(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 527 539**

(51) Int. CI.:

***G06F 21/10*** (2013.01)
***H04L 9/08*** (2006.01)
***H04N 21/2347*** (2011.01)
***H04N 21/266*** (2011.01)
***H04N 21/4405*** (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.07.2011 E 11733872 (3)**

(97) Fecha y número de publicación de la concesión europea: **15.10.2014 EP 2596450**

(54) Título: **Procedimiento de protección de un contenido**

(30) Prioridad:

**22.07.2010 FR 1056000**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**26.01.2015**

(73) Titular/es:

**VIACCESS (100.0%)**
**Les Collines de l'Arche Tour Opéra C**
**92057 Paris La Défense, FR**

(72) Inventor/es:

**NEAU, LOUIS**

(74) Agente/Representante:

**LINAGE GONZÁLEZ, Rafael**

## DESCRIPCIÓN

Procedimiento de protección de un contenido

**Campo técnico**

La invención se sitúa en el campo de la protección de contenidos, y se refiere más en particular a un procedimiento de protección de un contenido a distribuir en un parque de terminales de recepción conectados a una red de distribución de contenido y cada uno de los cuales tiene un nivel de seguridad específico dependiente de los medios técnicos de seguridad utilizados. El procedimiento según la invención plantea más específicamente acondicionar un nivel de seguridad predeterminado, la descodificación de dicho contenido, e incluye las etapas siguientes:

• en la emisión:

- generar una clave de codificación de dicho contenido,

- transformar la citada clave de codificación mediante un primer módulo de cálculo dispuesto en la cabecera de dicha red de distribución de contenido,

- codificar el contenido por medio de la clave transformada,

- transmitir el contenido codificado y la clave de codificación a los terminales, y

• en la recepción de dicho contenido y de la clave de codificación por parte de un terminal:

- transformar la citada clave de codificación por medio de un segundo módulo de cálculo dispuesto en el citado terminal,

- descodificar el contenido con la clave de codificación transformada.

El procedimiento según la invención se lleva a cabo por medio de un dispositivo que comprende:

- medios para generar una clave de codificación de dicho contenido,

- medios para transformar la citada clave de codificación mediante un primer módulo de cálculo dispuesto en la cabecera de dicha red de distribución de contenido,

- medios para codificar el contenido por medio de la clave transformada,

- medios para transformar el contenido codificado y la clave de codificación en los terminales, y

- medios para transformar la citada clave de codificación por medio de un segundo módulo de cálculo dispuesto en el citado terminal,

- medios para descodificar el contenido con la clave de codificación transformada.

La invención se refiere igualmente a un terminal de recepción de un contenido distribuido en forma codificada por medio de una clave de codificación transformada previamente mediante el procedimiento según la invención.

La invención se refiere también a un programa de ordenador memorizado en un soporte de registro y destinado, cuando se ejecuta por medio del ordenador, a llevar a cabo el procedimiento según la invención.

**Estado de la técnica anterior**

El aumento creciente de consumo de transmisión de datos por Internet ofrece a los operadores de servicios nuevas perspectivas en cuanto a la distribución de contenidos audiovisuales.

En la actualidad, en particular en el mercado de la IPTV, un gran número de operadores de servicios aspiran a ofrecer los mismos contenidos MPEG2-TS tanto a terminales de recepción de tipo PC como a terminales convencionales dotados de un descodificador (STB, acrónimo de Set Top Box). En estas condiciones, la norma DVB-CSA (acrónimo de Digital Video Broadcasting-Common Scrambling Algorithm) se ve como un freno al desarrollo de los servicios sobre nuevos terminales, puesto que al contrario que el estándar AES (Advanced Encryption Standard) por ejemplo, aquélla impone un elemento material complementario para la descodificación de los contenidos (por ejemplo, un descifrador DVB-CSA), típicamente una clave USB. El estándar AES se considera por lo tanto como una alternativa a la norma DVB-CSA para proteger contenidos de pago.

Uno de los riesgos consiste en ayudar a una segmentación o verticalización del mercado en función de los algoritmos implementados por cada uno de los diferentes actores, y a una pérdida de interoperabilidad en detrimento, a plazo, de los propios operadores de servicios.

Por otra parte, los operadores de servicios están obligados a respetar las condiciones de seguridad exigidas por los proveedores de programas. En efecto, estos último pueden imponer el hecho de que ciertos contenidos o ciertas calidades de contenidos, tales como por ejemplo los programas difundidos en calidad HD (Alta Definición) en 3D, no pueden ser accesibles en terminales de baja seguridad tal como los PCs, por ejemplo.

Además, los algoritmos de codificación utilizables para la protección de los contenidos MPEG2-TS son potencialmente múltiples y son susceptibles de variar en función de los terminales objetivados por el operador de servicios. Esto puede generar una complejidad y un coste suplementarios, especialmente para el operador de servicios con relación a las exigencias de los titulares de derechos e intereses industriales.

