(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 439 230**

(51) Int. CI.:

H04N 7/167 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.11.2005 E 05817128 (1)**

(97) Fecha y número de publicación de la concesión europea: **02.10.2013 EP 1815681**

(54) Título: **Unidad de tratamiento de datos de audio/vídeo digitales y método de control de acceso a dichos datos**

(30) Prioridad:

24.11.2004 EP 04106029

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.01.2014

(73) Titular/es:

NAGRAVISION SA (100.0%)
22, ROUTE DE GENÈVE
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

PUIATTI, JEAN-MICHEL;
GREMAUD, FABIEN;
MOREILLON, GUY;
FISCHER, NICOLAS;
NICOULIN, ANDRÉ y
HILL, MICHAEL JOHN

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Unidad de tratamiento de datos de audio/vídeo digitales y método de control de acceso a dichos datos

Campo de la técnica

[0001] La presente invención se refiere al ámbito de las unidades de tratamiento de datos de audio/vídeo digitales. Estas unidades son incluidas en diferentes equipos multimedia como por ejemplo ordenadores personales, equipos móviles o descodificadores de televisión digital de pago provistos de memorias dinámicas y estáticas (RAM Random Access Memory, EEPROM Electrically Erasable Programable Read-Only Memory, disco duro, etc.). Esta invención describe igualmente un método de control de acceso a dichos datos de audio/vídeo antes de su salida hacia un periférico utilizado por un usuario.

Estado de la técnica anterior

[0002] Una unidad de tratamiento de datos de audio/vídeo digitales como un descodificador de televisión digital o "set top box" incluye habitualmente un módulo principal que reagrupa varias o todas las funcionalidades esenciales para la desencriptación, para la descompresión y para la interfaz de los datos de audio/vídeo recibidos de una red de difusión por cable, hertziana, por satélite o por una línea telefónica pública.

[0003] El módulo comprende, entre otros, una unidad central que gestiona una unidad de desciframiento, una unidad de descompresión y diversas interfaces que permiten al módulo comunicarse con diferentes periféricos externos asociados al descodificador tales como un módulo de seguridad o aparatos multimedia. La mayoría de estos elementos son conectados a un bus central dentro del módulo. Este bus conecta igualmente memorias externas para la memorización temporal de los datos de trabajo o para el almacenamiento de un contenido de audio/vídeo destinado a una utilización ulterior.

[0004] El proceso de desencriptación, por la unidad de desciframiento, del flujo de datos de audio/vídeo proveniente de la red de difusión, necesita el almacenamiento intermediario de los datos en una memoria de tamaño relativamente importante separada del módulo principal. Estos datos almacenados pueden estar constituidos por bloques de datos de audio/vídeo, son a continuación descomprimidos antes de su encaminamiento hacia una interfaz de salida que permita su visualización en un televisor o su registro en un soporte magnético u óptico como un disco duro o un disco compacto (CD Compact Disc, DVD Digital Versatile Disc u otro).

[0005] La presencia de estos datos desencriptados en una memoria separada constituye un fallo en la protección de los datos de audio/vídeo comprimidos. De hecho, estos datos pueden ser desviados y recogidos para ser tratados y distribuidos por un sistema ajeno externo para utilizarlos de forma abusiva.

[0006] Además, los datos almacenados para una utilización futura, por ejemplo en un disco duro, pueden igualmente ser retomados y reproducidos sin autorización del proveedor, violando de este modo las prescripciones sobre los derechos de autor.

[0007] El documento US6286103 describe un decodificador de los datos cifrados de audio/vídeo donde un módulo de seguridad descifra los datos y los reencripta antes de transmitirlos al decodificador. Según una variante, la transmisión entre el módulo de seguridad y el decodificador se asegura por medio de una clave de sesión creada de un número aleatorio generado por el decodificador y cifrado con una clave publicada del módulo de seguridad. Este número, siendo combinado con la clave del desciframiento de los datos, varía con frecuencia lo cual permite la prevención o la representación más difícil del desciframiento por terceros que obtienen la clave dicha del desciframiento fraudulento.

[0008] El documento WO00/57636 describe varios usos de los módulos de seguridad en la forma de tarjetas personalizadas según las categorías de usuarios. En detalle, en una red de los decodificadores del contenido de los multimedia, se reencriptan los datos descifrados. El desciframiento es posible solamente cuando el decodificador se equipa de una tarjeta debidamente autenticada que contiene los parámetros específicos al usuario. Según una variante, una tarjeta es autenticada usando un número aleatorio generado por el decodificador y transmitido a la tarjeta. El último cifra el número aleatorio con una clave privada y lo vuelve a enviar al decodificador, que lo descifra con la clave pública correspondiente. Una comparación entre el número generado y el número recibido permite verificar la autenticidad de la tarjeta.

Breve descripción de la invención

[0009] El objetivo de la presente invención es paliar estos inconvenientes evitando que los datos desencriptados se hagan accesibles a los intentos de fraude o de reproducciones no autorizadas. Dicho de otro modo, los datos desencriptados no puedan ser utilizados sin el control del proveedor.

[0010] Este objetivo es alcanzado por una unidad de tratamiento de datos de audio/vídeo digitales encriptados con palabras de control provenientes de mensajes de control comprendiendo una unidad de desciframiento de los datos de audio/vídeo, una unidad de descompresión, una interfaz de entrada/salida de los datos de audio/vídeo tratados y medios de comunicación hacia un módulo de seguridad, las unidades de desciframiento y de descompresión comprendiendo respectivamente una unidad de encriptación y una unidad de desencriptación disponiendo cada una de por lo menos una clave personal y de una clave de encriptación común, caracterizada por el hecho de que comporta

- medios de transmisión protegida de la clave común y de la palabra de control extraída de un mensaje de control entre el módulo de seguridad, la unidad de desciframiento y la unidad de encriptación, dichos medios utilizando una clave se asoció a la clave personal de la unidad de encriptación.

- medios para descifrar datos de audio/vídeo con la palabra de control asociados a la unidad de desciframiento,

- medios para reencriptar los datos descifrados dichos con la clave común asociada a la unidad de encriptación,

- una unidad de memoria capaz de almacenar temporalmente los datos de audio/vídeo reencriptados con la clave común,

- medios de transmisión protegida de los datos de audio/vídeo reencriptados a la unidad de desencriptación aptos para comunicarse con el módulo de seguridad y con un generador de números aleatorios asociado a la unidad de desencriptación, dichos medios utilizando la clave personal de la unidad de desencriptación.

- medios de verificación de la integridad del número aleatorio, dichos medios autorizando, cuando el resultado de la verificación es positiva, la desencriptación por la unidad de desencriptación de los datos de audio/vídeo con la clave común.

