



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 351 776**

51 Int. Cl.:

H04N 5/00 (2006.01)

H04N 7/16 (2006.01)

H04N 7/167 (2006.01)

G06F 9/445 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **08151281 .6**

96 Fecha de presentación : **11.02.2008**

97 Número de publicación de la solicitud: **2088764**

97 Fecha de publicación de la solicitud: **12.08.2009**

54

Título: **Método de actualización y de gestión de una aplicación de tratamiento de datos audiovisuales incluida en una unidad multimedia mediante un módulo de acceso condicional.**

45

Fecha de publicación de la mención BOPI:
10.02.2011

45

Fecha de la publicación del folleto de la patente:
10.02.2011

73

Titular/es: **NAGRAVISION S.A.**
22, route de Genève
1033 Cheseaux-sur-Lausanne, CH

72

Inventor/es: **Philip, Serge;**
Le Buhan, Corinne y
Nicoulin, Andre

74

Agente: **Tomás Gil, Tesifonte Enrique**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Método de actualización y de gestión de una aplicación de tratamiento de datos audiovisuales incluida en una unidad multimedia mediante un módulo de acceso condicional.

Ámbito de la invención

La presente invención se refiere al ámbito de las unidades multimedia que incluye una aplicación de tratamiento de flujo de datos audiovisuales con acceso condicionado difundidas a través de emisores terrestres, satélites, cable o a través de una red de banda ancha y de alto caudal de datos por cable o inalámbrico del tipo WiFi, Wimax, UMTS etc.

Antecedentes técnicos

Las unidades multimedia son definidas aquí como ordenadores personales fijos o portátiles, descodificadores de televisión digital, televisores o teléfonos etc. a los que se conecta un módulo de acceso condicional y de descryptación. De una forma más particular, el objeto de la invención se sitúa a nivel de la actualización y de la gestión de los programas tanto del módulo de acceso condicional como de la aplicación de tratamiento de los flujos instalados en la unidad multimedia.

Numerosos descodificadores de televisión digital, así como televisores con receptor digital integrado y ordenadores personales provistos de las interfaces adecuadas utilizan para el control del acceso a los datos digitales de audio/vídeo teletransmitidos y su desaleatorización un módulo de acceso condicional CAM (Conditional Access Module). Normalmente, este módulo se presenta bajo la forma de una caja normalizada separable provista de un lector de tarjeta chip y de un conector compatible con una interfaz del ordenador. Un ejemplo se describe en la patente US6443361. Un tal módulo CAM proporcionado por un operador de televisión de pago desaleatoriza uno o varios flujos de datos de audio/vídeo procedentes de un cable, de un emisor terrestre hertziano, de un satélite, de un servidor de Internet a través de una red de comunicación por cable o inalámbrica (WebTV, IP TV) en función de claves o palabras de control recibidas del elemento dedicado al acceso condicional. Este último elemento, encargado de la seguridad de la descryptación de las claves de desaleatorización y de los derechos de acceso condicional, consiste habitualmente en una tarjeta chip o módulo de seguridad, insertado en el lector del módulo de acceso condicional CAM, considerado inviolable en el cual los derechos de un usuario son almacenados. Unos mensajes contenidos en el flujo teletransmitido que consiste en mensajes de control ECM (Entitlement Control Message) y mensajes de administración de los derechos EMM (Entitlement Administration Message) se dirigen hacia el módulo de seguridad que dispone de las claves de transmisión necesarios para la descryptación de estos mensajes. Las palabras de control (CW) contenidas en los mensajes de control ECM son descryptados luego devueltos al módulo de desaleatorización sola y únicamente si los derechos de acceso condicionales están presentes y verificados por el módulo de seguridad.

Un módulo CAM es en general conectado a la unidad multimedia huésped a través de una interfaz común DVB-CI (Dactilar Video Broadcasting - Common Interface) definida por la norma europea EN50221 "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications" editada por la CENELEC (Comisión Europea de Normalización Electrotécnica). Este documento describe una interfaz común que normaliza la estructura de los datos, la codificación de los canales, las informaciones de servicio, la interfaz con la unidad huésped y con el sistema de acceso condicional. Este último se utiliza para controlar el acceso a un servicio difundido que consiste en un conjunto de flujos elementales ofrecidos al usuario en forma de un programa de televisión por ejemplo. Según este documento, el módulo CAM ejecuta las aplicaciones comunicando con la unidad huésped y proporcionando al usuario funcionalidades complementarias a aquellas incluidas en la unidad huésped tales como el sistema de acceso condicional o una guía electrónica de programas. Es además compatible con el formato PCMCIA (Personal Computer Memory Card International Association), USB (Universal Serial Bus) u otro.