Si un algoritmo de codificación único fuera retenido para poder objetivar el conjunto de terminales, debería estar basado en una implementación lógica, típicamente una realización del AES. O en su caso, los titulares de derechos desean, según el tipo de contenido, poder hacer una diferenciación entre terminales que dispongan de la combinación de varios medios técnicos de seguridad, típicamente hardware, y los demás, con el fin de evitar poner en peligro su modelo económico.

En esta última hipótesis, una solución a ese problema consiste en discriminar los terminales, de modo que aquellos que no dispongan de los medios técnicos de seguridad requeridos, no puedan acceder a los contenidos protegidos. Esta solución puede generar períodos de pantalla en negro, a menos que se propongan múltiples canales de distribución de contenidos que tengan en cuenta la diversidad de terminales de recepción.

Un objeto de la invención es el de permitir que los operadores de servicio utilicen una solución única para codificar los contenidos distribuidos adaptables a terminales de recepción que tengan niveles de seguridad específica diferentes.

El nivel de seguridad específica de un terminal está definido por los medios técnicos usados en el terminal de recepción. Así, un terminal dotado de una clave USB destinado a descodificar el contenido tendrá un nivel de seguridad diferente del nivel de un terminal PC en el que la descodificación de un contenido se obtiene únicamente mediante una lógica.

Para una mejor comprensión en relación con la terminología propia de los dominios técnicos CAS y DRM, el lector puede remitirse, por ejemplo, a los documentos siguientes:

- sobre los sistemas de acceso condicional, “Functional Model of Conditional Access System”, EBU Review, Technical European Broadcasting Union, Bruselas, BE, núm. 266, 21 de Diciembre de 995;

- sobre los sistemas de gestión de derechos digitales, “DRM Specification”, Open Mobile Alliance OMA-TS-DRM-DRM-V2_0_2-20080723-A, Versión aprobada 2.0.2 – 23 de Julio de 2008.

Para simplificar la comprensión de la invención, se denominará de forma genérica “Agente DRM”:

- los componentes CAS o DRM de la cabecera de red que aseguran la construcción de las Licencias o de los ECM que protegen la clave del contenido codificado y lo asocian a las condiciones relativas al acceso al contenido,

- los componentes CAS o DRM en los terminales que aseguran el acceso a las Licencias o a los ECM que protegen la clave del contenido codificado y que controlan el acceso a esta clave según las condiciones relativas al acceso al contenido.

Por otra parte, el documento EP-1575292-A1 divulga un método de provisión de seguridad a un contenido cifrado transmitido por un difusor en un contexto de televisión de pago. Este método pone en práctica derechos de acceso al contenido gestionados por medio de EMM (Entitlement Management Message) y por medio de mensajes de control de tipo ECM.

**Exposición de la invención**

La invención preconiza entonces un procedimiento de protección de un contenido a distribuir en un parque de terminales de recepción conectados a una red de distribución de contenido y donde cada uno de ellos tiene un nivel de seguridad específico que depende de los medios técnicos de seguridad utilizados, que incluye además las etapas de:

en la emisión:

- aplicar a dicha clave de codificación, por medio de dicho primer módulo de cálculo, una función F definida en función de dicho nivel de seguridad específico,

y en la recepción:

- aplicar a dicha clave de codificación, por medio de dicho segundo módulo de cálculo, una función F definida en función de dicho nivel de seguridad específico.

Según la invención, los citados primer y segundo módulos de cálculo incluyen una o varias funciones Fi de transformación de la citada clave de codificación, correspondiendo cada función Fi a un nivel de seguridad Ni dado. Los medios técnicos de seguridad que definen los niveles de seguridad Ni en relación con las funciones Fi son software o bien materiales e incluyen al menos una de las características siguientes en el terminal:

- almacenaje de la clave de codificación en forma cifrada en una memoria no volátil del terminal,

- almacenaje del código aplicativo del terminal en forma cifrada en una memoria no volátil del terminal,

- cargo en la memoria volátil de dicho terminal del código aplicativo cifrado durante su ejecución,

- oscurecimiento de dicho código.

Según la invención, se entiende por primer y segundo módulo de cálculo todo componente material y lógico que lleve a cabo las funciones F o Fi respectivamente durante la emisión en cabecera de red y durante la recepción en el terminal.

Con preferencia, la clave de codificación es transmitida a los terminales cifrada por medio de un ECM o de una licencia, y la aplicación de la función F a la clave de codificación está pilotada por el operador a través de una señalización PMT (Program Mapping Table). En caso de que se hayan definido varios niveles de seguridad Ni, las informaciones de la PMT indican si una función Fi está lista para ser aplicada y en caso afirmativo, su identificación.