[0011] Un módulo de seguridad es aquí un dispositivo considerado inviolable que contiene diversas claves de encriptación/desencriptación así como los datos propios de un usuario que definen los derechos que ha comprado para la utilización de los datos de audio/vídeo. El módulo de seguridad puede encontrarse bajo diferentes formas tales como una tarjeta chip insertada en un lector, un circuito integrado soldado en una tarjeta madre, una tarjeta del tipo tarjeta SIM que se encuentra en la telefonía móvil, etcétera.

[0012] Los datos de audio/vídeo de un flujo difundido son descifrados por la unidad de desciframiento y luego encriptados completa o parcialmente con la clave común por la unidad de encriptación asociada a la unidad de desciframiento. Estos datos son a continuación exportados de la unidad de tratamiento a unidades externas tales como una memoria temporal que almacene el flujo provisional en curso de organización destinado al descompresor MPEG, o cualquier otro periférico interno o externo como un puerto USB, Firewire o disco duro.

[0013] Esta memoria temporal está constituida por una memoria con acceso aleatorio del tipo RAM para el almacenamiento temporal de datos en curso de tratamiento. Para el almacenamiento a más largo plazo, los datos son encaminados hacia un disco duro o grabador DVD. Durante la lectura de una u otra unidad de memoria, los datos son transmitidos a la unidad de descompresión a la cual está asociada la unidad de desencriptación, esta ultima necesitando la clave común asociada a dichos datos.

[0014] Esta clave común puede ser almacenada de numerosas maneras por ejemplo sencillamente en el módulo de seguridad. Según un modo preferido de la invención, ésta es encriptada por una clave local del módulo de seguridad y almacenada con los datos. El criptograma comprendiendo esta clave común contendrá preferiblemente una referencia a los datos, por un identificador. Durante la desencriptación de los datos, este criptograma es sometido al módulo de seguridad para la verificación.

[0015] Esta clave local puede ser reemplazada por una clave de red, permitiendo de este modo a otros miembros de esa red acceder al contenido del criptograma y en definitiva, al contenido encriptado.

[0016] En una primera etapa, el módulo de seguridad determina en base al identificador, si los derechos asociados a ese contenido son válidos, permitiendo así la descompresión y posteriormente la visualización de los datos en una pantalla por ejemplo. Éste requiere el envío de un número aleatorio por la unidad de desencriptación. Una vez recibido este número, el módulo de seguridad compone un mensaje comprendiendo al menos la clave común y el número aleatorio, todo ello estando encriptado por la clave personal de la unidad de desencriptación.

[0017] Según una variante de la invención, se efectúa una función matemática sobre el número aleatorio, función conocida por la unidad de desencriptación. De este modo el número recibido es o el número aleatorio propiamente, o una función directa del número aleatorio. El objetivo es poder asegurarse de que el número recibido corresponde al número aleatorio generado por la unidad de desencriptación.

[0018] Cuando este mensaje alcanza la unidad de desencriptación, es desencriptado por la clave personal, el número aleatorio recibido es comparado con el previamente generado. La clave común solo es utilizada si los dos números son idénticos.

[0019] Cuando estos dos números aleatorios difieren o si el resultado de la comparación es negativo, la unidad de desencriptación puede tomar varias iniciativas. La primera consiste en bloquear inmediatamente la desencriptación de los datos. Otra iniciativa consiste en bloquear de manera diferida, es decir, después de la desencriptación de un número predeterminado de bloques de datos de audio/vídeo. El bloqueo diferido es deseable para hacer más difícil los intentos de determinación del número aleatorio, a través de terceros, mediante intentos sucesivos.

[0020] El objetivo de esta supervisión por el módulo de seguridad es controlar la utilización de los datos, particularmente poder determinar el número de visualización de los datos. De este modo, en cada utilización de los datos, es necesario solicitar al módulo de seguridad que puede contar y decidir la utilización de dichos datos.

[0021] Gracias a la presencia de este número aleatorio en el mecanismo de carga de la clave común, se impide todo ataque de reproducción no autorizada (replay attack).

[0022] Otra ventaja de la unidad de tratamiento según la invención reside en que ningún dato descifrado sea almacenado en la memoria ni hecho accesible desde el exterior sea cual sea la interfaz utilizada.

[0023] La encriptación de los datos antes de su almacenamiento en la memoria es efectuada a través de un algoritmo apropiado que permite un tratamiento a la vez rápido y seguro.

[0024] La unidad de tratamiento de la presente invención forma un módulo que puede encontrarse también o en un ordenador personal o en un descodificador de televisión digital de pago. En el caso del ordenador, el módulo puede, por ejemplo, ser instalado en una tarjeta conectada al bus principal o directamente en la tarjeta madre.

[0025] En ambos casos se disponen unidades de memoria en forma de memoria con acceso aleatorio (RAM) o discos duros. Con el fin de evitar las copias no autorizadas, el contenido almacenado encriptado es desencriptado bajo control del módulo de seguridad.

[0026] En el caso de los descodificadores de televisión digital, la clave común utilizada es generada ya sea por el módulo seguridad, ya sea por la cabeza de la red de difusión "Head End" y transmitida mediante mensajes de administración EMM. En tal caso, esta clave es encriptada con las claves personales del módulo de seguridad y luego transmitida a dicho módulo. Cuando se cambia de canal, por ejemplo, la clave común puede cambiar, lo que implica el envío de un nuevo mensaje de administración EMM o la generación de una nueva clave por el módulo de seguridad.

[0027] En el caso de un ordenador personal, esta clave es o descargada de un servidor de un centro de gestión o generada por el módulo de seguridad que puede estar bajo la forma de una tarjeta chip o una "mochila" o una clave electrónica conectada a un puerto de comunicación del ordenador personal (puerto paralelo, puerto serie USB etc.).

[0028] La presente invención se refiere igualmente a un método de control de acceso a los datos de audio/vídeo digitales recibidos por una unidad de tratamiento comprendiendo una unidad de desciframiento de los datos de audio/vídeo, una unidad de descompresión, una interfaz de entrada/salida de los datos de audio/vídeo tratados y medios de comunicación hacia un módulo de seguridad, las unidades de desciframiento y de descompresión comprendiendo respectivamente una unidad de encriptación y una unidad de desencriptación utilizando al menos una clave personal y una clave de encriptación común, caracterizado por el hecho de que comprende las etapas siguientes:

- recepción de un mensaje de control conteniendo por lo menos una palabra de control por el módulo de seguridad,

- obtención por el módulo de seguridad de una clave común y generación de un criptograma encriptado con la clave personal de la unidad de encriptación comprendiendo la clave común y la palabra de control,

- transmisión del criptograma a la unidad de desciframiento desencriptación con la clave de dicho criptograma,

- carga de la clave común en la unidad de encriptación y autorización del desciframiento de los datos de audio/vídeo con la palabra de control,

- desciframiento de los datos de audio/vídeo y encriptación de dichos datos por la unidad de encriptación con la clave común,

- transmisión de dichos datos de audio/vídeo reencriptados a la unidad de desencriptación,

- selección por el módulo de seguridad de la clave común específica a los datos de audio/vídeo,

- transmisión de un número aleatorio por la unidad de desencriptación al módulo de seguridad,

- formación y posterior transmisión de un criptograma encriptado con la clave personal de la unidad de desencriptación conteniendo al menos la clave común y el número aleatorio,

- recepción del criptograma por la unidad de desencriptación,

- desciframiento de dicho criptograma con la clave personal de la unidad del desciframiento y de la verificación dichas de la integridad al azar

- desencriptación de dicho criptograma con la clave personal de dicha unidad de desencriptación y verificación de la integridad del número aleatorio comparando el número aleatorio recibido con el previamente generado.

