aparato para transmitir a terminales datos numéricos multiplexados en forma codificada en las que los datos de descifrado propios de cada terminal y los datos de descifrado comunes a las diferentes terminales se transmiten con dichos datos codificados.

Exposición de la invención

La invención propone un procedimiento de transmisión de mensajes de gestión de titularidad (EMM) de datos y/o servicios suministrados a una pluralidad de terminales de una red de intercambio de datos, caracterizado porque comprende las siguientes etapas:

En la emisión:

- definir un conjunto de tipos de mensajes EMM en función de al menos un criterio representativo del tipo de datos y/o servicios suministrados;

- definir una pluralidad de tipos de vías lógicas de transmisión y asociar a cada tipo de vía al menos un parámetro (STREAM_TYPE) para indicar a los terminales los tipos de EMM que pasan por cada una de las vías lógicas descritas;

- asignar a cada tipo de mensaje EMM al menos una vía entre las vías lógicas de transmisión definidas

- transmitir el parámetro (STREAM_TYPE) y dichas vías lógicas a cada terminal;

- multiplexar las vías lógicas de transmisión en un mismo flujo de datos;

- transmitir dicho flujo de datos a los terminales;

y en la recepción:

- cada terminal filtra los EMM entrantes en función del parámetro (STREAM_TYPE) y de al menos un parámetro de estado que depende del funcionamiento actual del terminal.

Preferiblemente, el parámetro (STREAM_TYPE) se transmite a cada terminal en una estructura de datos dinámica que representa una vía lógica de control.

De acuerdo con una realización preferida, la estructura dinámica se transmite en un EMM cifrado y tiene al menos uno de los siguientes campos:

- un primer campo (EMM_XID) para permitir al terminal identificar la vía lógica descrita por la estructura;

- un segundo campo (Version_Number) para indicar al terminal una evolución de los datos y/o una evolución de la estructura dinámica que corresponde a la transmisión de dichos nuevos datos por la vía descrita de modo que el terminal adapte su filtrado para recuperar dichos nuevos datos;

- un tercer campo (Listen_Time) para indicar al terminal un periodo de escucha de la vía descrita.

Dicho tercer campo (Listen_Time) representa un periodo mínimo fijo o un periodo mínimo variable, suficiente para permitir que el terminal recupere los mensajes transmitidos.

En una variante de realización, los tipos de vías lógicas definidos comprenden al menos:

- una vía RÁPIDA para transmitir mensajes EMM destinados a terminales que han solicitado expresamente estos mensajes.

- una vía DEDICADA para transmitir mensajes EMM que tienen objetivos funcionales iguales;

- una vía NORMAL para transmitir mensajes EMM cuyo contenido no es previsible y que pueden estar diferidos en el tiempo.

- una vía DIFERIDA para transmitir a los terminales mensajes EMM no urgentes y de diversos objetivos funcionales;

- una vía de DESVÍO para retransmitir a los terminales mensajes que ya se hayan transmitido por una vía diferente de la DEDICADA.

Preferiblemente, para las vías RÁPIDA, NORMAL, DIFERIDA y DEDICADA el periodo mínimo variable se estima en función de la cadencia de repetición de los envíos de mensajes EMM.

En un ejemplo de aplicación del procedimiento de acuerdo con la invención, los datos y/o servicios suministrados a los terminales representan programas multimedia.

En otro ejemplo de aplicación, los datos y/o servicios suministrados a los terminales representan programas audiovisuales.

En los dos tipos de aplicación los mensajes EMM se encapsulan en formato MPEG y se transmiten en modo difuso o en modo conectado. Además del contenido del EMM, las secciones MPEG obtenidas tienen también al menos las siguientes informaciones privadas:

- EMM_XID que representa el identificador del EMM;

- LG_EMM que representa la longitud del EMM.

El procedimiento de acuerdo con la invención se pone en práctica con un dispositivo que tiene:

- medios para definir un conjunto de tipos de mensajes EMM en función de al menos un criterio representativo del tipo de datos y/o servicios suministrados;

- medios para definir un conjunto de tipos de vías lógicas de transmisión en función del contenido a transmitir en cada vía;

- medios para asignar a cada tipo de mensaje EMM una vía lógica de transmisión;

- medios para multiplexar las vías lógicas de transmisión en un mismo flujo de datos;

- medios para transmitir dicho flujo de datos a los terminales, y

- medios para filtrar, a nivel de un terminal, los EMM entrantes en función de los tipos de vías definidos.

En la realización preferida de la invención, el dispositivo comprende:

- medios para asociar a cada tipo de vías al menos un parámetro (STREAM_TYPE) para indicar a los terminales los tipos de EMM que pasan por cada una de las vías lógicas descritas;

- medios para transmitir el parámetro (STREAM_TYPE) a cada terminal;

- medios para permitir a cada terminal filtrar los EMM entrantes en función del parámetro (STREAM_TYPE) y de al menos un parámetro de estado que refleje el actual funcionamiento del terminal.

Breve descripción de los dibujos

Otras características y ventajas de la invención resultarán de la siguiente descripción, tomada como ejemplo no limitante, en referencia a las figuras adjuntas en las que:

- la figura 1 ilustra esquemáticamente un sistema en el que se utiliza un dispositivo de transmisión de mensajes de gestión de titularidad (EMM) de acuerdo con la invención;

- la figura 2 representa un esquema del funcionamiento del dispositivo de acuerdo con la invención;

- la figura 3 representa esquemáticamente un modo de comunicación entre un generador de mensajes EMM y un Multiplexor de acuerdo con una realización preferida de la invención.

