(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 600 796**

(51) Int. CI.:

H04N 21/2347 (2011.01)
H04N 21/254 (2011.01)
H04N 21/4405 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/4627 (2011.01)
H04N 21/8355 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.12.2007 PCT/EP2007/064067**

(87) Fecha y número de publicación internacional: **26.06.2008 WO08074773**

(96) Fecha de presentación y número de la solicitud europea: **17.12.2007 E 07857697 (2)**

(97) Fecha y número de publicación de la concesión europea: **27.07.2016 EP 2103123**

(54) Título: **Procedimiento de control de acceso a un contenido digital aleatorizado**

(30) Prioridad:

19.12.2006 FR 0655632

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.02.2017

(73) Titular/es:

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

(72) Inventor/es:

NEAU, LOUIS

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Procedimiento de control de acceso a un contenido digital aleatorizado

La invención se sitúa en el campo de la protección de contenidos y se refiere de manera más específica a un procedimiento de control de acceso a un contenido digital aleatorizado por una clave secreta K y distribuido por un operador a al menos un terminal de recepción que consta de una multitud de módulos de control de acceso, aplicando cada módulo de control de acceso una técnica específica de determinación de la clave secreta K, procedimiento en el que el servidor de contenido transmite al terminal el contenido aleatorizado, y el servidor del derecho transmite al terminal unos datos de seguridad D(K) previamente definidos en función de la clave secreta K.

La invención también se refiere a un sistema de control de acceso a un contenido digital aleatorizado suministrado por un operador a un terminal de recepción que consta de una multitud de módulos de control de acceso distintos, aplicando cada módulo de control de acceso una técnica específica de determinación de la clave secreta K, constando dicho sistema de:

- un servidor de contenido que comprende unos medios para aleatorizar el contenido por un clave secreta K;

- un servidor del derecho que comprende unos medios para calcular unos datos de seguridad D(K) en función de la clave secreta K.

La invención se refiere también a un terminal de recepción de un contenido aleatorizado por una clave secreta K suministrada por un operador, constando dicho terminal de una multitud de módulos de control de acceso distintos aplicando cada uno una técnica específica de determinación de dicha clave secreta K, recibiendo dicho terminal, además, de dicho operador unos datos de seguridad D(K) que constan de un criterio de selección de un módulo de control de acceso entre la multitud de módulos de control de acceso del terminal para tratar dichos datos de seguridad D(K).

La invención se refiere, por último, a un programa de ordenador grabado en un soporte y destinado, cuando lo ejecuta un ordenador, a aplicar el procedimiento de acuerdo con la invención.

Estado de la técnica anterior

Los proveedores de contenidos explotan varios servicios distintos como, por ejemplo, las cadenas de televisión (televisión en directo), el vídeo a la carta (VOD por *Video On Demand*) o incluso los servicios de compra en línea de programas audiovisuales para distribuir unos datos y/o unos programas multimedia a los abonados. Estos servicios se despliegan en diversas redes de soporte y se pueden ofrecer en modo conectado o en modo no conectado a través de los canales de distribución bidireccionales o unidireccionales.

La forma de suministro y de utilización de los contenidos concernidos varía en función del servicio ofrecido y de la red de soporte utilizada.

Estas formas son, en particular:

- la difusión, para los servicios de televisión en directo;

- la difusión multimedia continua (*streaming*), para los servicios de video a la carta (VOD);

- la descarga, para los servicios de compra de programa;

- la (re)lectura de contenidos previamente recibidos y grabados localmente (PVR, por *Personal Video Recorder*, grabador personal de vídeo).

Las técnicas de protección de los contenidos suministrados a los abonados dependen de la naturaleza de los servicios explotados para distribuirlos y del tipo de redes de soporte utilizadas para ofrecer estos servicios.