Según una configuración compacta, el módulo CAM puede estar bajo la forma de un "dongle" o clave electrónica que incluye a la vez el módulo de seguridad y el módulo de descryptación integrados en uno o varios circuitos electrónicos. Este "dongle" se conecta a un puerto de comunicación del ordenador hacia periféricos externos como el puerto paralelo, el puerto serie USB, el puerto firewire IEEE 1394, etc. Un ejemplo de aplicación de un "dongle" al control de acceso a los datos encriptados se describe en el documento US2007256126.

La unidad multimedia incluye una aplicación particular del tipo Windows Media Player, Real Player, VLC Media Player etc. destinada a aprovechar o visualizar el contenido de los datos difundidos obtenidos después de la descodificación. Esta aplicación se protege en asociación con el módulo de acceso condicional CAM para controlar los registros, las transferencias o las copias del contenido sobre los soportes locales o distantes con el fin de evitar el abuso. Además, no es deseable que una tercera aplicación permita tratar los datos recibidos sin la autorización del difusor o del operador que controle el acceso a estos datos.

Una norma tal como CableCard (SCTE41 <http://www.scte.org>) se puede utilizar para proteger el flujo de datos audiovisuales entre el módulo de acceso condicional y la unidad multimedia. Tal solución necesita sin embargo una gestión rigurosa y protegida de las claves y algoritmos al seno de la unidad multimedia, lo que es difícil de asegurar sobre un largo período en particular en el caso de arquitecturas abiertas tales como se encuentran en los ordenadores personales.

En consecuencia, es deseable garantizar un sólido acoplamiento de la aplicación o del software de explotación del contenido descriptado instalado en la unidad multimedia con el software o microprograma (firmware) del módulo protegido de acceso condicional CAM.

5 Descripción breve de la invención

El objetivo de la presente invención es forzar la actualización de la aplicación de la unidad multimedia por medio del módulo de acceso condicional CAM con el fin de mantener constantemente la dependencia entre la aplicación y el microprograma. Dicho de otro modo, una actualización del microprograma del módulo CAM fuerza una actualización de la aplicación de la unidad multimedia. Es por lo tanto posible forzar una actualización de los mecanismos de seguridad de la unidad multimedia mediante los mecanismos de actualización del microprograma del módulo CAM.

Este objetivo se alcanza por un método de actualización y de gestión de una aplicación de tratamiento de datos audiovisuales incluida en una unidad multimedia, a través de un módulo de acceso condicional encargado de controlar el acceso a los datos audiovisuales encriptados difundidos en un flujo de transporte a través de una red de difusión y controlados por un centro de difusión y/o un centro de gestión, todos o parte de dichos datos siendo devueltos por el módulo de acceso condicional y transmitidos a dicha aplicación de tratamiento de datos audiovisuales, dicho módulo de acceso condicional utilizando un microprograma teniendo una versión corriente para tratar y devolver los datos a la aplicación, el método se caracteriza por el hecho de que incluye las etapas siguientes:

- recepción por el módulo de acceso condicional de informaciones de versiones máxima disponible y mínima requerida del microprograma del módulo de acceso condicional,
- lectura de las informaciones de versión mínima requerida y comparación con la versión corriente del microprograma del módulo de acceso condicional,
- lectura de las informaciones de versión máxima disponible y comparación con la versión corriente del microprograma del módulo de acceso condicional,
- cuando la comparación da un resultado que indica que la versión máxima disponible es superior a la versión corriente del microprograma cargado sobre el módulo de acceso condicional, transmisión a la aplicación de un mensaje de invitación de actualización del microprograma y actualización de dicho microprograma hacia la versión máxima disponible o al menos hacia una versión superior o igual a la versión mínima según las etapas siguientes.
- a) transmisión de una orden de actualización por el módulo de acceso condicional a la unidad multimedia,
- b) recepción de la orden de actualización por la unidad multimedia y transmisión de una solicitud de actualización al centro de gestión, a través de una red de comunicación,
- c) descarga por la unidad multimedia desde el centro de gestión de datos de actualización que incluye por una parte el microprograma del módulo de acceso condicional y por otra parte los datos de actualización de la aplicación de la unidad multimedia,
- d) instalación por una parte del microprograma en el módulo de acceso condicional, y por otra parte de los datos de actualización de la aplicación de la unidad multimedia.
- cuando la comparación da un resultado que indica que la versión mínima requerida es superior a la versión corriente del microprograma cargado sobre el módulo de acceso condicional, desactivación de las funciones de control de acceso a los datos audiovisuales y transmisión a la aplicación de un mensaje de error señalando la necesidad de una actualización del microprograma, según las etapas a) a d).

El objetivo del método es constreñir la actualización del microprograma hacia la versión máxima disponible aunque el módulo de acceso condicional puede funcionar correctamente con un microprograma de versión mínima. Una actualización hacia la versión mínima es de hecho imperativa para que el módulo de acceso condicional sea capaz de efectuar las operaciones de desaleatorización del flujo a fin de volver accesibles los contenidos difundidos a un usuario de la unidad multimedia mediante la aplicación.