- la figura 4 ilustra esquemáticamente la encapsulación de EMM en la sección MPEG de acuerdo con un ejemplo de puesta en práctica de la invención.

Exposición detallada de realizaciones particulares

La siguiente descripción se refiere a una aplicación particular del procedimiento de acuerdo con la invención en un sistema de distribución de programas audiovisuales a una pluralidad de terminales de abonados unidos a una red de intercambio de datos, tal como por ejemplo la red Internet o a una red privada de difusión de programas.

Este sistema permite a un primer conjunto 2 de equipos de gestión de abonados SMS, dispuestos por ejemplo en un operador comercial, comunicarse, mediante un segundo conjunto de equipos 6 de gestión de la titularidad de los abonados, con un tercer conjunto 4 de transmisión de la titularidad (EMM).

Cada abonado dispone de un decodificador 8 y de un procesador de seguridad en el que se inscribe la titularidad.

El tercer conjunto 4 tiene un primer módulo 10 denominado en la descripción a continuación B-SAS (por Broadcast Subscription Autorisation System) que permite asegurar la organización y la difusión de los EMM de acuerdo con las directrices procedentes de los equipos del primer conjunto 2. El primer módulo B-SAS comunica, por un lado, con equipos del conjunto 6 y por otro lado con un segundo módulo MUX 12 de multiplexado unido a un tercer módulo 14 de difusión de los EMM hacia el decodificador 8.

El conjunto 6 de equipos de gestión de la titularidad de los abonados tiene un primer equipo SAS 16 que asegura la gestión técnica de los procesadores de seguridad y de la titularidad y un segundo equipo STB-MS 18 que asegura la gestión de los terminales de los abonados.

La función del primer equipo SAS 16 es expresar las solicitudes de servicios procedentes de los SMS 2 de los diferentes operadores en mensajes EMM aprovechables por el procesador de seguridad o el terminal y transmitirlas al módulo B-SAS 10 para la transmisión en modo difuso hacia los terminales de los abonados o a un módulo I-SAS 17 para distribuir estos EMM en modo conectado. El primer equipo SAS 16 permite además realizar cerca del módulo B-SAS 10, solicitudes de adición, de envío y de sustitución de EMM destinados a los terminales y solicitudes de supresión de envío de EMM.

El segundo equipo STB-MS 18 permite también a los equipos SMS 2, definir y mantener las características de los terminales de los abonados.

El segundo equipo STB-MS 18 permite también realizar, cerca del módulo B-SAS 10, solicitudes de adición, de envío y de sustitución de EMM destinados a los terminales y solicitudes de supresión de envío de EMM. Este equipo STB-MS es adecuado para expresar las solicitudes de servicios procedentes de los SMS 2 de los diferentes operadores en mensajes aprovechables por el procesador de seguridad o el terminal y para transmitirlas al módulo I-SAS 17 para distribuir estos EMM en modo conectado.

El decodificador 8 situado en casa del abonado contiene el procesador de seguridad en el que se registra la titularidad de los abonados y cuya función es, de forma conocida, tratar los mensajes EMM contenidos en el flujo difuso, gestionar una interfaz IHM Hombre-Máquina presentada al abonado y comunicarse con el procesador de seguridad del abonado y con el servidor de un operador técnico.

La figura 2 representa un esquema de funcionamiento detallado del módulo B-SAS 10. Éste último tiene un primer bloque 20 para recoger mensajes procedentes del o de los primeros equipos SAS 16 o segundos equipos STB-MS 18, un segundo bloque 22 para gestionar las colas de espera, un tercer bloque 24 para gestionar la difusión de los EMM un cuarto bloque 26, controlado por un administrador, para definir las informaciones de configuración del sistema y un quinto bloque 28 de supervisión para recoger informaciones técnicas y aplicables en el sistema.

Los mensajes recogidos por el primer bloque 20 pueden ser solicitudes de envío de EMM, de sustitución o de supresión de EMM por medio de un protocolo de aplicación tal como TCP-IP, CORBA, HTTP+XML, RMI o un protocolo propio.

Definición de EMM

El dispositivo y el procedimiento de la invención permiten definir un conjunto de tipos de mensajes EMM en función de al menos un criterio representativo del tipo de datos y/o de servicios suministrados. A tal efecto, los equipos SAS 16 y STB 18 cadena arriba, solicitan la inserción de un EMM en un ciclo, especificando los modos de difusión (Referencia del modelo de transmisión, Fecha de inicio y de fin de la difusión del EMM) y la descripción del EMM (estructura de la cabecera, tamaño de la cabecera, contenido del EMM).

Previamente a la difusión de los EMM, se define una pluralidad de tipos de vías lógicas de transmisión con un parámetro (STREAM_TYPE) para indicar a los terminales los tipos de EMM que pasan por cada una de las vías lógicas descritas. Este parámetro (STREAM_TYPE) se transmite a cada terminal en forma de estructura de datos dinámica que representa una vía lógica de control que tiene al menos uno de los siguientes campos:

- un primer campo (EMM_XID) para permitir al terminal identificar la vía lógica descrita por la estructura;
- un segundo campo (Version_Number) para indicar al terminal una evolución de la estructura dinámica. Esta evolución señala al terminal la transmisión de nuevos datos por la vía descrita de modo que éste último adapte su filtrado para recuperar estos nuevos datos;
- un tercer campo (Listen_Time) para indicar al terminal un periodo de escucha de la vía descrita.