Tradicionalmente, los flujos de difusión (o *streaming*), así como los contenidos grabados en los mismos formatos que estos flujos, se pueden proteger mediante unos sistemas de acceso condicional (o CAS, por *Conditional Access System*), y los archivos de descarga, así como los contenidos previamente obtenidos mediante cualquier medio citado con anterioridad y grabados en el mismo formato que dichos archivos, se pueden proteger mediante unos sistemas de gestión de derechos digitales (o DRM, por *Digital Rights Management*).

Para entender mejor la terminología específica del campo de los sistemas de CAS, podrá remitirse al siguiente documento:

“FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM”, EBU REVIEW-TECHNICAL EUROPEAN

BROADCASTING UNION. Bruselas, BE, nº. 266, 21 de diciembre de 1995.

Se puede acceder a una presentación detallada de un sistema DRM (por ejemplo OMA-DRM) en los documentos citados por el consorcio « Open Mobile Alliance", tales como:

- "OMA DRM Approved Version 2.0 - 23" (marzo de 2007), o también

- "OMA DRM Specification V2.0 Draft Version 2.0 - 21" (junio de 2004).

La figura 1 ilustra de forma esquemática un sistema de distribución de contenidos en el que se aplica la protección de contenido mediante DRM.

Este sistema consta de un operador 1 que dispone de un servidor de contenido 2 asociado a un módulo 4 de conformación de dichos contenidos y a un servidor de licencias 6, y un equipo receptor 8 que consta de un agente DRM 10, un lector/decodificador de contenido 12 y un módulo de diálogo con el usuario.

En esta arquitectura, el servidor de contenido 2 recibe (flecha 14) del módulo de conformación 4 un contenido aleatorizado adaptado al formato DRM y transmite (flecha 15) este contenido al agente DRM 10.

El servidor de licencias 6 recibe del módulo de conformación 4 (flecha 16) información relativa a seguridad del contenido, como la clave de descifrado (o de desaleatorización) de este contenido y transmite (flecha 18) al equipo terminal 8 la licencia DRM asociada al contenido.

Hay que recordar que una licencia DRM corresponde a la yuxtaposición de información relativa al contenido, en particular su identificador y la clave criptográfica que permite descifrarla, y de información sobre las autorizaciones y restricciones de uso del contenido (número de lecturas, derechos de copia, fecha límite o periodo de utilización, beneficiario(s) del contenido, etc.). La licencia representa en particular el derecho de uso de un contenido, concedido al titular del terminal.

La figura 2 es una representación esquemática de un objeto de contenido 20 (*Content Object*) y de un objeto de derecho 22 (*Right Object*) que designa respectivamente un contenido digital y la licencia asociada a este contenido en el contexto DRM (por *Digital Right Management*).

El objeto de contenido 20 consta de un identificador del contenido 24 y de un documento 26 que consta de los datos (vídeo, audio, etc.) que se pueden descifrar mediante una clave K cuyo criptograma K* 28 está presente en el objeto de derecho 22. El criptograma K* se obtiene mediante el cifrado de la clave K por una clave Ke que depende del emisor del derecho y que la suministra de forma segura al terminal al cual está destinado el contenido.

El objeto de derecho 22 es una recopilación de datos que describen la manera en que se puede utilizar un contenido digital. Por ejemplo, en el caso de la especificación “OMA Digital Rights Management” establecida por la Open Mobile Alliance, el objeto de derecho se describe en un documento XML (por *Extensible Markup Language*, lenguaje de marcas extensible) que contiene en particular el identificador 30 de este derecho, un atributo 32 (*Stateful/Stateless,* con estados/sin estados) que precisa si el derecho se modifica a lo largo de su utilización, una o varias designaciones del contenido 34 (*Asset*) que comprende en particular el identificador 36 del contenido (ContentId) y el criptograma K* 28 de la clave K. El objeto de derecho 22 consta, además, de una descripción 38 de permisos y de restricciones que indican el uso que se puede hacer del contenido. El grado de seguridad del contenido o del recurso depende esencialmente del grado de seguridad de la licencia asociada a este contenido, y de manera más precisa del grado de seguridad de la clave de descifrado K.