Según una variante del método, cuando la versión mínima requerida es superior a la versión corriente del microprograma, la actualización del microprograma se puede efectuar directamente hacia la versión máxima disponible. La etapa de comparación de la versión corriente con las versiones máxima y mínima dará de este modo un resultado que indica que la versión corriente es superior a la versión mínima e igual a la versión máxima. En consecuencia, ningún mensaje de invitación a una actualización aparecerá.

Las informaciones de versión mínima y máxima del microprograma del módulo de acceso condicional son insertados sea en uno o varios mensajes de control ECM o en uno o varios mensajes de administración de los derechos EMM, sea en tablas de información de servicios tales como se definen por la norma ETSI EN300468, sea en mensajes o en tablas específicas difundidos en el flujo de transporte.

Estas informaciones de versiones son leídas y tratadas por el módulo de acceso condicional solo, independientemente del tipo de unidad multimedia y de la aplicación de tratamiento de datos audiovisuales instalada. La unidad multimedia funciona de este modo como esclava del módulo de acceso condicional en el momento de las operaciones de actualización del microprograma y de la aplicación.

De este modo en particular, la unidad multimedia no se puede utilizar por un usuario malintencionado para esquivar ella sola los mensajes de actualización difundidos en el flujo de transporte: el módulo de acceso condicional él mismo debería ser modificado con este fin.

Además, la actualización del microprograma a través de una solicitud de la aplicación al centro de gestión permite de forma secundaria a este último de controlar la autenticación de la aplicación y de la unidad multimedia que lo alberga en el momento de esta operación, lo que permite un control de legitimidad suplementario.

Además, la aplicación se empareja con el microprograma mediante claves, algoritmos de seguridad y/o protocolos de comunicación específicos que son normalmente renovados en el momento de una actualización conjunta de la versión de la aplicación y del microprograma. Este emparejamiento impide que una tercera aplicación no reconocida, por el difusor por ejemplo, pueda aprovechar los datos devueltos por el módulo de acceso condicional. Inversamente, un módulo de acceso condicional proveniente de una segunda unidad multimedia no será reconocido por una aplicación instalada en una primera unidad con un primer módulo teniendo un microprograma de versión diferente.

Breve descripción de la figura

La invención se comprenderá mejor gracias a la descripción detallada siguiente y que se refiere a la figura adjunta proporcionada a modo de ejemplo en modo alguno limitativo.

- la figura 1 ilustra un esquema funcional de una unidad multimedia equipada de un módulo de acceso condicional y que recibe datos con acceso controlado difundidos a partir de un emisor terrestre, un satélite o de un cable. La unidad multimedia está además conectada, a través de una red de comunicación, a un centro de gestión.

Descripción detallada de la invención

El sistema de recepción de datos de contenidos de audio video digitales con acceso controlado del ejemplo de la figura 1 se compone de una unidad multimedia PC bajo la forma de un ordenador portátil o fijo equipado de un módulo de acceso condicional CAM incluyendo un módulo de seguridad SM. El módulo de acceso condicional CAM funciona gracias a un microprograma P de una versión corriente dada en asociación con una aplicación APP de software del tipo Windows Media Player, Real Player, VLC Media Player etc. instalada en el ordenador y capaz de presentar a un usuario los datos de contenidos de audio video difundidos. Estos datos de contenidos se difunden a través de emisores terrestres TE y/o a través de satélites SAT y/o por un cable CAB en forma de flujo de transporte FT hacia la unidad multimedia equipada con medios de recepción apropiados. Un centro de difusión CD organiza el flujo FT integrando en él los datos necesarios para el control de acceso proporcionados por un centro de gestión CG. Se debe señalar que el centro de difusión CD y el centro de gestión CG pueden ser reunidos en una sola y misma entidad.

Según una variante, este flujo FT se encamina en una red de comunicación del tipo Internet de banda ancha y alto caudal por cable o inalámbrica a la cual se conecta el ordenador. Este modo de difusión es conocido bajo el nombre de WebTV o IP TV o televisión por Internet.

El flujo FT contiene igualmente mensajes de acceso condicional como los mensajes de control ECM y los mensajes de administración de los derechos de acceso EMM. Según una variante, al recibir el flujo por el ordenador PC, la aplicación APP de visionado efectúa un primer filtrado de los datos audiovisuales antes de transmitirlos al módulo de acceso condicional CAM que las descodifica con ayuda de palabras de control descriptadas por el módulo de seguridad SM desde los mensajes de control ECM en función de derechos almacenados en el módulo de seguridad SM. Los datos tratados de este modo son en general recodificados con una clave de sesión asociada a la aplicación APP antes de ser devueltos a ésta para el visionado.