- carga de la clave común y desencriptación de los datos de audio/vídeo si el resultado de la comparación es positiva.

Breve descripción de la figura

[0029] La invención se comprenderá mejor gracias a la siguiente descripción detallada y que se refiere a la única figura adjunta proporcionada a modo de ejemplo en modo alguno limitativo.

[0030] La figura 1 representa un esquema funcional de un ejemplo de unidad de tratamiento incluido en un descodificador de televisión digital de pago mostrando diferentes elementos externos a esta unidad implicados en el intercambio de datos y de claves tales como las memorias y el módulo de seguridad.

Descripción detallada de la invención

[0031] La figura 1 ilustra un ejemplo de aplicación de la unidad de tratamiento según la invención en un descodificador (STB) de televisión digital de pago. El descodificador (STB) comprende un procesador central (CPU) encargado de gestionar ciertas funciones de una unidad de desciframiento (DMX), de una unidad de descompresión (MPEG), y de interfaces que se comunican con las memorias (RAM; HD) y el módulo de seguridad (SM). La unidad de desciframiento (DMX) sirve no sólo para descifrar el flujo de datos de audio/vídeo entrante, sino también para convertir este flujo en diferentes formatos haciendo los datos que contiene compatibles con las diferentes aplicaciones del descodificador (STB).

[0032] Los datos de audio/vídeo (DT) son recibidos por la unidad de desciframiento (DMX) que los descifra con ayuda de las palabras de control (CW) provenientes de los mensajes de control (ECM). Los datos descifrados son a continuación encriptados por la unidad de encriptación (EC) con una clave de encriptación común (Ki). Los datos así encriptados pueden ser desencriptados ya sea inmediatamente, ya sea ulteriormente después del almacenamiento en una unidad de memoria tal como una memoria con acceso aleatorio (RAM), una memoria no volátil del tipo EEPROM o en un disco duro (HD). Tras una solicitud, los datos almacenados son encaminados hacia la unidad de desencriptación (DC) que se encarga de descodificarlos, bajo control del módulo de seguridad (SM), antes de su descompresión por la unidad de descompresión (MPEG).

[0033] Un programa mediador "middleware" (MD) coordina el funcionamiento de los diferentes programas que gestionan las unidades (DMX, MPEG, EC, DC) que pueden estar incluidas en un mismo módulo (UT). Éste gestiona también los accesos y los intercambios de datos efectuados por las unidades (DMX, MPEG, EC, DC) de y hacia el módulo de seguridad (SM) y las unidades de memoria (RAM, HD).

[0034] En un descodificador, el procesador central (CPU), considerado como poco seguro, no lleva todas las funciones de las unidades de encriptación (EC) y de desencriptación (DC). De hecho, en el caso de un procesador central que controle todas las unidades, un acceso a este procesador permitiría reprogramarlo o ponerlo en cortocircuito con un emulador externo con el fin de efectuar la encriptación y la desencriptación de los datos con una clave predeterminada conocida. Así, para evitar tal intervención, se pueden considerar varias soluciones:

- Utilización de un procesador central (CPU) cuya arquitectura descansa sobre una estructura protegida del tipo "Trust Zone" implementada en la parte material del corazón del procesador. Este ámbito de ejecución protegida permite una protección contra los ataques con programas de las memorias internas y externas del circuito del procesador así como de los periféricos. Los datos y el código protegido son marcados y divididos en el procesador central manteniendo una separación material diferenciada entre los datos protegidos y no protegidos. Esta separación permite al código protegido y a los datos ser ejecutados en un ambiente restringido de una manera segura y eficaz con respecto a un sistema de explotación quedando invulnerables a los ataques. Un dispositivo de control de seguridad conmuta el procesador central de un estado no protegido a un estado protegido donde el procesador accede a los niveles de privilegios más elevados para ejecutar el código confidencial. Éste puede así efectuar las tareas tales como la autentificación, los cálculos de firmas y el tratamiento de transacciones protegidas. Hace pues imposible acceder a la seguridad del procesador central o de modificarlo por un virus o una aplicación no autorizada.

- Implementación de una arquitectura basada en un sistema comprendiendo dos microprocesadores de los que el primero ejecuta el código protegido mientras que el segundo ejecuta las operaciones no protegidas. El primer

procesador está aislado por una parte de todo acceso proveniente del exterior y por otra parte, está protegido de todo ataque con programas procedente por ejemplo de un control no autorizado del segundo procesador no protegido. El primer procesador generará el número aleatorio, recibirá el mensaje del módulo de seguridad, lo desencriptará y cargará la clave común en la unidad de desencriptación. Cabe señalar que la unidad de desencriptación (o de encriptación) puede ser realizada en forma de programa por este primer procesador.

- Descentralización de la gestión de las claves y de los procesos de tratamiento en la unidad de desciframiento (DMX), respectivamente en la unidad de descompresión (MPEG) a través de procesadores apropiados que dirigen dichas unidades independientemente del procesador central (CPU). Las unidades de encriptación (EC) y de desencriptación (DC) son implementadas en forma de elementos materiales (hardware) en las unidades de descifrado (DMX) y de descompresión (MPEG) incluidas en la unidad de tratamiento (UT). Éstas pueden igualmente ser de soporte lógico en forma de microcódigo gestionado por el procesador dedicado a las operaciones protegidas según una u otra de las tres soluciones descritas anteriormente. Estos elementos de soporte lógico son coordinados y sus tareas son atribuidas por el programa personalizado "middleware" (MD).

[0035] La memoria (RAM) con acceso aleatorio puede ser similar a aquella utilizada en los ordenadores personales, como por ejemplo una memoria del tipo SDRAM (Synchronous Dynamic Random Access Memory) o del tipo SRAM (Static Random Access Memory) beneficiándose de un tiempo de acceso más rápido.