En el equipo receptor 8, el agente DRM 10 evalúa el derecho del usuario para acceder al contenido en función de la descripción 38 encapsulada en la licencia DRM. Con la condición de una autorización suministrada por el agente DRM 10, el lector de contenido 12 permite el acceso al contenido protegido y desaleatoriza este contenido.

La figura 3 ilustra de manera esquemática una arquitectura clásica de un sistema de distribución de contenidos protegidos por un sistema de acceso condicional CAS.

Las referencias idénticas designarán los elementos que cumplen la misma función en los sistemas de la figura 2 y de la figura 3.

El sistema ilustrado en la figura 3 consta de un modulo 40 de conformación de dichos contenidos al cual está asociado un módulo 42 de gestión de acceso condicional. El equipo receptor 8 del usuario consta en este caso de un módulo 44 de acceso condicional y de un procesador de seguridad 46. Este procesador de seguridad está en particular destinado a tratar los datos de seguridad relativos al sistema de acceso condicional, en particular los mensajes de control de acceso ECM y EMM introducidos a continuación. Puede ser externo o estar integrado en el terminal, y de equipo, como una tarjeta con chip, o de soporte lógico.

En esta arquitectura, el módulo 42 genera unos mensajes ECM (por “Entitlement Control Message”, mensaje de control de derecho) que contiene las condiciones de acceso a un contenido y la clave de desaleatorización de ese, habitualmente llamada palabra de control (CW por “Control Word”) y transmite estos mensajes (flecha 48) al módulo 40 de conformación. Este módulo aleatoriza el contenido y le asocia los mensajes ECM. El módulo 42 de gestión de acceso condicional gestiona, además, unos mensajes EMM (por “Entitlement Management Message”, mensaje de gestión de derecho) y transmite estos mensajes (flecha 50) al terminal 8 para garantizar la gestión de los títulos de acceso adquiridos por el usuario. De este modo, los títulos de acceso o los medios de adquirirlos (por ejemplo unas fichas para la compra impulsiva de programas) los genera y los inscribe a distancia el operador 1 en una memoria no volátil del procesador de seguridad 46.

En el equipo terminal 8 el módulo 44 de acceso condicional consta de un primer módulo 52 de tratamiento de los mensajes ECM y EMM en cooperación con el procesador de seguridad 46. Otros tratamientos complementarios, relativos a unas funciones particulares como la compra impulsiva de un programa en PPV (por “Pay Per View”, paga por ver) que necesitan el consentimiento del usuario, los gestiona un segundo módulo 54 de tratamiento. Cuando se cumplen las condiciones de acceso al contenido definidas en los ECM, el módulo 44 de acceso condicional suministra al terminal 8 la palabra de control CW, permitiendo que este desaleatorice el contenido y que restituya el contenido no cifrado al usuario. El terminal 8 dispone, además, de un módulo 56 de diálogo con el usuario.

La multiplicación de los servicios suministrados a los terminales, fijos o móviles, y la diversificación de los contenidos suministrados en el marco de estos servicios así como la ausencia de una norma única para la protección de estos contenidos, hacen difícil la implementación y la interacción, en un mismo terminal, de varias técnicas de protección de contenidos.

De este modo, la combinación, en un mismo terminal de recepción, de técnicas distintas de protección de contenidos, choca con la diferencia de formatos de los datos tratados por cada una de estas técnicas y con el tipo de tratamiento de los datos de seguridad específico de cada una de estas técnicas.

De forma general, la diversidad de las técnicas de protección de contenidos constituye un obstáculo para la convergencia de los servicios, en el sentido de su transparencia desde el punto de vista del usuario.

El objetivo de la invención es, por una parte, homogeneizar la protección de los contenidos en un mismo terminal que soporta al menos dos técnicas de protección de contenidos distintos, y por otra parte, hacer que una de estas técnicas se beneficie de las seguridad de otra, y de manera más particular hacer que se beneficie de una solución de tipo DRM normalizada del nivel de seguridad elevado de una solución CAS propietaria.