En un modo preferido de realización del procedimiento conforme a la invención, el citado segundo módulo de cálculo incluye varias funciones Fi de transformación de la citada clave de codificación, correspondiendo cada función Fi a un nivel de seguridad Ni dado que varía entre un nivel mínimo de seguridad y un nivel máximo de seguridad que corresponde al nivel de seguridad específico del terminal.

A título de ejemplo, la función F es una función de sentido único tal como la codificación de una clave por sí misma con un algoritmo AES o TDES.

En una aplicación particular del procedimiento según la invención, el contenido a distribuir es un flujo digital que incluye un componente de base que necesita el nivel mínimo de seguridad y al menos un componente suplementario que necesita un nivel superior de seguridad. En tal caso, la codificación del contenido por medio de la clave de codificación transformada se aplica ya sea globalmente a todos los componentes del flujo, o ya sea de forma selectiva a cada componente del flujo.

El procedimiento según la invención se lleva a cabo por medio de un dispositivo emisor de un contenido a distribuir en un parque de terminales de recepción (4, 8, 70), conectados a una red de distribución de contenido y cada uno de los cuales tiene un nivel de seguridad específico que depende de los medios técnicos de seguridad utilizados, incluyendo el dispositivo un generador (16) de clave de codificación de dicho contenido, un codificador de contenido por medio de la clave transformada, medios para transmitir el contenido codificado y la clave de codificación a los terminales, incluyendo además este dispositivo una o varias funciones Fi de transformación de la citada clave de codificación K, correspondiendo cada función Fi a un nivel de seguridad Ni dado.

El procedimiento según la invención se aplica a un terminal de recepción de un contenido perteneciente a un parque de terminales de recepción conectados a una red de distribución de contenido y cada uno de los cuales tiene un nivel de seguridad específica que depende de los medios técnicos de seguridad utilizados, siendo el citado contenido distribuido en forma codificada por medio de una clave de codificación previamente transformada por un primer módulo de cálculo dispuesto la cabecera de la red. El terminal según la invención incluye un segundo módulo de cálculo destinado a aplicar a la citada clave de codificación una transformación que permita encontrar la clave transformada utilizada en la emisión para codificar el contenido transmitido.

Este terminal incluye un programa de ordenador memorizado en un soporte de registro y que incluye instrucciones para realizar, cuando se ejecuta en un ordenador, las etapas del procedimiento según la invención.

El procedimiento según la invención se pone en práctica durante la emisión mediante un programa de ordenador memorizado en su soporte de registro y que incluye las instrucciones para calcular, cuando son ejecutadas por un ordenador, una clave de codificación transformada por medio de una función F.

Además, en el lado de recepción, el procedimiento según la invención se lleva a cabo por medio de un programa de ordenador memorizado en un soporte de registro y que incluye instrucciones para encontrar, cuando se ejecutan mediante un ordenador, la clave de codificación transformada en la emisión por medio de la citada función F.

**Breve descripción de los dibujos**

Otras características y ventajas de la invención se pondrán de relieve a partir de la descripción que sigue, tomada a título de ejemplo no limitativo, con referencia a las figuras anexas, en las que:

- la figura 1 ilustra esquemáticamente una arquitectura de distribución de un contenido protegido usando el procedimiento según la invención, y

- la figura 2 ilustra esquemáticamente un ejemplo de aplicación del procedimiento según la invención en el caso de un contenido protegido distribuido en transmisión adaptativa.

**Exposición detallada de modos de realización particulares**

La figura 1 ilustra esquemáticamente una arquitectura de distribución de un contenido protegido que incluye una plataforma 2 de acondicionamiento del contenido a distribuir dispuesta en la cabecera de la red, un primer terminal receptor 4 dotado de un módulo de descodificación 6 de bajo nivel de seguridad, y un segundo terminal receptor 8 dotado de un módulo de descodificación 10 de nivel de seguridad elevado con relación al del primer terminal receptor 4. La plataforma 2 incluye además una memoria 12 destinada al almacenamiento del contenido a distribuir, un generador de señalización PMT (Program Mapping Table) 14, un generador de clave de codificación 16, un agente DRM (acrónimo de Digital Right Management) 18, y un módulo de codificación 20 que incluye un codificador 22, un selector de clave de codificación 24, y un primer módulo de cálculo 26 que incluye varias funciones Fi de transformación de la citada clave de codificación, correspondiendo cada función Fi a un nivel de seguridad Ni dado específico de uno de los terminales de recepción 4, 8.