[0036] Según un ejemplo de configuración, el descodificador puede contener un bus (B) al cual pueden ser conectados varios tipos de unidades de almacenamiento como la memoria con acceso aleatorio (RAM), una memoria programable borrable (EEPROM) o Flash EEPROM, o uno o varios discos duros (HD). Además, los datos de audio/vídeo encriptados pueden ser encaminados hacia una red local (LAN) a través del bus (B) y un puerto (P) para ser utilizados por otros descodificadores o unidades de tratamiento. La seguridad de estos datos está protegida por su encriptación con la clave común (Ki). Las unidades de tratamiento o descodificadores conectados a esta red (LAN) son equipadas para gestionar y desencriptar los datos de audio/vídeo en función de los derechos almacenados en su módulo de seguridad.

[0037] Con el fin de optimizar la velocidad de tratamiento, la encriptación en la unidad de encriptación (EC) es habitualmente efectuada con un algoritmo rápido entrañando un proceso de mezclas de bloques y/o de direcciones. Por ejemplo los bloques de datos pueden ser codificados a través de una función XOR (o exclusivo) cuyos parámetros son determinados por la clave común (Ki). Una función similar puede igualmente codificar las direcciones de memoria atribuidas a los diferentes bloques que deben ser almacenados. Otro método de encriptación consiste en codificar el orden en el cual los bloques son almacenados en la memoria mediante la clave común (Ki). Este tipo de mezcla de direccionamiento puede ser fácilmente realizado por un circuito FPLA (Field Programable Logic Array) incorporado en la unidad de encriptación (EC). Evidentemente se puede utilizar otros algoritmos más sofisticados para esta encriptación.

[0038] La encriptación con la clave común (Ki) solo puede ser parcial, es decir, no concernir más que a una parte de los bloques de datos que deben ser almacenados o más que a una parte de las direcciones de memorias en las que estos bloques serán almacenados. Preferiblemente, la encriptación llevará los datos destinados al usuario final (payload) tales como las imágenes y el sonido y no los encabezamientos de los paquetes de datos o los archivos que sirven para el tratamiento de éstos.

[0039] En una primera variante, la clave de encriptación común (Ki) es transmitida por un centro de gestión o por la cabeza de la red de difusión (Head End) a través de un mensaje de administración (EMM). Este mensaje (EMM) que contiene igualmente los derechos de desciframiento de los datos de audio/vídeo propios para cada usuario es tratado por el módulo de seguridad (SM) en general en forma de una tarjeta chip insertada en un lector apropiado del descodificador (STB). Esta clave de encriptación común (Ki) es susceptible de cambiar en cada cambio de canal de difusión lo que implica que el nuevo mensaje de administración (EMM) difundido contendrá una nueva clave común (Ki).

[0040] Según una variante utilizada, cuando se desea reducir el número de mensajes transmitidos por el centro de gestión o la cabeza de red "Head End", la clave común Ki puede ser generada por el módulo de seguridad (SM). Este proceso es ejecutado independientemente de los mensajes de administración (EMM) siempre que los derechos incluidos en estos últimos sean válidos y permitan el desciframiento de los datos (DT) por la unidad de desciframiento (DMX). De hecho, el módulo de seguridad (SM), debido a que recibe los mensajes de control ECM comprendiendo las palabras de control (CW) incluidas en el flujo de datos (DT) de audio/vídeo, dispone de la información de un cambio de canal, lo que le permite generar una nueva clave común (Ki).

[0041] Cuando recibe los datos de audio/vídeo (DT) la unidad de desciframiento (DMX) los descifra con una palabra de control (CW) que el módulo de seguridad (SM) extrae de un mensaje de control ECM. Esta palabra de control (CW) es transmitida a la unidad de desciframiento (DMX) ya sea descifrada, ya sea encriptada por la clave personal Kec de la unidad de encriptación (EC) o por otra clave puesta a disposición de la unidad de desciframiento (DMX) por el programa personalizado "middleware" (MD).

[0042] Paralelamente, el módulo de seguridad obtiene una clave común (Ki) y encripta ésta con la clave personal (Kec) de la unidad de encriptación (EC). La clave (Ki) proviene bien de un mensaje de administración (EMM) o bien del propio módulo de seguridad que la genera, como se describe más arriba.

[0043] Este criptograma Kec(Ki) es transmitido a la unidad de encriptación (EC) que extrae de ésta la clave común (Ki) y con la cual reencripta los datos descifrados por la unidad de desciframiento (DMX).

[0044] Según una variante preferida, el método de control de acceso a los datos (DT) de audio/vídeo digitales recibidos por una unidad de tratamiento (UT) comprendiendo una unidad de desciframiento (DMX) de los datos de audio/vídeo, una unidad de descompresión (MPEG), una interfaz de entrada/salida de los datos de audio/vídeo tratados y medios de comunicación hacia un módulo de seguridad (SM), las unidades de desciframiento (DMX) y de descompresión (MPEG) comprendiendo respectivamente una unidad de encriptación (EC) y una unidad de desencriptación (DC) utilizando al menos una clave personal (Kec, Kdc) y una clave de encriptación común (Ki), está caracterizado por el hecho de que comprende las etapas siguientes:

- recepción de un mensaje de control (ECM) conteniendo una palabra de control (CW) por el módulo de seguridad (SM),

- obtención por el módulo de seguridad de una clave común Ki y generación de un criptograma Kec(Ki, CW, H(Ki, CW)) encriptado con la clave personal Kec de la unidad de encriptación (EC) comprendiendo la clave común (Ki), la palabra de control (CW), y una primera huella H(Ki, CW).

- transmisión del criptograma Kec(Ki, CW, H(Ki, CW)) a la unidad de desciframiento (DMX) desencriptación con la clave Kec de dicho criptograma y verificación de la integridad de la clave común Ki y de la palabra de control CW.

- carga de la clave común (Ki) en la unidad de encriptación (EC) y autorización del desciframiento de los datos de audio/vídeo con la palabra de control (CW) cuando el resultado de la verificación es positivo.

- desciframiento de los datos de audio/vídeo y encriptación de dichos datos por la unidad de encriptación (EC) con la clave común (Ki),

- transmisión de dichos datos reencriptados a la unidad de desencriptación (DC),

- selección por el módulo de seguridad de la clave común (Ki) específica a los datos de audio/vídeo,

- solicitud por el módulo de seguridad (SM), de un número aleatorio (AL) de la unidad de desencriptación (DC),

- formación y posterior transmisión de un criptograma Kdc(Ki, AL, H(Ki, AL)) encriptado con la clave personal (Kdc) de la unidad de desencriptación (DC) conteniendo al menos la clave común, (Ki) el número aleatorio (AL), y una segunda huella H(Ki, AL),

- recepción del criptograma Kdc(Ki, AL, H(Ki, AL)) por la unidad de desencriptación (DC)

- desencriptación de dicho criptograma con la clave personal Kdc de dicha unidad de desencriptación (DC) y verificación de la integridad de la clave común (Ki) y del número aleatorio (AL).