El ordenador PC dispone de una vía de retorno hacia un centro de gestión CG a través de una red de comunicación NET, constituida por un conjunto de servidores y de bases de datos, conectado al centro de difusión CD. Esta vía permite transmitir al centro de gestión CG salvo diversas solicitudes de actualización de los programas asociados al ordenador PC y a sus aplicaciones, una solicitud R de actualización del microprograma P del módulo de acceso condicional CAM. La vía de retorno, independiente de los canales de difusión del flujo, utiliza en general el protocolo IP (Internet Protocol) para la transmisión de los datos del ordenador hacia el centro de gestión CG.

El microprograma P del módulo CAM se define aquí por uno o varios componentes que incluye sea el software de funcionamiento del módulo CAM, sea una o varias claves, uno o varios algoritmos de encriptación/descriptación, sea las interfaces, pilotos y protocolos de comunicación con la aplicación APP instalada en el ordenador asociada al módulo CAM y otros diversos parámetros, y/o variables de funcionamiento. Una actualización UPD del microprograma P se vuelve necesaria cuando uno o varios de estos componentes de software cambian o evolucionan hacia una versión mejorada en relación a la versión corriente, sea una clave, un algoritmo o un parámetro etc. La motivación de esta actualización puede ser una mejora funcional o de forma más general de seguridad.

El microprograma P puede contener igualmente informaciones sobre el tipo, la versión y los parámetros necesarios para la compatibilidad de la aplicación con el módulo CAM. Un microprograma P puede contener una actualización completa destinada a reemplazar todos los componentes que forman el microprograma P corriente, sea el microprograma P puede contener uno o varios de los componentes aislados como por ejemplo una o varias claves, uno o varios algoritmos, uno o varios parámetros o una o varias variables destinadas a renovar solamente el o los componentes correspondientes del microprograma P que ha o han evolucionado.

Cuando tal actualización UPD del microprograma P está disponible, el centro de gestión CG introduce los datos de información de versión correspondiente a la versión del microprograma P alcanzada cuando la actualización es efectuada. Estos se componen de una referencia a una versión mínima requerida para una recepción normal de los datos del flujo de transporte establecidos en un formato legible por el software del módulo de acceso condicional CAM y de una referencia a una versión máxima disponible. Esta última versión es sea superior, sea igual a la versión mínima. En este último caso, el módulo de acceso condicional dejará de funcionar hasta que la actualización sea efectiva, lo que impone restricciones inaceptables en la mayoría de los casos sobre el número de solicitudes de actualizaciones simultáneas a tratar por el centro de gestión así como de cese de servicio para los usuarios de la aplicación. El desfase entre las versiones máxima disponible y mínima requerida constituyen por lo tanto un modo de transporte de ajuste a disposición del centro de gestión en función de sus restricciones particulares tales como la exposición en el tiempo del número de solicitudes de actualización.

Según una variante de la invención, un retraso de gracia se puede asociar a la versión mínima con el fin de evitar la sobrecarga de las solicitudes de actualización cuando la versión mínima transmitida es superior a la versión corriente de numerosos módulos de acceso condicional. Este retraso de gracia puede tomar la forma de una duración relativa a la recepción del mensaje por el módulo de acceso condicional, o la forma de una fecha y/u hora fija. Este retraso de gracia se puede preprogramar en la versión corriente del microprograma o estar transmitido por un mensaje teletransmitido conjuntamente a los datos de información de versión.

Los datos de información de versión pueden ser transmitidos sea en mensajes específicos M de actualización sea en los mensajes de control ECM o de administración EMM difundidos en la circulación de datos con acceso controlado según las normas DVB, ver por ejemplo el documento "Functional model of a conditional access system", EBU Project Group B/CA.

Elas pueden igualmente ser transmitidas en tablas de información de servicios tales como definidas por la norma ETSI EN300468. Este documento titulado Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB Systems publicado por el ETSI describe la estructura de las informaciones de servicios SI. La norma ISO/IEC 13818-1 MPEG-2 "Information technology - Generic coding of moving pictures and associated audio information: Systems" define las informaciones específicas de programas PSI (Program Specific Information).

Los datos PSI permiten configurar el módulo de acceso condicional CAM asociado a la aplicación APP de la unidad multimedia PC de manera automática para desmultiplexar y descodificar los diferentes programas y servicios del flujo de transporte FT.

Estos datos PSI se estructuran en cuatro tipos de tablas que se transmiten por secciones, a saber.

1) La tabla de asociación de programas (PAT) Program Association Table:

Esta indica para cada servicio del multiplex la localización es decir los valores de los identificadores de paquetes PID (Packet Identifier) de los paquetes del flujo de transporte de la tabla de organización de los programas PMT (Program Map Table) correspondiente. Esta proporciona igualmente la localización de la tabla de información red NIT (Network Information Table).