El primer terminal receptor 4 incluye además un descodificador 28, un agente DRM 30 y una memoria 32 destinada al almacenamiento del contenido en forma descodificada. El segundo terminal receptor 8 incluye asimismo un descodificador 34, un agente DRM 36, una memoria 38 destinada al almacenamiento del contenido en forma descodificada, y un segundo módulo de cálculo 40 que incluye las funciones Fi de transformación de la citada clave codificada, correspondiendo cada función Fi a un nivel de seguridad Ni dado.

En funcionamiento, durante la emisión, el generador 14 genera una clave K de codificación del contenido a distribuir, y transmite la clave K generada al agente DRM 18 para codificar el contenido por medio de la clave K.

El generador de señalización PMT (Program Mapping Table) 14 transmite al selector de clave de codificación 24 el identificador de una función F a aplicar a la clave K para transformarla con anterioridad a la codificación del contenido. La función F se define en función del nivel de seguridad específica en el módulo de descodificación del terminal de recepción destinado a recibir el contenido.

Tras la aplicación de la función F a la clave K, el primer módulo de cálculo 26 proporciona al codificador 22 una clave transformada F(K) que servirá para codificar el contenido. El contenido codificado se proporciona a continuación a un módulo de transmisión 50 para ser transmitido a los terminales 4 y 8. La clave de codificación es transmitida asimismo, en forma cifrada, a los terminales por medio de un ECM o de una licencia.

En el lado de recepción, el terminal 4 no dispone de módulo de cálculo de la función F, ni podrá generar la clave transformada F(K) que ha servido para codificar el contenido en la cabecera de red y por consiguiente, el descodificador 6 no podrá descifrar el contenido recibido. Por el contrario, el terminal 8, que dispone de un segundo módulo de cálculo 40 podrá, tras la recepción de la señalización PMT que permite identificar la función F utilizada por el primer módulo de cálculo 26, generar la clave transformada F(K) y descodificar el contenido por medio de esa clave transformada.

Debe apreciarse que los citados primer y segundo módulos de cálculo 26 y 40 están programados para aplicar cada una de varias funciones Fi de transformación de la citada clave de codificación que dependen de medios técnicos para la seguridad de los terminales de recepción del contenido y que varían entre un nivel mínimo de seguridad y un nivel máximo de seguridad.

De ese modo, a cada función Fi se ha asignado por programación un nivel de seguridad Ni dado, teniendo en cuenta este nivel de seguridad Ni los medios técnicos de provisión de seguridad que se mencionan a continuación, dados a título de ejemplo no limitativo:

- posibilidad de almacenamiento de una clave de codificación en forma cifrada en una memoria no volátil del terminal,

- posibilidad de almacenamiento del código aplicativo del terminal en forma cifrada en una memoria no volátil del terminal,

- posibilidad de cargar en una memoria volátil de dicho terminal el código aplicativo cifrado durante su ejecución, y

- posibilidad de oscurecimiento de dicho código.

Por ejemplo, el nivel de seguridad específico de un terminal puede ser cuantificado según la siguiente tabla:

| **Medio técnico de provisión de seguridad** | **Nivel Sí/No** | **Terminal Modelo A** | **Terminal Modelo B** | **Terminal Modelo C** | **Terminal Modelo D** |
|---|---|---|---|---|---|
| Protección del CW* nivel Chipset | 50/0 | Sí :50 | No :0 | Sí :50 | No :0 |
| Código cifrado en memoria no volátil | 15/0 | Sí :15 | Sí :15 | No :0 | No :0 |
| Código cifrado en memoria volátil (RAM) durante ejecución | 30/0 | No :0 | No :0 | No :0 | No :0 |
| Oscurecimiento del código | 05/0 | No :0 | Sí :5 | Sí :5 | No :0 |
| Nivel de seguridad específico (NI) (Suma Total) | Nivel Máx. 100 | 65 (nivel superior) | 20 (nivel moderado) | 55 (nivel reforzado) | 0 (nivel bajo) |

En el ejemplo dado en la tabla que antecede, se comprende que el nivel de seguridad específico de un terminal varía de 0 a 100 según la presencia parcial o completa de los medios técnicos de provisión de seguridad. Se pueden prever, por lo tanto, en el primer y segundo módulos de seguridad, tantas funciones Fi como niveles de seguridad específicos Ni (en su caso, 16 niveles diferentes).

En el ejemplo de la figura 1, el terminal 4 tiene un nivel de seguridad que está definido por el hecho de que el único módulo utilizado para descodificar un contenido es una lógica constituida por el agente DMR 30, mientras que el terminal 8 tiene un nivel de seguridad definido por el hecho de que además de la lógica constituida por el agente DRM 36, el descodificador 34 incluye el segundo módulo de cálculo 40 que está programado para aplicar la función F de transformación a la clave K. La generación de la función F está comandada, a partir de la cabecera de red, por la plataforma 2 por medio de la señalización PMT que transporta una descripción de la función F utilizada, en la cabecera de la red, por el primer módulo de cálculo 26 para generar la clave transformada F(K).