- cuando el resultado de la verificación es positivo, comparación del número aleatorio (AL) recibido con el previamente generado.

- carga de la clave común (Ki) y desencriptación de los datos de audio/vídeo si el resultado de la comparación es positiva.

[0045] El módulo de seguridad (SM) transmite la clave común (Ki) con la palabra de control (CW) todo ello encriptado por la clave personal (Kec) a la unidad de desciframiento (DMX) y a la unidad de encriptación (EC). Con el fin de asegurar su integridad, este criptograma Kec(Ki, CW) puede también incluir una huella H(Ki, CW) constituyendo un código de autentificación o MAC (Message Authentication Code). Este código es calculado a partir de la clave común (Ki) y de la palabra de control (CW), en general, con una función de comprobación aleatoria unidireccional del tipo MD2, MD4, MD5 (Message Digest) o SHA, (Secure Hash Algorithm). Cuando recibe el criptograma Kec(Ki, CW, H(Ki, CW)), el procesador protegido lo desencripta con la clave (Kec) luego calcula una huella H(Ki, CW))' a partir de la clave (Ki) y de la palabra de control (CW) recibidas y la compara con la huella H(Ki, CW) recibida. La clave (Ki) y la palabra de control (CW) sólo serán reconocidas como válidas si la comparación de la huella H(Ki, CW))' calculada con aquella H(Ki, CW) recibida da un resultado positivo. El procesador protegido es entonces autorizado a cargar la palabra de control en la unidad de desciframiento (DMX) así como la clave común en la unidad de encriptación (EC). Esto permite descifrar los datos de audio/vídeo con la palabra de control (CW) y encriptar los datos descifrados por la unidad de encriptación (EC).

[0046] Una ventaja del acoplamiento de la clave común (Ki) con la palabra de control (CW) es que hace imposible cruzar dos flujos entrantes en un descodificador equipado con dos sistemas de recepción o "tuner". La clave común Ki de un flujo autorizando una desencriptación gratuita no podrá reemplazar la clave común Ki de un flujo comportando derechos restringidos. El cruce de los dos mensajes tendría como consecuencia que las palabras de control sean igualmente cruzadas. Otra palabra de control distinta a la esperada tiene como resultado hacer el desciframiento nulo.

[0047] Esta variante es particularmente pertinente cuando se carga la clave de encriptación y desencriptación en una misma operación. En modo directo, es posible no aplicar el protocolo implementando una variable aleatoria para cargar la clave común en la unidad de desencriptación (DC). El procesador protegido, encargado de las operaciones de seguridad en la unidad de tratamiento de la invención, recibe un mensaje encriptado por su clave personal conteniendo la palabra de control y la clave común Ki. Esta clave es cargada simultáneamente en la unidad de encriptación y la unidad de desencriptación. Con el fin de asegurarse que se ha cargado la clave buena y no que un programa interfaz ha reemplazado un mensaje por otro, la presencia de la palabra de control prohíbe todo cambio de mensaje. Si se quiere obtener el flujo descifrado, sólo el mensaje original podrá ser utilizado.

[0048] Cabe señalar que en una implementación que aplique un procesador protegido o un procesador central disponiendo de un modo protegido, la clave personal (Kec) de la unidad de encriptación (EC) y de la unidad de desencriptación (DC) es idéntica y es de hecho la clave personal del procesador protegido.

[0049] Los datos reencriptados por la unidad de encriptación (EC) con la clave común (Ki) son por ejemplo almacenados en un disco duro (HD) o en una memoria no volátil (EEPROM) para ser desencriptados ulteriormente. El módulo de seguridad (SM) crea un criptograma KL(Ki, ID) compuesto por la clave común (Ki) y un identificador (ID) del contenido (C), todo ello encriptado por una clave local (KL) del módulo de seguridad (SM). Este criptograma puede ser almacenado ya sea en el disco duro (HD) con el contenido encriptado con la clave común (Ki) ya sea en el módulo de seguridad (SM) o en una memoria separada.

[0050] Cabe señalar que este criptograma puede ser encriptado con otras claves personales como por ejemplo la clave personal (Kec) de la unidad de encriptación (EC) o aquella (Kdc) de la unidad de desencriptación (DC) que son conocidas por el módulo de seguridad (SM).

[0051] Estos datos reencriptados pueden igualmente ser encaminados hacia una red local (LAN) a través del puerto (P) para su tratamiento, visualización inmediata o diferida. En este último caso, los datos son memorizados en un disco duro u otra unidad de memoria de una unidad de tratamiento o descodificador miembro de la red local (LAN). Su desencriptación será por lo tanto efectuada por una unidad de tratamiento o descodificador diferente a aquel que los ha encriptado.

[0052] Durante la lectura del contenido encriptado Ki(C) almacenado en el disco duro (HD), el criptograma KL(Ki, ID) es transmitido por el programa personalizado "middleware" (MD) al módulo de seguridad (SM) que lo desencripta utilizando la clave (KL) para extraer de éste el identificador (ID). Éste es interpretado por el módulo de seguridad que determina un parámetro relativo a la utilización de los datos de audio/vídeo almacenados que corresponden, por ejemplo, al número de lecturas autorizadas del contenido (C) una vez desencriptado. Luego el módulo de seguridad (SM) envía una orden a la unidad de desencriptación (DC) que genera un número aleatorio o variable aleatoria (AL) y lo transmite al módulo de seguridad (SM). Este último prepara un nuevo criptograma Kdc(Ki, AL) compuesto por la variable aleatoria (AL) y la clave común (Ki) previamente extraída del criptograma KL(Ki, ID), todo ello encriptado por la clave personal (Kdc) de la unidad de desencriptación (DC). Este criptograma Kdc(Ki, AL) es transmitido a la unidad de desencriptación (DC) que lo desencripta con su clave personal (Kdc). La variable aleatoria (AL) recibida y extraída del criptograma Kdc(Ki, AL) es entonces comparada con la variable aleatoria (AL) generada previamente. Si las dos variable aleatorias (AL) corresponden, la clave común (Ki) es considerada como válida. Ésta es entonces cargada en la unidad de desencriptación (DC) que obtiene de este modo el contenido (C) descifrado. La unidad de descompresión (MPEG) descomprime el contenido (C) obtenido y lo convierte en una señal de audio/vídeo (AV) analógica del tipo banda de base (video compuesto, RGB) compatible con un televisor por ejemplo.