2) La tabla de acceso condicional CAT (Conditional Access Table)

Esta proporciona las informaciones propias de los sistemas de acceso condicional utilizados en el multiplex que incluye la localización del flujo de mensajes de administración EMM (Entitlement Administration Menssage).

3) La tabla de organización de los programas PMT (program Map Table)

Esta identifica e indica las localizaciones de los flujos que constituyen cada servicio y la localización de los campos de referencia de reloj de programa para un servicio.

4) La tabla de información red NIT (network Information Table)

Su localización se define según la norma ISO/IEC 13818-1 MPEG-2, el formato de los datos no estando comprendido en esta norma. Ella proporciona las informaciones sobre la red física como la designación de los emisores (hertzianos o satelitarios) que permiten encontrar otros flujos de transporte sobre la red.

ES 2 351 776 T3

Las informaciones específicas de programas PSI se completan a través de datos que permiten al usuario de identificar los servicios y los acontecimientos transportados en un múltiplex o en una red. Estos datos se reparten en tablas tales como:

- 5 - la tabla de asociación de paquetes BAT (Bouquet Association Table) que proporciona además del nombre del paquete (conjunto de programas o de servicios puestos a disposición de usuarios por un difusor), la lista de los servicios disponibles en cada paquete. Esta tabla es facultativa.
- la tabla de descripción de servicio SDT (Service Description Table) conteniendo los datos que describen los
10 servicios como los nombres y los proveedores de los servicios.

Las informaciones sobre los contenidos de los programas figuran en las tablas de información sobre los acontecimientos EIT (Event Information Table) que se refieren a cada servicio a partir de su identificación según la norma
15 DVB. Estas informaciones describen las diferentes emisiones proponiendo las informaciones semejantes a aquellas que se encuentran en una revista tradicional de programas TV.

Las tablas mencionadas arriba tienen cada una al menos una sección reservada a los datos suplementarios que el difusor puede introducir sea en este caso las informaciones de versión mínima y máxima del microprograma P del
20 módulo CAM.

Por razones de seguridad, la integridad de estas informaciones de versión, cualquiera que sea su modo de emisión es decir por mensaje de control ECM, de administración EMM, mensaje específico o por tablas de información de servicio, debe ser verificada por el módulo de acceso condicional CAM. Con el fin de impedir su modificación por
25 la aplicación APP o por otro software instalado en la unidad multimedia, estas son de preferencia acompañadas de su firma constituida por una huella de las informaciones obtenidas con ayuda de una función matemática de elección arbitraria unidireccional y cifrada por una clave conocida del módulo CAM o del módulo de seguridad SM.

Según una variante, estas informaciones de versión se encriptan a través de una clave conocida del módulo CAM
30 o del módulo de seguridad SM.

Después de la lectura de las informaciones de versión, el módulo de acceso condicional CAM compara antes de todo su versión corriente con la referencia de la versión mínima del microprograma P capaz de asegurar la descricp-
tación de los datos del flujo de transporte.

En caso de diferencia puesta en evidencia por una versión corriente inferior a la versión mínima leída, las funciones de control de acceso a los datos audiovisuales del módulo de acceso condicional CAM son desactivados volviendo el módulo CAM no apto para descodificar los datos del flujo. El módulo CAM transmite entonces un mensaje de error a la aplicación APP que hace aparecer sobre la pantalla de la unidad multimedia y advierte al usuario de la necesidad de una actualización del microprograma P. Una orden es igualmente transmitida a la unidad multimedia PC que se
40 encarga de enviar, a través de la red de comunicación nítida, una solicitud R de descarga de actualización al centro de gestión CG. Este último transmite a la unidad multimedia PC, después de la verificación de la solicitud R, los datos de actualización UPD de preferencia en forma encriptadas con una clave conocida del módulo CAM o del módulo de seguridad SM y firmadas. La encriptación y la firma sirven para prevenir todo reemplazo abusivo del microprograma P por descarga desde un tercer servidor no reconocido por el difusor.

La descarga de la actualización del microprograma P puede efectuarse sea manualmente por transmisión de una orden, por ejemplo, en forma de un click sobre un botón apropiado en respuesta al mensaje aparecido sobre una pantalla solidaria con la unidad multimedia, sea completamente automáticamente, sin intervención del usuario, desde
50 la recepción de la orden por la unidad multimedia.

Desde el final de la descarga, la instalación de la actualización del microprograma P se desarrolla simultáneamente por una parte en el módulo de acceso condicional CAM y por otra parte en la aplicación APP de la unidad multimedia PC. Este proceso de instalación, como el de la descarga, puede igualmente efectuarse manualmente bajo orden o
55 automáticamente.