En un ejemplo de realización, la citada función F es una función de sentido único (“one way function”), es decir, una función difícilmente reversible. Una primera posibilidad para la función F consiste en utilizar un algoritmo de cifrado tal como AES o TDES para el cifrado de K como con una clave K. Cualquier otra función de sentido único puede ser conveniente tal como, por ejemplo, la “Rabin function” o una función de cálculo de MAC tal como “SHA 256”. Para evitar una reproducción pirata de la función F por vía lógica, se preferirá para F una función cuyo cálculo por medio de una lógica ejecutada por un microprocesador convencional (para PC o Set Top Box) sea larga de efectuar (10 segundos, lo que corresponde por ejemplo a un criptoperíodo) con relación a la misma función ejecutada por un componente material especializado (Digital Signal Processor, Digital Logic Array) exclusivo para los terminales que disponen del módulo de cálculo y gracias al cual la función F será ejecutada instantáneamente (típicamente, algunas decenas de milisegundos). Bajo esta óptica, para aprovechar la diferencia de comportamiento, se podrán utilizar para la función F los ejemplos de funciones de sentido único citados anteriormente, encadenando un número importante de iteraciones sucesivas (por ejemplo, encadenamiento de 10000 operaciones SHA 256 sobre el último resultado obtenido).

El contenido a distribuir es por ejemplo un flujo digital que incluye una componente de base que tiene el nivel mínimo de seguridad y al menos una componente suplementaria que tiene el nivel superior de seguridad. En ese caso, la codificación del contenido por medio de la clave de codificación transformada se aplica tanto globalmente a todas las componentes del flujo, como selectivamente a cada componente del flujo.

La figura 2 ilustra una arquitectura destinada a aplicar el procedimiento según la invención a un flujo en un contexto de transmisión adaptativa.

En esta arquitectura la plataforma 2 de acondicionamiento del contenido a distribuir incluye una memoria 50 para almacenar los contenidos a distribuir, un codificador A/V 52, un generador de clave de codificación 54, un agente DRM 56, y un codificador 58. La plataforma 2 comunica con un multiplexor 60 adaptado para transmitir los contenidos a un terminal 70. Este último incluye un agente DRM 72, un módulo de adaptación de flujo 74, un descodificador 76, un descodificador 78, y una memoria 80 para el almacenaje de los contenidos recibidos.

En el lado de emisión, un contenido a distribuir, proporcionado por la memoria 50, es acondicionado por el codificador 52 de modo que se suministran cuatro flujos distintos que transportan el mismo contenido teniendo, por ejemplo, respectivamente para cada caudal de 300 Kbit/s, 700 Kbit/s, 1,5 Mbit/s y 4 Mbit/s, asociado a cada caudal, un nivel de calidad y un nivel de seguridad condicionantes que se utilizan para codificar la función de transformación F.

Se debe apreciar que la a0plicación del procedimiento conforme a la invención 90, 92, 94 y 96 a transmisión adaptativa, necesita una sincronización de las claves de codificación sobre los flujos asociados a las diferentes calidades de un mismo contenido, todo ello a fin de poder conmutar de una calidad a otra, típicamente en función del caudal disponible para utilizarlo, sin impacto sobre la continuidad del servicio prestado.

En funcionamiento, el codificador 58 proporciona los flujos 90, 92, 94 y 96 al multiplexor 60, y el agente DRM 56 de la plataforma 2 proporciona la clave de codificación K al agente DRM 72 del terminal 70. Los flujos 90, 92, 94 y 96 son transmitidos a continuación por el multiplexor 60 al módulo de adaptación de flujo 74 que los transmite al descodificador 76. El descodificador 76 está programado para descodificar el, o los, flujo(s) que tiene(n) un caudal dado en función del tipo de terminal de recepción 70 y/o de los derechos de acceso al contenido adquiridos por ese terminal. De ese modo, un terminal recibirá el contenido con uno de los caudales de 300 Kbit/s o 700 Kbit/s o 1,5 Mbit/s o 4 Mbit/s. El contenido así descodificado, o bien se visualiza, o bien se almacena en la memoria 80, en función de los derechos de acceso asociados al terminal 70.