Una vía lógica es una sub-parte de un flujo identificado con un PID en la señal difusa. La definición de dichas vías lógicas permite multiplexarlas en un mismo flujo en el que los EMM que pasan por una misma vía tienen el mismo identificador EMM_XID. De este modo, en la recepción, el terminal puede filtrar los EMM entrantes en un flujo seleccionando solamente los EMM de una o de varias vías particulares. Para hacer esto, el terminal filtra los EMM entrantes colocando una máscara en la cabecera del flujo de datos.

En una realización particular, el tamaño del identificador EMM_XID es de 8 bits, lo que permite multiplexar hasta 8 vías de EMM en un flujo asignando un bit a cada vía.

Para asignar a cada tipo de mensaje EMM al menos una vía entre las vías lógicas de transmisión definidas, el módulo B-SAS 10 dispone de características técnicas unidas a los modelos de transmisión que le permiten de este modo determinar la vía de difusión de un EMM. Los desplazamientos temporales entre la fecha de inicio y la fecha de finalización de la difusión los determina cada modelo. Las vías lógicas definidas se multiplexan en un mismo flujo de datos y después se transmiten a los terminales.

Adición de EMM

Durante la solicitud de adición de un EMM, el módulo B-SAS 10 realiza los siguientes tratamientos:

Análisis sintáctico de la petición,

Verificación de la existencia del modelo de transmisión,

Verificación de la coherencia de las fechas de difusión,

Verificación de la validez del identificador del EMM,

Actualización de la base de datos,

Orientación del EMM hacia el bloque 22 de gestión de las colas de espera,

Gestión de errores (sobrecarga del equipo, ...),

Confirmación de la recepción de la solicitud.

Sustitución de EMM

Los equipos SAS 16 o STB-MS cadena arriba, pueden solicitar la sustitución de un EMM en un ciclo especificando el identificador del EMM a sustituir. Este mensaje lo utilizará, por ejemplo, el primer equipo SAS 16 para aumentar la población prevista por un EMM en el marco de una inscripción a una oferta comercial.

Durante la solicitud de una sustitución de EMM, el módulo B-SAS 10 realiza los siguientes tratamientos:

Análisis sintáctico de la petición;

verificación de la existencia del modelo de transmisión;

Verificación de la coherencia de las fechas de difusión;

Verificación de la validez del identificador del EMM a sustituir;

Verificación de la validez del identificador del nuevo EMM;

Actualización de la base de datos;

Orientación del EMM hacia el bloque 22 de gestión de las colas de espera;

Gestión de errores (sobrecarga del equipo ...);

Confirmación de la recepción de la solicitud.

Supresión de EMM

Durante la solicitud de una supresión de EMM, el módulo B-SAS 10 realiza los siguientes tratamientos:

Análisis sintáctico de la petición;

Verificación de la validez del identificador del EMM;

Actualización de la base de datos;

Supresión de la difusión del EMM en la vía asociada;

Gestión de errores;

Confirmación de la recepción de la solicitud.

Nótese que, incluso aunque únicamente el módulo B-SAS 10 gestiona la supresión de EMM al finalizar el periodo de validez, los equipos SAS 16 o STB-Ms 18 puede suprimir explícitamente la difusión de un EMM.

Gestión de las colas de espera

El módulo B-SAS 10 debe permitir cumplir las restricciones, particularmente las de los terminales y al mismo tiempo, las de ofrecer una calidad de servicio regular. A tal efecto, el segundo bloque 22 permite:

organizar los EMM difusos para permitir que el terminal los valide;

controlar el ancho de banda de las vías EMM en un transpondedor. Generalmente este ancho de banda es del orden de 50 a 500 kbits/segundo.

programar la difusión de ciertos EMM expresada en periodos de tiempo muy cortos;

programar la difusión de ciertos EMM durante un periodo de tiempo lo suficientemente largo para que los traten todos los terminales.

orientar los EMM que no tienen carácter de urgencia, en colas de mensajes con diferentes características y organizar estas filas o vías lógicas de modo que el ancho de banda de EMM sea aceptable para un terminal.

Descripción de los tipos de vía definidos

En una realización preferida de la invención, los tipos de vías lógicas definidos comprenden una vía RÁPIDA, una vía DEDICADA, una vía NORMAL, una vía DIFERIDA y una vía de DESVIO.

La vía RÁPIDA se utiliza en el caso en el que es seguro que el terminal está a la escucha de está vía en el momento de la difusión de un EMM que le concierne. La utilización más habitual es la difusión de titularidades específicas para un servicio interactivo que solicita el terminal a un proveedor de servicio. Esta vía también puede utilizarse para la reclamación de un usuario. Los EMM se repiten en esta vía rápida cierto número de veces, con una temporización entre cada envío, y después se suprime su difusión. Si el número de mensajes en la cola se vuelve demasiado grande, el periodo de tiempo de ciclo de la vía se acerca al límite de la garantía de calidad de servicio.

La vía DEDICADA transmite EMM cuyas características son iguales. Se identifican dos tipos de EMM para formar vías dedicadas: EMM de renovación de titularidad y EMM de cambio de claves.

Cada vía dedicada se regula independientemente de las otras vías, para la organización de la difusión o para respetar el ancho de banda asignado a la vía. Solamente las vías rápidas pueden interrumpir su funcionamiento.