Después de la etapa de instalación de la actualización del microprograma P en el módulo de acceso condicional CAM y de los datos procedentes del microprograma P que sirven para actualizar la aplicación APP en la unidad multimedia PC, las funciones de control de acceso a los datos audiovisuales del microprograma P del módulo de acceso condicional CAM son reactivadas. La actualización del microprograma P corriente es entonces efectuada al menos hacia una versión mínima.

La actualización del microprograma P del módulo de acceso condicional CAM y los datos de actualización de la aplicación APP de la unidad multimedia PC comprenden un protocolo de comunicación protegida entre el módulo de acceso condicional CAM y la aplicación APP utilizando un algoritmo y claves de cifrado y/o una actualización de claves de emparejamiento del microprograma P con la aplicación APP.

El emparejamiento es, por ejemplo, efectuado según el mecanismo descrito en el documento EP1078524B1 en el cual los datos intercambiados entre el microprograma P del módulo CAM y la aplicación APP se cifran por una clave única de emparejamiento almacenada por una parte en el módulo CAM y por otra parte en la unidad multimedia PC.

5 El microprograma P del módulo de acceso condicional CAM se empareja a la aplicación APP de la unidad de multimedia PC para asegurar un funcionamiento conjunto de los dos partes solamente con las versiones previamente instaladas.

10 No es por lo tanto posible actualizar el módulo CAM independientemente de la aplicación APP ni inversamente. En caso que esta instalación de las actualizaciones no pueda ser efectuada de manera sincrónica en la unidad multimedia PC y en el módulo de acceso condicional CAM, la unidad multimedia PC o preferentemente la aplicación APP no será reactivada por lo tanto incapaz de explotar los datos del flujo de la manera esperada. El método según la invención asegura de este modo una evolución en paralelo de las dos partes del microprograma P mientras que impide que una aplicación cualquiera y no reconocida pueda descodificar los datos del flujo difundido.

15 Las informaciones de versión contienen, además de la referencia a la versión mínima requerida, una referencia a una versión máxima del microprograma P que sería ventajoso de cargar en el módulo CAM. Cuando esta versión máxima es superior a las versiones corriente y mínima, un mensaje aparece sobre la pantalla de la unidad multimedia incitando al usuario a una descarga ulterior de la nueva versión. Esta última no es absolutamente necesaria para un funcionamiento correcto del conjunto formado por la aplicación de la unidad multimedia y del módulo de acceso condicional CAM. La versión máxima puede también sea corresponder a una versión superior a la versión mínima proporcionando las funcionalidades suplementarias sea a la última versión disponible del microprograma P. En ese caso, el módulo CAM queda activado contrariamente por si acaso la versión corriente es detectada como siendo inferior a la versión mínima.

25 Según una variante, con el fin de animar a los usuarios a cargar la versión máxima, y cuando ésta es superior a las versiones corriente y mínima, el funcionamiento del conjunto aplicación - módulo de acceso condicional CAM se puede alterar o limitar a la descriptación de un número restringido de canales de audio/vídeo del flujo de transporte.

30 El método según la invención permite por lo tanto una actualización del microprograma en dos tiempos cuando la versión corriente es inferior a las versiones mínima y máxima. Contrariamente a la obligación de la actualización a la versión mínima, la actualización a la versión máxima es recomendable. De este modo, una unidad multimedia equipada con un módulo CAM de versión mínima puede funcionar durante un cierto tiempo sin conexión a la red de comunicación NET liberando las actualizaciones incluso si las informaciones de versión indican la disponibilidad de una versión máxima.

40 Este período de funcionamiento mínimo puede ser terminado sea por el usuario respondiendo al mensaje de invitación de actualización después de la conexión de la unidad multimedia a la red de comunicación NET, sea por el difusor. Este último reemplaza, en las informaciones de versión, la referencia a la versión mínima por la referencia a la versión máxima. Esta operación permite al difusor de desactivar los módulos CAM cuyo microprograma no está en la versión máxima disponible. De este modo una actualización a la versión máxima se vuelve imperativa porque la versión corriente es inferior a la versión mínima que corresponde en tal caso a la versión máxima que el difusor desea imponer.