**REIVINDICACIONES**

1.- Procedimiento de protección de un contenido a distribuir en un parque de terminales de recepción (4, 8, 70) conectados a una red de distribución de contenido y de los que cada uno tiene un nivel de seguridad especifico que depende de los medios técnicos de provisión de seguridad utilizados, incluyendo el procedimiento las etapas siguientes:

• en la emisión:

- generar una clave de codificación K de dicho contenido,

- transformar la citada clave de codificación K por medio de un primer módulo de cálculo (26) dispuesto en la cabecera de dicha red de distribución de contenido,

- codificar el contenido por medio de la clave transformada,

- transmitir el contenido codificado y la clave de codificación a los terminales (4, 8, 70), y

• a la recepción de dicho contenido y de la clave de codificación por parte de un terminal (4, 8, 70):

- transformar la citada clave de codificación por medio de un segundo módulo de cálculo (40) dispuesto en el citado terminal (4, 8, 70),

- descodificar el contenido con la clave de codificación transformada;

estando el procedimiento caracterizado además por las etapas que consisten en:

en la emisión,

- aplicar a la citada clave de codificación K, por medio de dicho primer módulo de cálculo (26), una función F definida en función de dicho nivel de seguridad específico,

y en la recepción,

- aplicar a la citada clave de codificación, por medio de dicho segundo módulo de cálculo (40), una función F definida en función de dicho nivel de seguridad específico.

2.- Procedimiento según la reivindicación 1, en el que los citados primer módulo de cálculo (26) y segundo módulo de cálculo (40) incluyen, cada uno de ellos, varias funciones Fi de transformación de la citada clave de codificación K, correspondiendo cada función Fi a un nivel de seguridad Ni dado.

3.- Procedimiento según la reivindicación 1, en el que los citados medios técnicos de provisión de seguridad son o bien software o bien materiales.

4.- Procedimiento según la reivindicación 3, en el que los citados medios de provisión de seguridad incluyen al menos una de las características siguientes:

- almacenamiento de la clave de codificación en forma cifrada en una memoria no volátil del terminal,

- almacenamiento del código aplicativo del terminal en forma cifrada en una memoria no volátil del terminal,

- cargo en una memoria volátil de dicho terminal del código aplicativo cifrado durante su ejecución, y

- el oscurecimiento de dicho código.

5.- Procedimiento según la reivindicación 1, en el que la clave de codificación K es transmitida, en forma cifrada, a los terminales (4 8, 70) a través de un ECM o de una licencia DRM (Digital Right Management).

6.- Procedimiento según la reivindicación 1, en el que la aplicación de la función F a la clave de codificación K está pilotada por el operador a través de una señalización PMT (Program Mapping Table).

7.- Procedimiento según la reivindicación 2, en el que dicho segundo módulo de cálculo incluye varias funciones Fi de transformación de la citada clave de codificación, correspondiendo cada función Fi a un nivel de seguridad Ni dado que varía entre un nivel mínimo de seguridad y un nivel máximo de seguridad correspondiente al nivel de seguridad específico del terminal.

8.- Procedimiento según la reivindicación 7, en el que la citada función F es una función de sentido único.

9.- Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el contenido a distribuir es un flujo digital que incluye una componente de base que tiene el nivel mínimo de seguridad y al menos una componente suplementaria que tiene un nivel superior de seguridad.

10.- Procedimiento según la reivindicación 9, en el que la codificación del contenido por medio de la clave de codificación transformada se aplica ya sea globalmente a todas las componentes del flujo, o ya sea selectivamente a cada una de las componentes del flujo.

11.- Aplicación del procedimiento según la reivindicación 10 a un flujo en un contexto de transmisión adaptativa, en la que la función F se aplica a las componentes del flujo de mejores calidades.

12.- Dispositivo emisor de un contenido a distribuir en un parque de terminales de recepción (4, 8, 70), conectados a una red de distribución de contenido y de los que cada uno tiene un nivel de seguridad específico que depende de los medios técnicos de provisión de seguridad utilizados, incluyendo el dispositivo un generador (16) de clave de codificación de dicho contenido, un codificador del contenido por medio de la clave transformada, medios para transmitir el contenido codificado y la clave de codificación a los terminales, estando el dispositivo caracterizado porque incluye, además, una o varias funciones Fi de transformación de la citada clave de codificación K, correspondiendo cada función Fi a un nivel de seguridad Ni dado.

13.- Terminal de recepción de un contenido perteneciente a un parque de terminales de recepción conectados a una red de distribución de contenido y de los que cada uno tiene un nivel de seguridad específico que depende de los medios técnicos de provisión de seguridad utilizados, siendo el citado contenido distribuido en forma codificada por medio de una clave de codificación previamente transformada por un primer módulo de cálculo (26) dispuesto en a la cabecera de la red, siendo la citada clave transmitida a dicho terminal, caracterizado porque comprende un segundo módulo de cálculo destinado a aplicar a la citada clave de codificación una transformación que permita hallar la clave transformada utilizada en la emisión para codificar el contenido transmitido.

14.- Programa de ordenador memorizado sobre un soporte de registro y que incluye instrucciones para calcular, cuando éstas son ejecutadas por medio de un ordenador, una clave de codificación transformada en la emisión por medio de una función F del procedimiento de la reivindicación 1.