Otro objetivo de la invención es facilitar la aplicación, por el operador, de variaciones y de evoluciones del procedimiento de control de acceso utilizado con el fin de reforzar la protección de los contenidos.

El documento WO 2005/045554 A describe un método de protección de contenido digital en el que el contenido se cifra por una primera clave que está a su vez cifrada por una segunda clave, a continuación se difunde dicho contenido cifrado y dicha primera clave, a continuación se asigna un derecho a dicha segunda clave que se transmite a continuación con este derecho a un terminal móvil a través de una red móvil.

El documento EP 1 406 446 A1 describe un método en el que a un contenido recibido por una red lo trata, en primer lugar, un primer circuito para generar una información de control, y luego un segundo circuito acoplado al primer circuito que utiliza dicha información de control para proteger dicho contenido antes de su distribución en la red.

Exposición de la invención

Los objetivos de la invención se consiguen por medio de una combinación, en un mismo terminal, de al menos dos técnicas de protección de contenidos.

De manera más precisa, este objetivo se consigue por medio de un procedimiento de control de acceso a un contenido digital aleatorizado por una clave secreta K y distribuido por un operador provisto de un servidor de contenido y de un servidor de derecho a al menos un terminal de recepción que consta de una multitud de módulos de control de acceso, aplicando cada módulo de control de acceso una técnica específica de determinación de la clave secreta K.

Este procedimiento consta de las siguientes etapas:

- el servidor de contenido transmite al terminal (8) el contenido aleatorizado;

- el servidor de derecho (6, 42) transmite al terminal (8) unos datos de seguridad D(K) previamente definidos en función de la clave secreta K.

El procedimiento de acuerdo con la invención consta, además, de las siguientes etapas:

- en la emisión, el servidor de derecho incorpora en los datos de seguridad D(K) un criterio de selección que permite a uno al menos de los módulos de control de acceso entre los diferentes módulos de control de acceso del terminal decidir tratar solo los datos D(K) para intentar obtener la clave secreta K, o transmitir al menos una parte de estos a uno de los demás módulos de control de acceso del terminal;

- al recibir dichos datos de seguridad D(K) por uno de dichos módulos de control de acceso, dicho módulo de control de acceso:

analiza los datos D(K) para obtener dicho criterio de selección y, de acuerdo con su valor;

termina el tratamiento de los datos D(K) para obtener la clave secreta K; o

transmite una parte o todos los datos de seguridad D(K) a uno al menos de los demás módulos de control de acceso.

Cada una de las técnicas de protección de contenidos puestas en juego puede ser un sistema de acceso condicional, o CAS, o un sistema de gestión de derechos digitales, o DRM. El módulo de control de acceso correspondiente es, por tanto, respectivamente, un módulo de acceso condicional o un agente DRM. En ambos casos, este módulo dispone de un proceso de determinación de la clave K que consta, en particular, al menos de la evaluación del derecho del terminal de recepción para desaleatorizar el contenido recibido, o el descifrado de un criptograma K* de la clave secreta K, a partir de mensajes de tipo ECM y/o EMM; en el caso de un CAS, o de una licencia de DRM, en el caso de un DRM.

En una primera variante de realización, dicho criterio de selección se puede deducir de la sintaxis de dichos datos de seguridad D(K). Por ejemplo, de la longitud excesiva o insuficiente de un campo de los datos de seguridad D(K), como el campo de los datos criptográficos, un módulo de control de acceso puede deducir que este campo contiene unos datos que no están destinados a que este los trate.

En una segunda variante de realización, dicho criterio de selección es un bit o un grupo de bits entre los datos de seguridad D(K). Por ejemplo, un campo de estos datos está consagrado a un identificador de la técnica de determinación de la clave K que hay que aplicar.

De manera preferente, el contenido aleatorizado y los datos de seguridad se transmiten al terminal respectivamente por el servidor de contenidos y por el servidor de derecho simultáneamente o de forma escalonada en el tiempo.

En una primera forma de realización, los datos de seguridad D(K) constan al menos de un ECM y/o al menos de una licencia de DRM.