[0053] En los sistemas descritos en los documentos citados US6286103 y WO00/57636, el número aleatorio desempeña respectivamente un papel de asegurar la transmisión de datos entre el módulo de seguridad y el aparato y un papel de la verificación de la autenticidad del módulo de seguridad. En la actual invención, se utiliza para verificar la validez (o la antigüedad) de la clave común permitiendo descifrando los datos para prevenir la copia no-autorizada de los datos cifrados con una clave que deba ser caducada. Además, el hecho de solicitar el módulo de seguridad en cada desciframiento asegura una seguridad a los datos incluso que el aparato no es confiable. En hecho, la clave común es bien generada, bien controlada después de la recepción de un mensaje EMM de la administración por el módulo de seguridad solamente.

[0054] Según una variante, el número aleatorio (AL) generado por la unidad de desencriptación (DC) puede ser transmitido en forma encriptada con la clave personal (Kdc) de dicha unidad de desencriptación (DC). Al poseer el módulo de seguridad (SM) esta clave personal Kdc, podrá desencriptar la variable aleatoria (AL) para formar el criptograma Kdc(Ki, AL). Con el fin de asegurar su integridad, el número aleatorio (AL) puede igualmente ser transmitido acompañado de una huella H(AL) calculada a partir de dicho número aleatorio (AL), este conjunto siendo encriptado con la clave personal (Kdc) de la unidad de desencriptación (DC).

[0055] Según otra variante, el criptograma Kdc(Ki, AL) incluye una huella H(Ki, AL) calculada por el módulo de seguridad (SM) a partir de la clave común (Ki) y del número aleatorio (AL) para formar el criptograma Kdc(Ki, AL, H(Ki, AL)). Cuando este criptograma es recibido por la unidad de desencriptación (DC), ésta verifica antes de todo la huella H(Ki, AL) por comparación con una huella H(Ki, AL)' que calcula con la clave (Ki) y el número (AL) extraídos del

criptograma y la huella H(Ki, AL) extraída del criptograma. Si los resultados de esta comparación y aquella de los números aleatorios (AL), como se describe más arriba, son positivos, la clave común (Ki) es cargada en la unidad de desencriptación (DC) y la desencriptación del contenido puede ejecutarse.

[0056] En una variante, el criptograma K_L(Ki, ID) acompañando el contenido Ki(C) almacenado puede incluir otras informaciones relativas al contenido (C) como por ejemplo un título T, la duración D o un código N describiendo el tipo de contenido (deporte, película, reportaje etcétera…). El criptograma puede ser simbolizado por K_L(Ki, ID, T, D, N).

[0057] La ventaja de un tal criptograma K_L(Ki, ID, T, D, N) es la posibilidad de gestionar los derechos de un contenido en función de su naturaleza y del tiempo. De hecho, el identificador (ID), y el código (N) por ejemplo, permite al módulo de seguridad limitar el número de visualizaciones.

[0058] Durante la visualización directa o "en directo" de un contenido, es decir, sin registro duradero en una unidad de memoria, la unidad de tratamiento descifra el contenido con ayuda de la palabra de control (CW), luego lo encripta con la clave común (Ki) para desencriptarlo directamente antes de la descompresión. Durante una primera etapa, el módulo de seguridad (SM) almacena la palabra de control (CW) y un identificador (ID) del contenido (C) para determinar si la desencriptación con la clave común (Ki) puede tener lugar o no según los derechos contenidos en el módulo de seguridad (SM).

[0059] En este modo "en directo", la clave común (Ki), obtenida por el módulo de seguridad (SM), es transmitida a la vez a la unidad de encriptación (EC) y a la unidad de desencriptación (DC). Esta clave Ki es transmitida bien en forma encriptada con las claves personales (Kec, Kdc) de las unidades respectivas (EC, DC) o bien encriptada con la clave (Kec) de la unidad de encriptación (EC) únicamente. En este último caso, es transmitida a la unidad de desencriptación (DC) por una conexión (CS) material directa protegida conectando dicha unidad de desencriptación (DC) a la unidad de encriptación (EC). La etapa de control que utiliza el número aleatorio (AL) como en el modo de lectura de datos almacenados ya no es necesaria porque la unidad de desencriptación (DC) recibe la clave (Ki) de una fuente segura.

REIVINDICACIONES

1. Unidad de tratamiento (UT) de datos de audio/vídeo digitales encriptados con palabras de control (CW) que provienen de mensajes de control (ECM) que comprende una unidad de desciframiento (DMX) de los datos de audio/vídeo, (DT) una unidad de descompresión (MPEG), una interfaz de entrada/salida de los datos de audio/vídeo tratados y medios de comunicación hacia un módulo de seguridad (SM), las unidades de desciframiento (DMX) y de descompresión (MPEG) comprendiendo respectivamente una unidad de encriptación (EC) y una unidad de desencriptación (DC) disponiendo cada una de por lo menos una clave personal (Kec, Kdc) y de una clave de encriptación común (Ki), caracterizada por el hecho de que comporta

- medios de transmisión protegida de la clave común (Ki) y de la contraseña de control (CW) extraída de un mensaje de control (ECM) entre el módulo de seguridad (SM), la unidad de desciframiento (DMX) y la unidad de encriptación (EC), dichos medios de transmisión forman un criptograma Kec(Ki, CW, H(Ki, CW)) utilizando una clave personal (Kec) de la unidad de encriptación (EC) que encripta la clave común (Ki), la palabra de control (CW), y una huella H(Ki, CW) obtenida por una función de comprobación aleatoria unidireccional, que sirven para la verificación de la integridad de la clave común (Ki) y de la palabra de control (CW) después de la desencriptación de dicho criptograma Kec(Ki, CW, H(Ki, CW)) con la clave (Kec) personal de la unidad de encriptación (EC), la clave común (Ki) que es cargada en la unidad de encriptación (EC) solamente si el resultado de la verificación es positivo,

- medios para reencriptar datos de audio/video (DT) con la palabra de control (CW) asociados a la unidad de desciframiento (DMX),

- medios para reencriptar dichos datos descifrados con la clave común (Ki) asociados a la unidad de encriptación (EC),

- una unidad de memoria (RAM, HD) capaz de almacenar temporalmente los datos de audio/vídeo (DT) reencriptados con la clave común (Ki),

- medios de transmisión protegida de los datos de audio/vídeo (DT) reencriptados a la unidad de desencriptación (DC) aptos para comunicarse con el módulo de seguridad (SM) y con un generador de números aleatorios (AL) asociado a la unidad de desencriptación (DC), dichos medios utilizando la clave personal (Kdc) de la unidad de desencriptación (DC).

- medios de verificación de la integridad del número aleatorio (AL), dichos medios autorizando, cuando el resultado de la verificación es positivo, la desencriptación por la unidad de desencriptación (DC) de los datos de audio/vídeo (DT) con la clave común (Ki).

2. Unidad de tratamiento según la reivindicación 1, **caracterizada por el hecho de que** comprende los medios de bloqueo inmediato o diferido de la unidad de desencriptación (DC) cuando el resultado de la verificación es negativo.