15.- Programa de ordenador memorizado en un soporte de registro y que incluye instrucciones para hallar, cuando éstas son ejecutadas por medio de un ordenador, la clave de codificación transformada en la emisión por medio de la citada función F según la reivindicación 14.

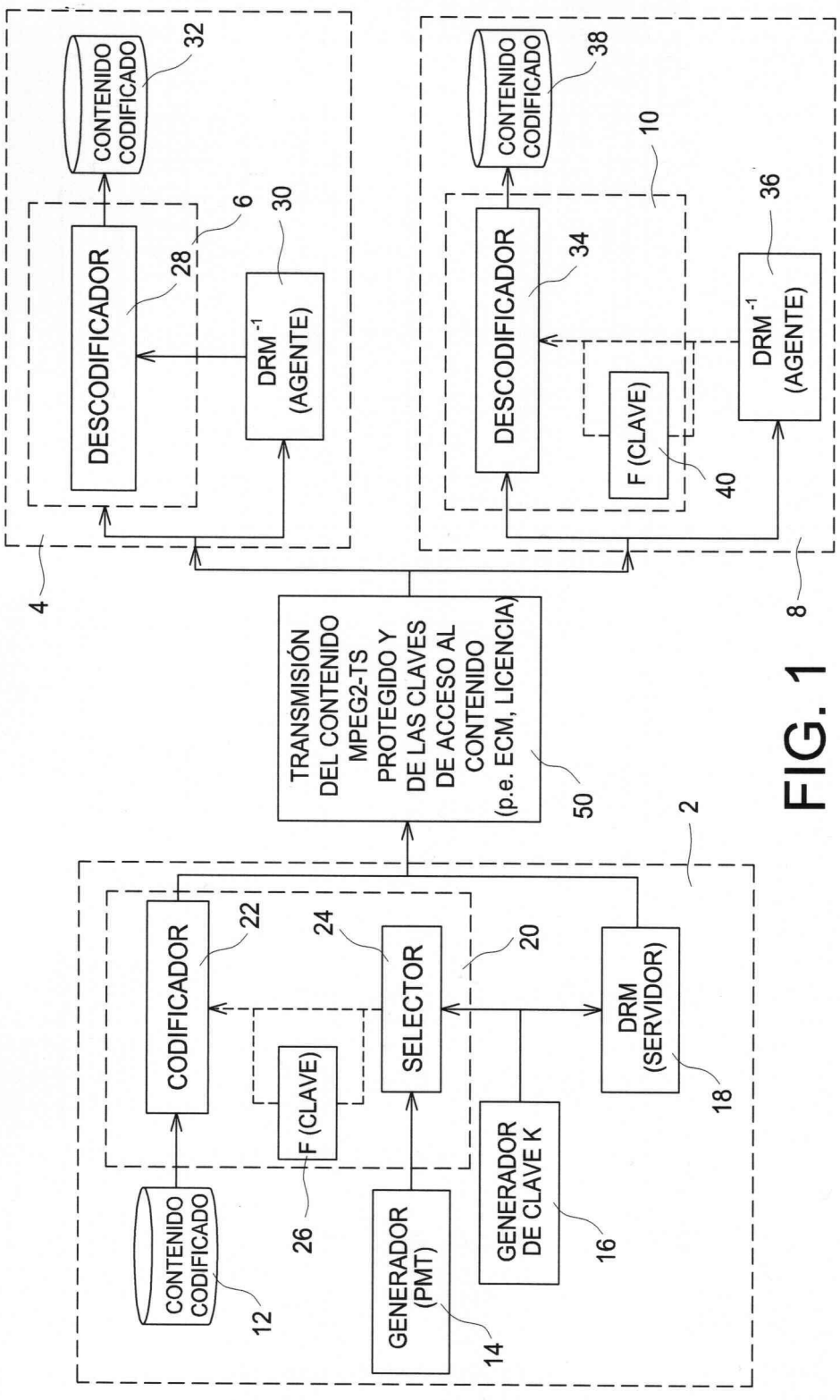
CONTENIDO CODIFICADO
32
DESCODIFICADOR
28
6
30
DRM -1 (AGENTE)
4
CONTENIDO CODIFICADO
38
10
DESCODIFICADOR
34
F (CLAVE)
40
36
DRM -1 (AGENTE)
8
TRANSMISIÓN DEL CONTENIDO MPEG2-TS PROTEGIDO Y DE LAS CLAVES DE ACCESO AL CONTENIDO (p.e. ECM, LICENCIA)
50
2
CODIFICADOR
22
24
SELECTOR
20
DRM (SERVIDOR)
18
F (CLAVE)
26
CONTENIDO CODIFICADO
12
GENERADOR (PMT)
14
GENERADOR DE CLAVE K
16