En una variante de esta forma de realización, el mensaje ECM se encapsula en la licencia de DRM.

En otra variante, dicho conjunto de datos de seguridad D(K) consta, además, de un mensaje EMM destinado a actualizar o a inscribir una clave o título de acceso en una memoria no volátil de dicho terminal.

De acuerdo con otra característica de la invención, dichos datos de seguridad D(K) se cifran total o parcialmente.

De este modo, la invención permite resolver la heterogeneidad de los sistemas de protección de contenidos utilizados a causa de la diversidad de los servicios explotados para suministrar un contenido.

Esta también permite al operador llevar a cabo variaciones y evoluciones del sistema de protección de contenidos utilizado con el fin de reforzar la protección de los contenidos.

El procedimiento de acuerdo con la invención se aplica mediante un sistema de control de acceso a un contenido digital aleatorizado suministrado por un operador a un terminal de recepción que consta de una multitud de módulos de control de acceso distintos, aplicando cada módulo de control de acceso una técnica específica de determinación de la clave secreta K, constando dicho sistema de:

- un servidor de contenido que comprende unos medios para aleatorizar el contenido por una clave secreta K;

- un servidor de derecho que comprende unos medios para calcular unos datos de seguridad D(K) en función de la clave secreta K.

El sistema de acuerdo con la invención se caracteriza por el hecho de que:

- el servidor de derecho consta, además, de unos medios para incorporar en los datos de seguridad D(K) un criterio de selección que permite a uno al menos de los módulos de control de acceso entre los diferentes módulos de

control de acceso del terminal decidir tratar solo los datos D(K) para intentar obtener la clave secreta K, o de transmitir al menos una parte de estos a uno de los demás módulos de control de acceso del terminal.

El terminal de recepción del contenido aleatorizado por la clave secreta K suministrado por el operador consta de una multitud de módulos de control de acceso distintos aplicando cada uno una técnica específica de determinación de dicha clave secreta K. Este terminal recibe, además, de dicho operador unos datos de seguridad D(K) que constan de un criterio de selección de un módulo de control entre la multitud de módulos de control de acceso del terminal.

Este terminal se caracteriza por que uno de dichos módulos de control de acceso consta de unos medios para analizar dicho criterio de selección de manera que decida tratar solo los datos D(K) para intentar obtener la clave secreta K, o transmitir al menos una parte de estos a uno de los demás módulos de control de acceso del terminal.

En una forma particular de realización, el terminal de acuerdo con la invención consta de dos módulos de control de acceso, en el que el primer módulo es un agente DRM (*Digital Rights Management*) y el segundo módulo es un módulo de acceso condicional, y una tarjeta con chip como procesador de seguridad.

Breve descripción de los dibujos

Se mostrarán otras características y ventajas de la invención en la descripción que viene a continuación, tomada a título de ejemplo no limitativo, en referencia a las figuras adjuntas en las que:

- la figura 1, descrita con anterioridad, ilustra de manera esquemática un sistema de distribución de contenidos en el que se aplica una técnica de protección de contenidos de tipo DRM;

- la figura 2, descrita con anterioridad, es una representación esquemática de un objeto de contenido (*Content Object*) y de un objeto de derecho (*Right Object*) que designan respectivamente un contenido digital y una licencia asociada a este contenido en el contexto de una técnica de protección de contenidos de tipo DRM;

- la figura 3, descrita con anterioridad, ilustra de manera esquemática una arquitectura clásica de un sistema de distribución de contenidos en el que se aplica una técnica de protección de contenidos de tipo CAS;

- la figura 4 representa un diagrama de bloques general de un ejemplo particular de sistema de acuerdo con la invención;

- la figura 5 ilustra de manera esquemática un ejemplo particular de aplicación del procedimiento de acuerdo con la invención en el sistema de la figura 4;

- la figura 6 es un organigrama que ilustra las etapas del procedimiento de acuerdo con la invención.