45 **Referencias citadas en la descripción**

50 *Esta lista de referencias citada por el solicitante ha sido recopilada exclusivamente para la información del lector. No forma parte del documento de patente europea. La misma ha sido confeccionada con la mayor diligencia; la OEP sin embargo no asume responsabilidad alguna por eventuales errores u omisiones.*

Documentos de patente citados en la descripción

- 55 ■ US 6443361 B [0003]
- US 2007256126 A [0005]
- 60 ■ EP 1078524 B1 [0042]

60

65

REIVINDICACIONES

1. Método de actualización y de gestión de una aplicación APP de tratamiento de datos audiovisuales incluida en una unidad multimedia PC, a través de un módulo de acceso condicional CAM a cargo de controlar el acceso a los datos audiovisuales encriptados difundidos en un flujo de transporte FT a través de una red de difusión y controlados por un centro de difusión CD y/o un centro de gestión CG, todos o parte de dichos datos siendo devueltos por el módulo de acceso condicional CAM y transmitidos a dicha aplicación APP de tratamiento de datos audiovisuales, dicho módulo de acceso condicional CAM utilizando un microprograma P teniendo una versión corriente para tratar y devolver los datos a la aplicación APP,

- el método se **caracteriza** por el hecho de que incluye las etapas siguientes:

- recepción por el módulo de acceso condicional CAM de informaciones de versiones máxima disponible y mínima requerida del microprograma P del módulo de acceso condicional CAM,

- lectura de las informaciones de versión mínima requerida y comparación con la versión corriente del microprograma P del módulo de acceso condicional CAM,

- lectura de las informaciones de versión máxima disponible y comparación con la versión corriente del microprograma P del módulo de acceso condicional CAM,

- cuando la comparación da un resultado que indica que la versión máxima disponible es superior a la versión corriente del microprograma P cargado sobre el módulo de acceso condicional CAM, transmisión a la aplicación APP de un mensaje de invitación de actualización del microprograma P y actualización de dicho microprograma P hacia la versión máxima disponible o al menos hacia una versión superior o igual a la versión mínima según las etapas siguientes.

a) transmisión de una orden de actualización por el módulo de acceso condicional CAM a la unidad multimedia PC,

b) recepción de la orden de actualización por la unidad multimedia PC y transmisión de una solicitud R de actualización al centro de gestión CG, a través de una red de comunicación NET,

c) descarga por la unidad multimedia PC desde el centro de gestión CG de datos de actualización UPD que incluye por una parte el microprograma P del módulo de acceso condicional CAM y por otra parte datos de actualización de la aplicación APP de la unidad multimedia PC,

d) instalación por una parte del microprograma P en el módulo de acceso condicional CAM, y por otra parte de los datos de actualización de la aplicación APP de la unidad multimedia PC.

- cuando la comparación da un resultado que indica que la versión mínima requerida es superior a la versión corriente del microprograma P cargado sobre el módulo de acceso condicional CAM, desactivación de las funciones de control de acceso a los datos audiovisuales y transmisión a la aplicación APP de un mensaje de error señalando la necesidad de una actualización del microprograma P, según las etapas a) a d).

2. Método según la reivindicación 1 **caracterizado** por el hecho de que la actualización del microprograma P del módulo de acceso condicional CAM y los datos de actualización de la aplicación APP de la unidad multimedia PC se emparejan de manera que la actualización del módulo de acceso condicional CAM necesita la actualización de la aplicación APP para tratar y devolver los datos a la aplicación APP.

3. Método según la reivindicación 1 **caracterizado** por el hecho de que las funciones de control de acceso a los datos audiovisuales del microprograma P del módulo de acceso condicional CAM son reactivados después de la etapa de instalación de la actualización del microprograma P en el módulo de acceso condicional CAM y de los datos de actualización de la aplicación APP en la unidad multimedia PC, la actualización del microprograma P corriente estando efectuada al menos hacia una versión mínima.

4. Método según la reivindicación 2 **caracterizado** por el hecho de que la actualización del microprograma P del módulo de acceso condicional CAM y los datos de actualización de la aplicación APP de la unidad multimedia PC comprenden un protocolo de comunicación protegida entre el módulo de acceso condicional CAM y la aplicación APP utilizando un algoritmo y claves de cifrado y/o una actualización de claves de emparejamiento del microprograma P con la aplicación APP.

5. Método según la reivindicación 1 **caracterizado** por el hecho de que las informaciones de versiones máxima disponible y mínima requerida del microprograma P se transmiten en uno o varios mensajes de control ECM o en uno o varios mensajes de administración EMM, dichos mensajes siendo conducidos hacia el módulo de acceso condicional CAM.

6. Método según la reivindicación 1 **caracterizado** por el hecho de que las informaciones de versión del microprograma P son transmitidas, en secciones reservadas al difusor en una o varias tablas de información de servicios tales como definidas por la norma ETSI EN300468, dichas tablas siendo conducidas hacia el módulo de acceso condicional CAM.

5

7. Método según las reivindicaciones 1 a 6 **caracterizado** por el hecho de que las informaciones de versión del microprograma P se transmiten en forma firmada con una clave conocida del módulo de acceso condicional CAM.

10

8. Método según las reivindicaciones 1 a 6 **caracterizado** por el hecho de que las informaciones de versión del microprograma P se transmiten en forma cifrada con una clave conocida del módulo de acceso condicional CAM.