La vía NORMAL está presente obligatoriamente y permite emitir EMM cualesquiera. Esta vía transmite el conjunto de mensajes necesarios para el uso permanente por parte del abonado (gestión del procesador de seguridad, datos privados ...).

Durante el funcionamiento, el terminal escucha este tipo de vía durante el periodo de tiempo especificado en el descriptor de la vía o durante un cambio en el descriptor de la vía. Esta escucha puede ser permanente.

La vía DIFERIDA solamente está presente periódicamente en el flujo. Esta vía permite emitir EMM que pueden aceptar un tratamiento con un desplazamiento temporal tales como EMM de gestión técnica del procesador de seguridad o de información. La lectura de esta vía por el terminal la provocará puntualmente el cambio del número de versión de la vía.

La vía de DESVÍO permite descargar las otras vías lógicas que ya se hayan difundido durante varios ciclos y que ya hayan sido valoradas por el terminal en un gran número de casos. Las modalidades de difusión de EMM se especifican en el modelo de transmisión. El terminal se pondrá a la escucha de esta vía en la puesta en marcha del terminal o en un cambio del número de versión de la vía.

De acuerdo con una realización preferida de puesta en práctica del procedimiento, una vía de control, también llamada vía 0, transmite un EMM cifrado de descripción con destino los terminales, en el que se describen las características técnicas de las vías lógicas que comparten el mismo PID. Este EMM de descripción se genera por el módulo B-SAS 10 en función de los parámetros de configuración y del contenido a transmitir en las vías.

Al recibir el EMM de descripción, cada terminal se coloca en esta vía 0 para recuperar y analizar el descriptor para determinar las vías lógicas que debe escuchar y en que condiciones. Cada terminal calculará los criterios de filtrado en función del resultado del análisis de los descriptores.

Los EMM difundidos deben cumplir las siguientes restricciones:

El periodo de difusión del EMM debe ser válido.

- para un EMM difundido en una vía RÁPIDA no debe alcanzarse la cantidad máxima de difusión;
- para un EMM transmitido en los otros tipos de vía, la fecha de difusión debe estar comprendida entre la fecha de inicio y la fecha de finalización de la difusión especificada.

La programación del envío de los EMM permite al terminal captar el conjunto de EMM del flujo en un mínimo de ciclos.

Para cumplir esta restricción un algoritmo llamado de difusión aleatoria organiza el envío de los EMM programando aleatoriamente los EMM a enviar en un ciclo de difusión.

La temporización entre dos EMM transmitidos por la vía de control (vía 0) debe ser como mínimo de 100 ms.

Gestión de la difusión de los EMM

En el ejemplo de realización descrito, la definición de los recursos de difusión y la gestión de la difusión de los EMM está de acuerdo con el protocolo EMMG/PDG, parte de la normativa ETSI TS 103 197 "Head-End implementation of DVB Simulcrypt". Este protocolo prevé la utilización de "Channel" y de "streams", que designan en la descripción a continuación "canal" y "flujo" respectivamente, para comunicarse con el módulo MUX 12 de multiplexado.

Gestión del "channel" y del "stream"

Como se ilustra esquemáticamente en la figura 3, la comunicación entre un generador 30 de mensajes EMM y el módulo MUX 12 se realiza a través de un canal 34 identificado mediante un identificador client_id que identifica el sistema de acceso condicional y que puede ser particular para cada operador.

El módulo B-SAS 4 establece un "channel" 32 por operador o por grupo de operadores, que permite la creación de uno o varios "streams" 34 identificados por los stream_id (Stream_id 1, Stream_id 2, ...) únicos en el "channel". Un "stream" 34 está compuesto por una vía de comando y por una vía de datos por la que pasan los EMM en paquetes MPEG2 TS. La vía de datos puede estructurarse de acuerdo con los protocolos TCP/IP o UDP/IP en modo difuso.

Cada "streams" 34 da lugar a la creación de un componente 36 del transpondedor identificado con un identificador de paquete PID (por Packet Identifier) a la salida del módulo MUX 12.

De acuerdo con una variante de realización, por defecto, el módulo B-SAS 4 solamente crea un "stream" 34. Se crea un segundo "stream" 34 si el número de vías por operador supera 8 (número máximo de vías multiplexadas en un mismo flujo EMM). El generador 30 de EMM y el módulo de multiplexado MUX 12 negocian la banda de paso, por iniciativa del generador 30, para cada "stream" 34.

Gestión del envío de los EMM

La preparación de los EMM para su difusión hacia el multiplexor 13 se realiza en dos etapas. La primera etapa consiste en la encapsulación de los EMM en la sección MPEG 2, la segunda etapa consiste en componer paquetes de transporte MPEG 2 TS para enviar al(a los) MUX 12.

Las secciones MPEG obtenidas mediante encapsulado tienen al menos las siguientes informaciones privadas:

- EMM_XID que representa el identificador del EMM;
- LG_EMM que representa la longitud del EMM, y
- el contenido del EMM.

Las reglas de encapsulado son las siguientes:

Un y solamente un EMM por sección,

Una o varias secciones encadenadas por EMM.

El módulo B-SAS 10 compone paquetes MPEG2 TS de tamaño fijo (188 octetos, comprendiendo la cabecera). Por lo tanto, las secciones MPEG2 se encuentran en el interior del paquete o distribuidas entre dos o más de dos paquetes.