Exposición detallada de formas particulares de realización

Se va a describir a continuación la invención, en referencia a las figuras 4, 5 y 6, en un ejemplo de realización en el que un operador 1 suministra un contenido digital que representa unos datos o unos programas audiovisuales aleatorizados por una clave secreta K a un terminal de recepción 8 que soporta una técnica de protección basada en la norma OMA DRM (*Open Mobile Alliance*, *Digital Right Management*) y una técnica de protección basada en un CAS (*Conditional Access System*).

Por supuesto, la invención no está limitada al contexto descrito con anterioridad y se aplica sean cuales sean las técnicas de protección de contenido utilizadas.

A continuación en esta descripción, las referencias idénticas designarán los elementos comunes a las figuras de la técnica anterior y a las figuras que ilustran la invención.

En referencia a la figura 4, el operador 1 dispone de un servidor de contenido 2 asociado a un módulo 4 de conformación de dichos contenidos y a un servidor de licencias 6.

El terminal 8 consta de dos módulos de control de acceso, el primero es un agente DRM 10 conforme con la norma OMA DRM, que comunica a través de una interfaz 60 con el segundo que es un módulo de acceso condicional 46, que consta de un procesador de seguridad, como una tarjeta con chip, que contiene unos títulos de acceso al contenido aleatorizado. Dicho procesador de seguridad se puede implementar en forma de *software* sin salirse del marco de la invención.

De forma previa al suministro del contenido al terminal 8, el módulo 4 de conformación genera unos datos específicos para la técnica DRM, ilustrados de forma esquemática en la figura 5, que consta de un objeto de contenido 20 (*Content Object*) y de un objeto de derecho 22 (*Right Object*) llamado habitualmente licencia.

El objeto de contenido 20 consta de un identificador del contenido 24 y de un documento 26 que consta de los datos (vídeo, audio, etc.) cifrados por la clave K.

El objeto de derecho 22 constituye los datos de seguridad D(K) y consta, en particular, del identificador 30 de este derecho, precisando un atributo 32 (*Stateful*/*Stateless*) si el derecho se modifica a lo largo de su utilización, el identificador 36 del contenido asociado a esta licencia, una descripción 38 de permisos y de restricciones que indican el uso que se puede hacer del contenido, y unos datos criptográficos 70, que contienen al menos la clave K.

En el ejemplo de realización descrito, estos datos criptográficos 70 comprenden un ECM que consta del criptograma K* de la clave K y al menos de un condición de acceso, un identificador AlgoId del algoritmo de tratamiento del ECM por el procesador de seguridad 46, y unos parámetros Param 72 necesarios para la ejecución del algoritmo designado por el identificador AlgoId.

Los datos criptográficos 70 pueden, además, constar de un mensaje EMM que puede interpretar el procesador de seguridad 46 que permite, por ejemplo, actualizar o inscribir una clave o un título de acceso en la memoria no volátil del terminal.

En funcionamiento, de forma previa a la emisión del contenido, el servidor de licencia incorpora en los datos de seguridad D(K) un criterio de selección que permite a uno al menos de los módulos de control de acceso (10, 46) entre los diferentes módulos de control de acceso del terminal 8 decidir tratar solo los datos D(K) para intentar obtener la clave secreta K, o transmitir al menos una parte de estos a uno de los demás módulos de control de acceso del terminal.

Dicho criterio de selección bien se puede deducir de la sintaxis de dichos datos de seguridad D(K), o bien es un bit o un grupo de bits entre los datos de seguridad D(K).

En la forma de realización descrita, dicho criterio de selección es el valor del identificador AlgoId del algoritmo de tratamiento del ECM.

El servidor de contenidos 2 transmite el contenido aleatorizado al terminal 8 (flecha 80) y el servidor de licencias 6 transmite la licencia de DRM descrita en la figura 5 al terminal 8 (flecha 82).

Estas transmisiones pueden ser simultáneas o escalonadas en el tiempo.

Al nivel del terminal, para descifrar el contenido aleatorizado, el agente DRM 10 trata la estructura de datos de seguridad 70.