FIG. 1

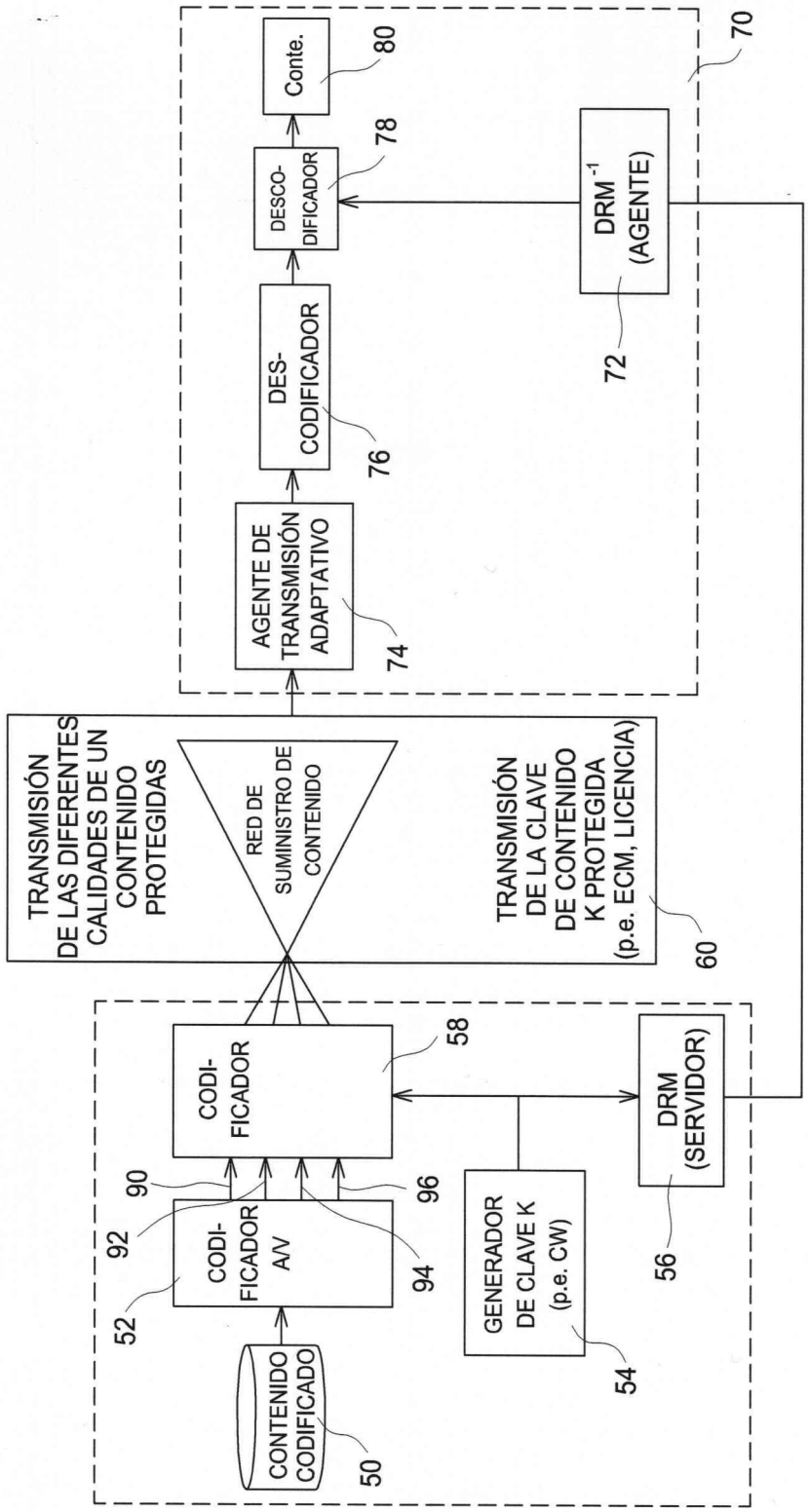
CONTENIDO CODIFICADO
50
CODI-FICADOR A/V
52
90
92
94
96
CODI-FICADOR
58
GENERADOR DE CLAVE K (p.e. CW)
54
DRM (SERVIDOR)
56
TRANSMISIÓN DE LAS DIFERENTES CALIDADES DE UN CONTENIDO PROTEGIDAS
RED DE SUMINISTRO DE CONTENIDO
TRANSMISIÓN DE LA CLAVE DE CONTENIDO K PROTEGIDA (p.e. ECM, LICENCIA)
60
AGENTE DE TRANSMISIÓN ADAPTATIVO
74
DES-CODIFICADOR
76
DESCO-DIFICADOR
78
Conte.
80
DRM -1 (AGENTE)
72
70

FIG. 2