Un paquete TS respeta el formato ilustrado esquemáticamente en la figura 4 de acuerdo con la normativa ISO/1EC 13818-1 "Generic coding of moving pictures and associated audio information: Systems". Este paquete tiene un primer campo 40 de sincronización Sync que comprende ocho bits, una cabecera (ent) 42, un puntero "ptr" 44 y un bloque 46 que comprende los datos útiles (DATA);

La cabecera 42 comprende:

- un bit indicador de error de transporte (transport_error_indicator);
- un bit indicador del inicio de una sección en el paquete (payload_unit_start_indicator);
- un bit indicador de la prioridad de transporte (transport priority);
- un bloque de trece bits que representa el identificador PID del paquete;
- dos bits de control de codificación;
- dos bits de control del campo de adaptación;
- dos bits de índice de continuidad.

El bit payload_unit_start_indicator indica si se inicia una sección en el paquete. Si este es el caso, este bit vale 1 y el campo "prt" se reasigna e indica el rango del inicio de la sección en los datos útiles 46.

Si este no es el caso, el bit payload_unit_start_indicator vale cero y el campo "prt" no existe. Este es el caso de una sección en más de dos paquetes o de un paquete rellenado parcialmente.

Intercambios del módulo B_SAS 10 con los otros equipos

Las necesidades de los diferentes clientes que solicitan el equipo se expresan en el módulo BSAS 10 por medio de un suceso disparador que puede ser un mensaje que pasa por las interfaces del equipo emisor/BSAS o las solicitudes provienen por ejemplo de un gerente de explotación.

Necesidades del primer equipo SAS 16

Envío de un EMM

El primer equipo SAS 16 comunica al módulo B_SAS 10 mensajes EMM para difundirlos hacia un decodificador 8. Esta comunicación se realiza mediante una petición en la que el primer equipo SAS 16 específica los modos de difusión del EMM, particularmente el modelo de transmisión a utilizar y las fechas de inicio y de finalización de la transmisión. El módulo B_SAS 10 constituye y organiza el envío de EMM en las vías lógicas especificadas por el modelo de transmisión y en función de las fechas de difusión sobre las que pueden aplicarse desplazamientos temporales.

Sustitución de un EMM

El equipo SAS 16 puede adaptarse para optimizar la difusión de los EMM con destino al módulo B_SAS 10. En este caso, el primer equipo SAS 16 sustituye un EMM en difusión por otro EMM que especifica una población más completa. El primer equipo SAS 16 solicita al módulo B_SAS 10 la sustitución de un EMM por otro en la difusión.

Supresión del envío de un EMM

El primer equipo SAS 16 también puede solicitar al B_SAS 10 la supresión inmediata de un EMM, de la difusión en curso.

Necesidades del segundo equipo STB-MS 18

El STB-MS gestiona el parque de terminales de uno o varios operadores. Como tal, este equipo puede realizar, cerca del B_SAS 10, solicitudes de envío o de sustitución de EMM destinados a los terminales y solicitudes de supresión de envío de EMM.

Envío de un EMM

Los EMM destinados al terminal se suministran al módulo B_SAS 10 mediante un mensaje de la interfaz STB-MS/BSAS. Este mensaje y el tratamiento asociado son iguales a los del primer equipo SAS 16.

Sustitución de un EMM

El equipo STB-MS 18, como el primer equipo SAS 16, puede adaptarse para optimizar la difusión de sus EMM y utiliza a tal efecto el mismo comando que el primer equipo SAS 16. El equipo STB-MS 18 permite también a los equipos SMS 2 definir y mantener las características de los terminales de abonados.

Supresión del envío de un EMM

Igualmente, el segundo equipo STB-MS 18 puede solicitar al módulo B SAS 10 la supresión de un EMM de la difusión en curso.

Necesidades del decodificador

El terminal recibe flujos de EMM emitidos por diferentes módulos B_SAS 10. Estos EMM los suministran los diferentes equipos conectados al módulo B_SAS 10, a saber el o los SAS 16 y el o los STB-MS 18 y se emiten con destino al procesador de seguridad, a uno o varios procesadores de seguridad o a uno o varios terminales.

Recepción del descriptor de vías lógicas

El terminal debe ser capaz de extraer de la señal los mensajes de gestión que le conciernen. Para realizar esta función, el módulo B_SAS 10 transmite en la vía de control, el descriptor y los modos de difusión de las diferentes vías lógicas que constituyen el flujo.

Recepción de los EMM emitidos por el módulo B_SAS 10

El terminal debe ser capaz de extraer de una vía lógica el conjunto de mensajes de gestión que le concierne y en caso necesario reconstituirlos en el caso de EMM divididos en varias secciones. Además, algunos componentes del terminal, tales como desmultiplexores, imponen restricciones de difusión particularmente al número de EMM difundidos por un mismo procesador de seguridad en periodos de tiempo definidos.

El módulo B_SAS 10 valida estas restricciones aplicando un algoritmo de difusión aleatoria de los EMM y cumpliendo las restricciones MPEG de recorte de sección.