3. Unidad de tratamiento según la reivindicación 1, **caracterizada por el hecho de que** comprende un procesador que incluye un ámbito de ejecución protegido implementado en la parte material del corazón de dicho procesador, los datos y el código protegido siendo marcados y divididos, manteniendo una separación material diferenciada entre los datos protegidos y no protegidos en dicha unidad de tratamiento.

4. Unidad de tratamiento según la reivindicación 1, **caracterizada por el hecho de que** incluye dos procesadores, el primero que ejecuta el código protegido es aislado de todo acceso proveniente del exterior y por otra parte de un control no autorizado del segundo procesador no protegido.

5. Unidad de tratamiento según la reivindicación 1, **caracterizada por el hecho de que** las unidades de desciframiento (DMX) y de descompresión (MPEG) tienen cada una un procesador independiente del procesador central (CPU), dirigido por un programa personalizado "middleware" (MD) comprendiendo medios de gestión de los accesos y de los intercambios de datos efectuados por la unidad de encriptación (EC) y por la unidad de desencriptación (DC) de y hacia la unidad de memoria (RAM, HD).

6. Unidad de tratamiento según la reivindicación 1, **caracterizado por el hecho de que** las unidades de encriptación (EC) y de desencriptación (DC) son implementadas en forma de elementos materiales (hardware) en las unidades de descifrado (DMX) y de descompresión (MPEG).

7. Unidad de tratamiento según la reivindicación 1, **caracterizada por el hecho de que** las unidades de encriptación (EC) y de desencriptación (DC) son implementadas en forma de microcódigo gestionado por los procesadores de las unidades de descifrado (DMX) y de descompresión (MPEG).

8. Unidad de tratamiento según la reivindicación 1, **caracterizada por el hecho de que** la interfaz de entrada/salida está conectada a un bus (B) al cual están conectadas las unidades de encriptación (EC) y de desencriptación (DC) y la unidad de memoria constituida por al menos una memoria (RAM) con acceso aleatorio de almacenamiento intermediario de los datos en curso de tratamiento y/o un disco duro (HD).

9. Unidad de tratamiento según la reivindicación 8, **caracterizada por el hecho de que** la interfaz de entrada/salida, conectada al bus (B), incluye un puerto (P) de entrada/salida hacia una red local a la cual son conducidos los datos encriptados por la unidad de encriptación (EC).

10. Unidad de tratamiento según la reivindicación 1, **caracterizada por el hecho de que** forma un módulo integrado en un ordenador personal.

11. Unidad de tratamiento según la reivindicación 1, **caracterizada por el hecho de que** forma un módulo integrado en un descodificador de televisión de pago.

12. Método de control de acceso a los datos (DT) de audio/vídeo digitales recibidos por una unidad de tratamiento (UT) que comprende una unidad de desciframiento (DMX) de los datos de audio/vídeo, una unidad de descompresión (MPEG), una interfaz de entrada/salida de los datos de audio/vídeo tratados y medios de comunicación hacia un módulo de seguridad (SM), las unidades de desciframiento (DMX) y de descompresión (MPEG) comprendiendo respectivamente una unidad de encriptación (EC) y una unidad de desencriptación (DC) utilizando al menos una clave personal (Kec, Kdc) y una clave de encriptación común (Ki), **caracterizado por el hecho de que** comprende las etapas siguientes:

- recepción de un mensaje de control (ECM) que contiene por lo menos una palabra de control (CW) por el módulo de seguridad (SM),

- obtención por el módulo de seguridad de una clave común (Ki) y generación de un criptograma Kec(Ki, CW, H(Ki, CW)) que incluye la clave común (Ki), la palabra de control (CW), y una huella H(Ki, CW), obtenida por una función de comprobación aleatoria unidireccional, encriptados con la clave personal (Kec) de la unidad de encriptación (EC), dicha huella H(Ki, CW) que sirve para la verificación de la integridad de la clave común Ki y de la palabra de control CW después de la desencriptación de dicho criptograma Kec(Ki, CW, H(Ki, CW)) con la clave (Kec) personal de la unidad de encriptación (EC), la clave común (Ki) estando cargada en la unidad de encriptación (EC) solamente si el resultado de la verificación es positivo

- transmisión del criptograma Kec(Ki, CW) a la unidad de desciframiento (DMX), desencriptación con la clave (Kec) de dicho criptograma,

- carga de la clave común (Ki) en la unidad de encriptación (EC) y autorización del desciframiento de los datos de audio/vídeo (DT) con la palabra de control (CW),

- desciframiento de los datos de audio/vídeo (DT) y encriptación de dichos datos por la unidad de encriptación (EC) con la clave común (Ki),

- transmisión de dichos datos de audio/vídeo (DT) reencriptados a la unidad de desencriptación (DC),

- selección por el módulo de seguridad de la clave común (Ki) específica de los datos de audio/vídeo (DT),

- transmisión por la unidad de desencriptación (DC) de un número aleatorio (AL) al módulo de seguridad (SM),

- formación y posterior transmisión de un criptograma Kdc(Ki, AL) encriptado con la clave personal (Kdc) de la unidad de desencriptación (DC) conteniendo al menos la clave común, (Ki) y el número aleatorio (AL),

- recepción del criptograma Kdc(Ki, AL) por la unidad de desencriptación (DC),

- desencriptación de dicho criptograma con la clave personal (Kdc) de dicha unidad de desencriptación (DC) y verificación de la integridad del número aleatorio (AL) comparando el número aleatorio (AL) recibido con aquel previamente generado.

- carga de la clave común (Ki) y desencriptación de los datos de audio/vídeo (DT) si el resultado de la comparación es positivo.

13. Método según la reivindicación 12 **caracterizado por el hecho de que** el criptograma Kdc(Ki, AL) encriptado con la clave (Kdc) personal de la unidad de desencriptación (DC) incluye más de una huella H(Ki, AL) que sirve para la verificación de la integridad de la clave común Ki y del número aleatorio (AL) después de la desencriptación de dicho criptograma Kdc(Ki, AL) con la clave (Kdc) personal de la unidad de desencriptación (DC), el número aleatorio (AL) recibido estando comparado con el previamente generado solamente si el resultado de la verificación es positivo.

14. Método según la reivindicación 12 **caracterizado por el hecho de que** cuando el resultado de la comparación es negativo, la unidad de desencriptación (DC) es bloqueada ya sea inmediatamente, ya sea después de la desencriptación de un número predeterminado de bloques de datos audio/vídeo.

15. Método según la reivindicacion 12 o 13 **caracterizado por el hecho de que** la primera huella H(Ki, CW) y la segunda huella H(Ki, AL) constituyen respectivamente un primer código de autentificación calculado a partir de la clave común (Ki) y de la palabra de control (CW) y un segundo código de autentificación calculado a partir de la clave común (Ki) y del número aleatorio (AL), dichos códigos siendo calculados con una función de comprobación aleatoria unidireccional.