9. Método según la reivindicación 1 **caracterizado** por el hecho de que el flujo de datos audiovisuales encriptados se filtra por un módulo de recepción externa o integrado a la unidad multimedia antes del tratamiento por el módulo de acceso condicional CAM.

15

10. Método según la reivindicación 1 **caracterizado** por el hecho de que el flujo de datos audiovisuales encriptados se filtra y es tratado por el módulo de acceso condicional CAM.

20

11. Método según la reivindicación 1 **caracterizado** por el hecho de que las operaciones de descarga y de instalación de la actualización del microprograma P se efectúan manualmente con ayuda de órdenes transmitidas por un usuario a la unidad multimedia PC en respuesta a los mensajes de error y de invitación transmitidos por el módulo de acceso condicional CAM.

25

12. Método según la reivindicación 1 **caracterizado** por el hecho de que las operaciones de descarga y de instalación de la actualización del microprograma P se efectúan automáticamente sin la intervención de un usuario.

30

35

40

45

50

55

60

65

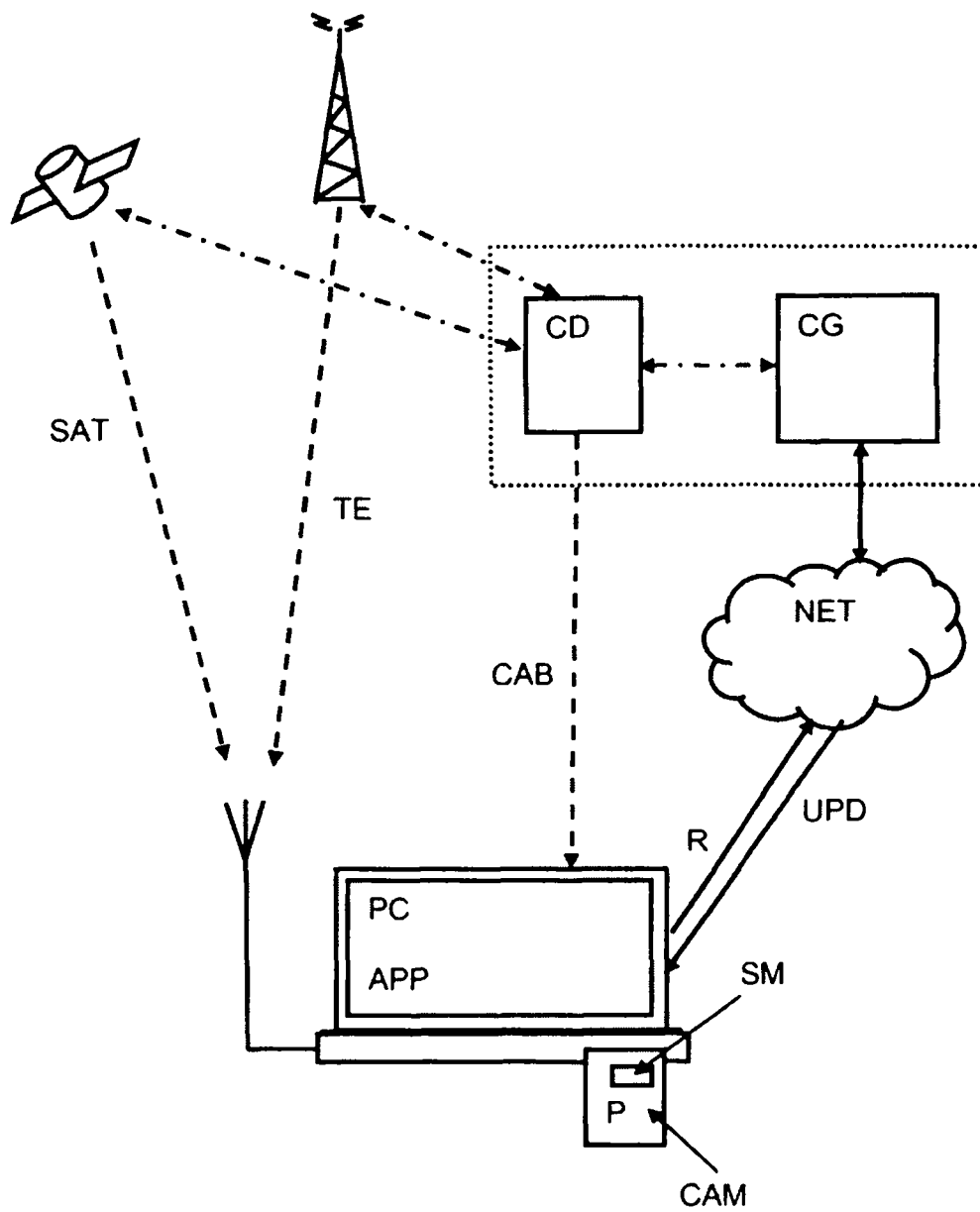


Fig. 1