REIVINDICACIONES

1. Procedimiento de transmisión de mensajes de gestión de titularidad (EMM) de datos y/o servicios suministrados a una pluralidad de terminales de una red de intercambio de datos, en la cual cada terminal recibe un contenido codificado con una clave CW transmitida en un mensaje de control de acceso ECM y al menos una clave de descifrado de dicha clave CW transmitida en un mensaje de gestión de titularidad EMM, procedimiento **caracterizado** porque comprende las siguientes etapas:

En la emisión:

- definir un conjunto de tipos de mensajes EMM en función de al menos un criterio representativo del tipo de datos y/o servicios suministrados;
- definir una pluralidad de tipos de vías lógicas de transmisión y asociar a cada tipo de vía al menos un parámetro (STREAM_TYPE) para indicar a los terminales los tipos de EMM que pasan por cada una de las vías lógicas descritas;
- asignar a cada tipo de mensaje EMM al menos una vía entre las vías lógicas de transmisión definidas
- transmitir el parámetro (STREAM_TYPE) y dichas vías lógicas a cada terminal;
- multiplexar las vías lógicas de transmisión en un mismo flujo de datos;
- transmitir dicho flujo de datos a los terminales;

y en la recepción:

- cada terminal filtra los EMM entrantes en función del parámetro (STREAM_TYPE) y de al menos un parámetro de estado que depende del funcionamiento actual del terminal.

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado** porque dicho parámetro (STREAM_TYPE) se transmite a cada terminal en una estructura de datos dinámica que representa una vía lógica de control.

3. Procedimiento de acuerdo con la reivindicación 2, **caracterizado** porque dicha estructura de datos dinámica se transmite en un EMM cifrado.

4. Procedimiento de acuerdo con la reivindicación 3, **caracterizado** porque dicha estructura dinámica tiene al menos uno de los siguientes campos:

- un primer campo (EMM_XID) para permitir al terminal identificar la vía lógica descrita por la estructura;
- un segundo campo (Version_Number) para indicar al terminal una evolución de los datos y/o una evolución de la estructura dinámica que corresponde a la transmisión de dichos nuevos datos por la vía descrita de modo que el terminal adapte su filtrado para recuperar dichos nuevos datos;
- un tercer campo (Listen_Time) para indicar al terminal un periodo de escucha de la vía descrita.

5. Procedimiento de acuerdo con la reivindicación 4, **caracterizado** porque dicho tercer campo (Listen_Time) representa un periodo mínimo fijo suficiente para recuperar los mensajes transmitidos.

6. Procedimiento de acuerdo con la reivindicación 4, **caracterizado** porque dicho tercer campo (Listen_Time) representa un periodo mínimo variable en función de la cadencia de repetición de los envíos de mensajes EMM.

7. Procedimiento de acuerdo con una de las reivindicaciones 5 ó 6, **caracterizado** porque los tipos de vías lógicas definidos comprenden al menos:

- una vía RÁPIDA para transmitir mensajes EMM destinados a terminales que han solicitado expresamente estos mensajes;
- una vía DEDICADA para transmitir mensajes EMM que tienen objetivos funcionales iguales;
- una vía NORMAL para transmitir mensajes EMM cuyo contenido no es previsible y que pueden estar diferidos en el tiempo;
- una vía DIFERIDA para transmitir a los terminales mensajes EMM no urgentes y de diversos objetivos funcionales;

- una vía de DESVÍO para retransmitir a los terminales mensajes que ya se hayan transmitido por una vía diferente de la DEDICADA.

8. Procedimiento de acuerdo con las reivindicaciones 6 y 7, **caracterizado** porque para las vías RÁPIDA, NORMAL, DIFERIDA y DEDICADA el periodo mínimo variable se estima en función de la cadencia de repetición de los envíos de mensajes EMM.

9. Procedimiento de acuerdo con una de las reivindicaciones 1 a 8, **caracterizado** porque los datos y/o servicios suministrados a los terminales representan programas multimedia.

10. Procedimiento de acuerdo con la reivindicación 9, **caracterizado** porque los datos y/o servicios suministrados a los terminales representan programas audiovisuales.

11. Procedimiento de acuerdo con una de las reivindicaciones 1 a 10, **caracterizado** porque los mensajes EMM se transmiten en modo difuso.

12. Procedimiento de acuerdo con una de las reivindicaciones 1 a 10, **caracterizado** porque los mensajes EMM se transmiten en modo conectado.

13. Procedimiento de acuerdo con una de las reivindicaciones 11 ó 12, los mensajes EMM se encapsulan en un formato MPEG.

14. Procedimiento de acuerdo con la reivindicación 13, **caracterizado** porque las secciones MPEG obtenidas tienen al menos las siguientes informaciones privadas:

- EMM_XID que representa el identificador del EMM;
- LG_EMM que representa la longitud del EMM, y
- el contenido del EMM.

15. Dispositivo de transmisión de mensajes de control de acceso (EMM) a datos y/o servicios suministrados a una pluralidad de terminales en una red de intercambio de datos, **caracterizado** porque comprende:

- medios (16, 18) para definir un conjunto de tipos de mensajes EMM en función de al menos un criterio representativo del tipo de datos y/o servicios suministrados;
- medios (10) para definir un conjunto de tipos de vías lógicas de transmisión en función del contenido a transmitir en cada vía;
- medios (4) para asignar a cada tipo de mensaje EMM una vía lógica de transmisión y para asociar a cada tipo de vías al menos un parámetro (STREAM_TYPE) para indicar a los terminales los tipos de EMM que pasan por cada una de las vías lógicas descritas;
- medios (12) para multiplexar las vías lógicas de transmisión en un mismo flujo de datos;
- medios para transmitir dicho flujo de datos a los terminales, y
- medios para filtrar, a nivel de un terminal, los EMM entrantes en función de los tipos de vías definidos.