16. Método según la reivindicación 12 **caracterizado por el hecho de que** la clave común (Ki) es generada por el módulo de seguridad (SM).

17. Método según la reivindicación 12 caracterizado por el hecho de que la clave común (Ki) es extraída de un mensaje de administración (EMM) proveniente de un centro de gestión.

18. Método según la reivindicación 12 **caracterizado por el hecho de que** los datos descifrados y reencriptados por la clave común (Ki) son almacenados en una unidad de memoria (RAM, HD), efectuándose su desencriptación ulteriormente.

19. Método según la reivindicación 12 **caracterizado por el hecho de que** los datos descifrados y reencriptados por la clave común (Ki) son encaminados hacia una red local (LAN) a través de un puerto (P) de la unidad de tratamiento, efectuándose su desencriptación inmediata o diferida por una unidad de tratamiento miembro de dicha red local (LAN).

20. Método según la reivindicación 12 **caracterizado por el hecho de que** durante la transmisión de los datos de audio/vídeo (DT) hacia la unidad de desencriptación (DC), el módulo de seguridad crea y almacena un criptograma de control KL(Ki, ID) encriptado por una clave local (KL) de dicho módulo de seguridad (SM) conteniendo al menos un identificador (ID) de los datos de audio/vídeo y la clave común (Ki), dicha clave (Ki) se selecciona desencriptando el criptograma de control con la clave local (KL), y el identificador (ID) siendo leído por el módulo de seguridad (SM) que determina un parámetro relativo a la utilización de los datos de audio/vídeo almacenados.

21. Método según la reivindicación 20 **caracterizado por el hecho de que** el criptograma de control KL(Ki, ID) es almacenado en el módulo de seguridad (SM).

22. Método según la reivindicación 20 **caracterizado por el hecho de que** el criptograma de control KL(Ki, ID) es almacenado en la unidad de memoria (RAM, HD) y acompaña los datos de audio/vídeo encriptados.

23. Método según la reivindicación 20 **caracterizado por el hecho de que** el criptograma de control KL(Ki, ID) encriptado por la clave local (KL) del módulo de seguridad (SM) y conteniendo la clave común (Ki) incluye las informaciones adicionales relativas a la naturaleza y al tipo de los datos de audio/vídeo (DT) almacenados en la unidad de memoria (RAM, HD).

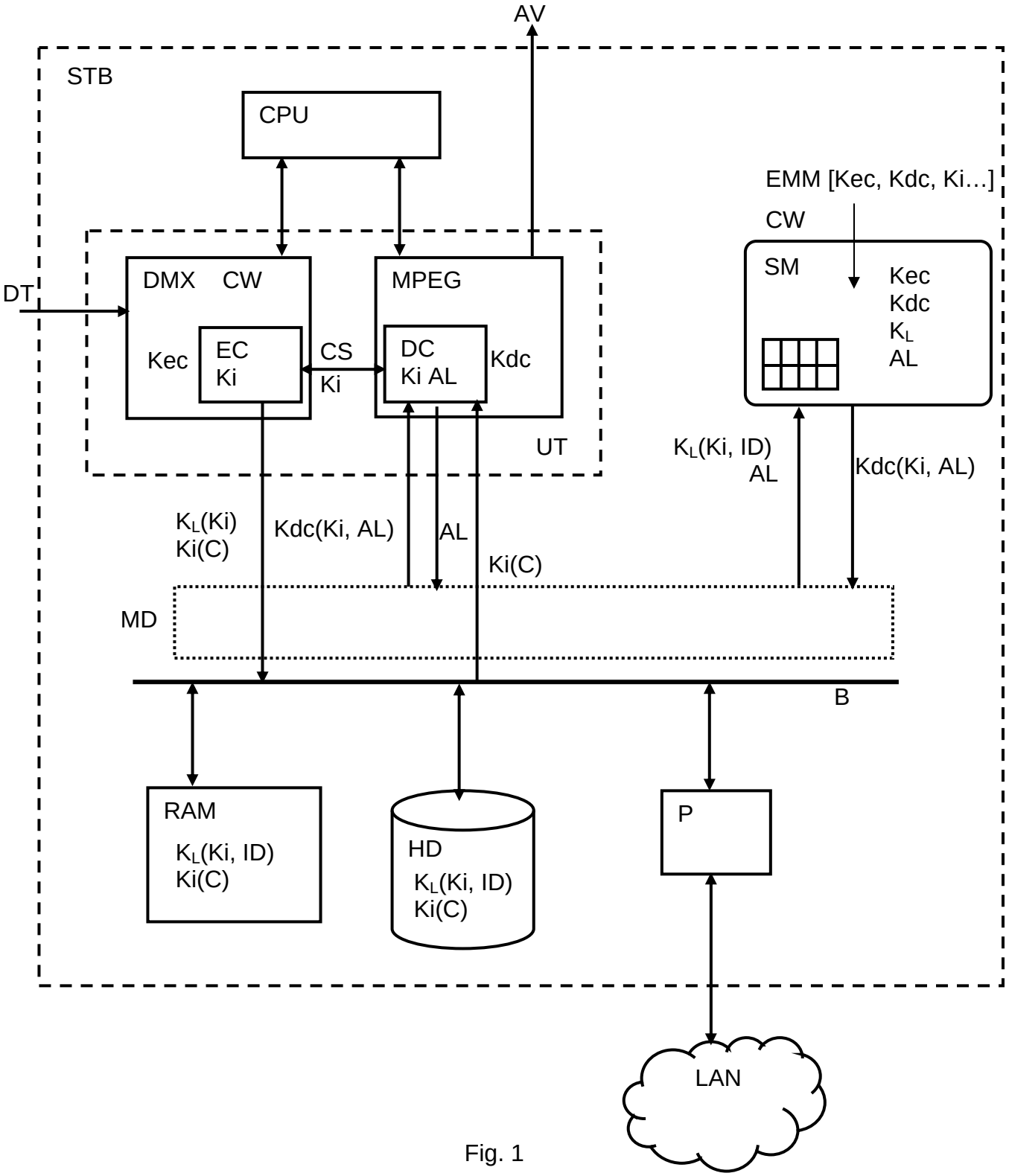
AV
STB
CPU
EMM [Kec, Kdc, Ki…]
CW
SM
Kec
Kdc
K_L
AL
DT
DMX CW
Kec
EC
Ki
CS
Ki
MPEG
DC
Ki AL
Kdc
UT
K_L(Ki, ID)
AL
Kdc(Ki, AL)
K_L(Ki)
Ki(C)
Kdc(Ki, AL)
AL
Ki(C)
MD
B
RAM
K_L(Ki, ID)
Ki(C)
HD
K_L(Ki, ID)
Ki(C)
P
LAN

Fig. 1