16. Dispositivo de acuerdo con la reivindicación 15, **caracterizado** porque comprende:

- medios (36) para transmitir el parámetro (STREAM_TYPE) a cada terminal;
- medios (22) para permitir a cada terminal filtrar los EMM entrantes en función del parámetro (STREAM_TYPE) y de al menos un parámetro de estado que refleje el actual funcionamiento del terminal.

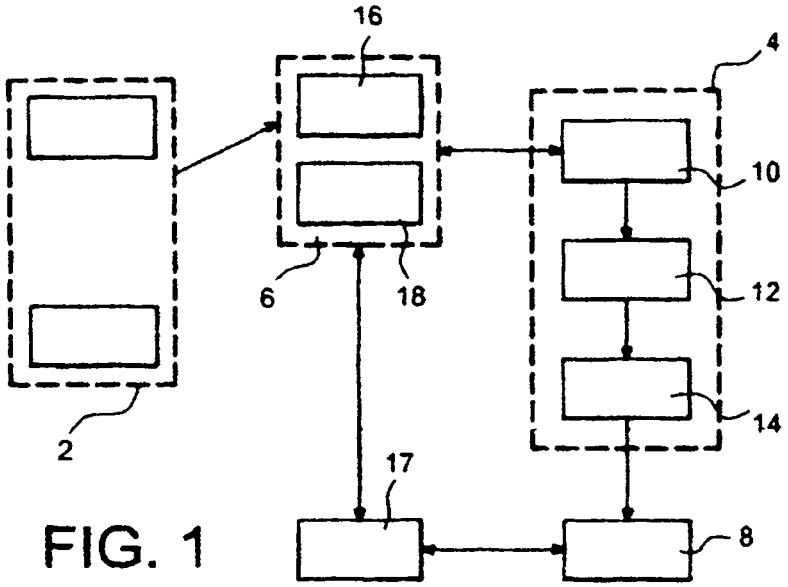
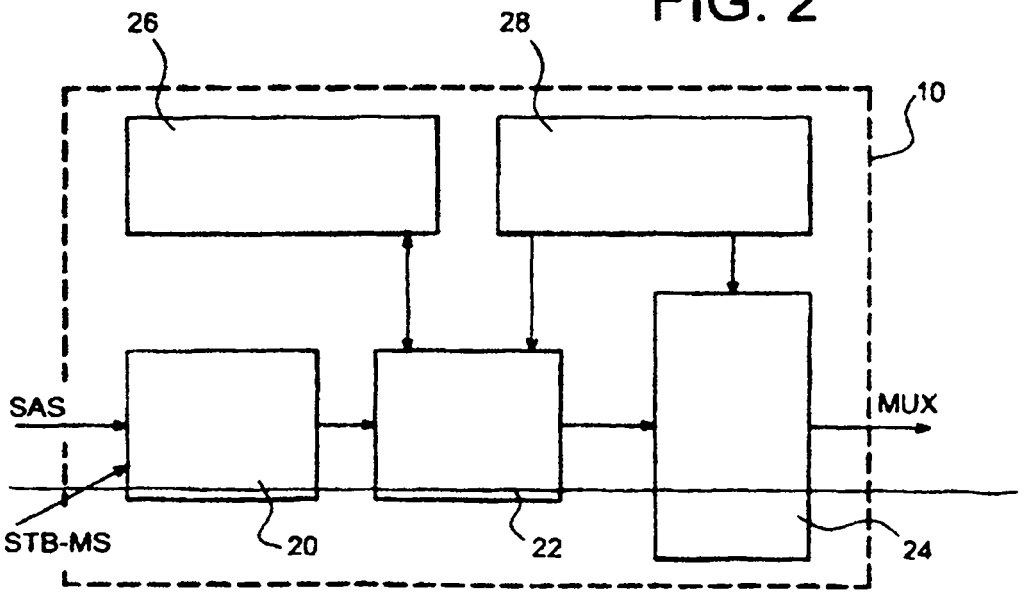


FIG. 1

FIG. 2



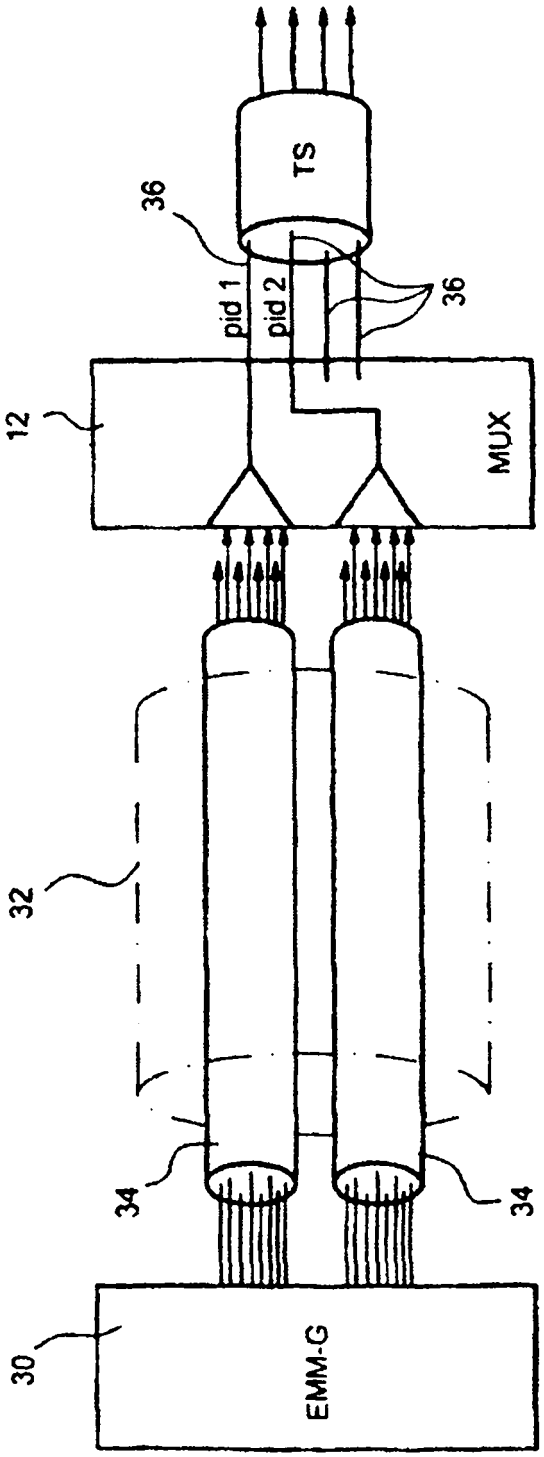


FIG. 3

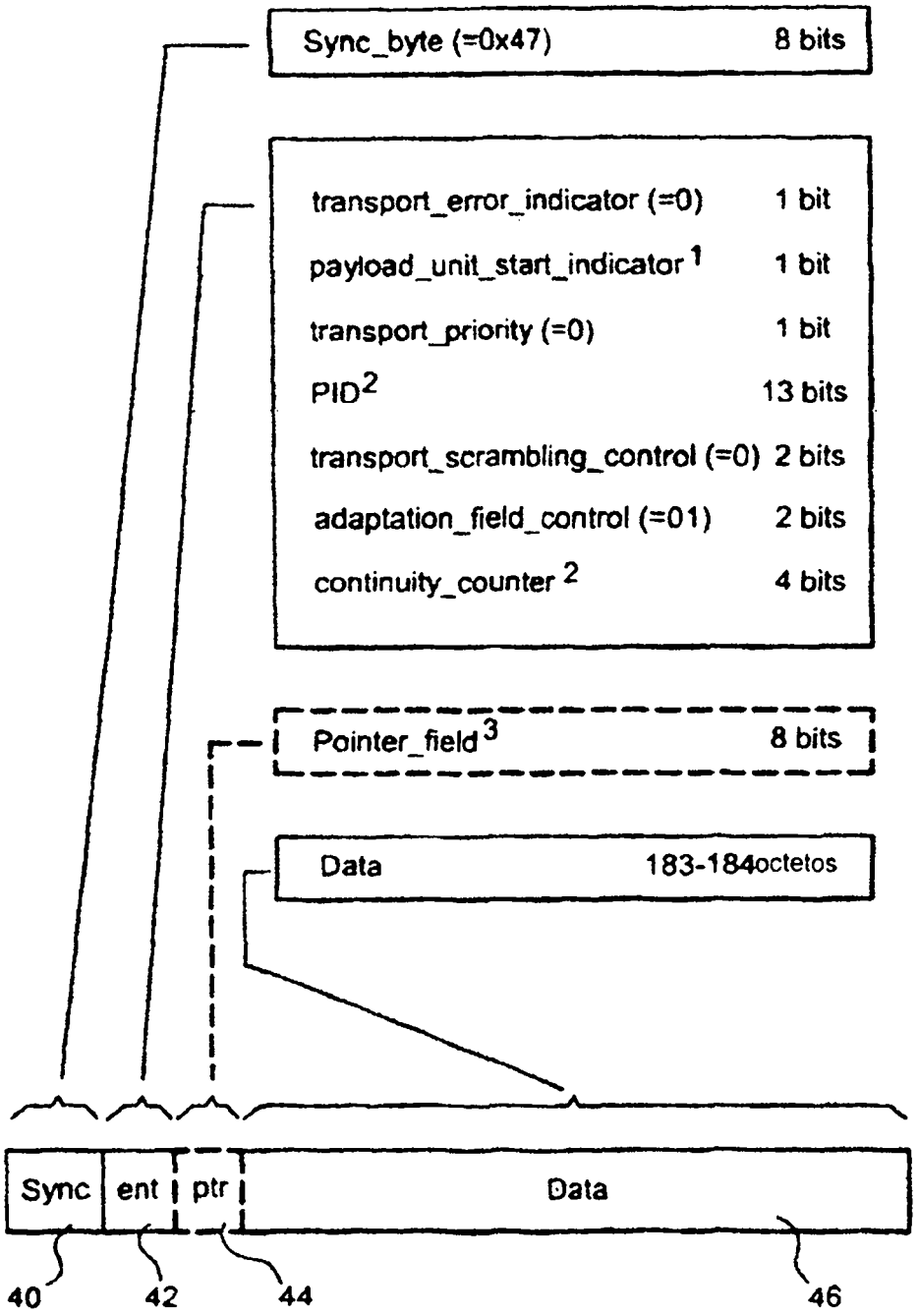

Sync_byte (=0x47) 8 bits
transport_error_indicator (=0) 1 bit
payload_unit_start_indicator 1 1 bit
transport_priority (=0) 1 bit
PID 2 13 bits
transport_scrambling_control (=0) 2 bits
adaptation_field_control (=01) 2 bits
continuity_counter 2 4 bits
Pointer_field 3 8 bits
Data 183-184octetos
Sync
ent
ptr
Data
40
42
44
46

FIG. 4