Por el valor particular del identificador AlgoId, detecta que la licencia no contiene el criptograma de la clave K como habitualmente sino un conjunto de datos, tradicionalmente un mensaje ECM, destinado a la técnica CAS con la cual coopera. El agente DRM ejecuta entonces el algoritmo designado por el identificador AlgoId, con los parámetros Param 72, para extraer el ECM de la licencia DRM. Una vez extraído el ECM, este se transmite por el agente DRM 10, a través de la interfaz 60, al procesador de seguridad 46. Este último, de forma conocida en sí misma, trata el ECM (bloque 84, figura 5), es decir verifica que se cumplen las condiciones de acceso contenidas en el ECM y descifra el criptograma K* si estas condiciones de acceso las cumple al menos un título de acceso, y a continuación devuelve (flecha 86, figura 5) la clave K extraída del ECM al agente DRM 10. Este último utiliza esta clave para desaleatorizar el contenido.

Las etapas esenciales del procedimiento de acuerdo con la invención se van a describir a continuación en referencia a la figura 6.

En la etapa 90, el terminal recibe el contenido aleatorizado y la licencia DRM asociada a este contenido.

Hay que señalar que la obtención del contenido protegido y la obtención de la licencia se pueden hacer en cualquier orden.

En la etapa 92, el usuario solicita el acceso al contenido. En la etapa 94, el agente DRM determina la licencia asociada a este contenido, eventualmente con un diálogo complementario con el usuario para seleccionar una licencia entre varias posibles.

En la etapa 96, el agente DRM 10 verifica la sintaxis, la integridad y la autenticidad de la licencia DRM, así como las autorizaciones y restricciones 38 que condicionan el acceso al contenido.

Si la licencia presenta una anomalía o si no se cumplen estas autorizaciones y restricciones 38, el agente DRM 10 deniega el acceso al contenido en la etapa 100.

Si la licencia es correcta y si se cumplen las autorizaciones y restricciones 38, el agente DRM 10 extrae los datos relativos a la clave K de descifrado del contenido (etapa 102).

En la etapa 104, el agente DRM 10 analiza el identificador del algoritmo AlgodId y detecta, en particular, si los datos relativos a la clave K extraídos en la etapa 102 hay que suministrarlos al sistema CAS.

Si este no es el caso, el criptograma K* lo descifra el agente DRM 10 en la etapa 106 de acuerdo con el procedimiento habitual específico de la técnica DRM.

Si este es el caso, los datos extraídos en la etapa 102 constituyen un ECM y en la etapa 108 el agente DRM 10 transmite este ECM al módulo de acceso condicional. El procesador de seguridad 46 asociado a este último trata en la etapa 110 el ECM recibido y verifica, en la etapa 112, si el mensaje ECM es correcto y si la condición de acceso contenido en este ECM la cumple al menos un título de acceso presente en el procesador de seguridad 46.

En caso negativo, en la etapa 114, el procesador de seguridad 46 envía un mensaje de error al agente DRM 10. Este último deniega entonces el acceso al contenido en la etapa 100.

En caso afirmativo, en la etapa 116, el procesador de seguridad 46 descifra el criptograma K* presente en el ECM, y el módulo de acceso condicional transmite, en la etapa 118, la clave K al agente DRM a través de la interfaz 60.

En la etapa 120, el agente DRM 10 desaleatoriza el contenido por medio de la clave K.

REIVINDICACIONES

1. Procedimiento de control de acceso a un contenido digital aleatorizado por una clave secreta K y distribuida por un operador provisto de un servidor de contenido (2) y de un servidor de derecho (6, 42) a al menos un terminal de recepción (8) que comprende una multitud de módulos de control de acceso (10, 46), aplicando cada módulo de control de acceso una técnica específica de determinación de la clave secreta K, procedimiento en el que:

- el servidor de contenido (2) transmite al terminal (8) el contenido aleatorizado;

- el servidor de derecho (6, 42) transmite al terminal (8) unos datos de seguridad D(K) previamente definidos en función de la clave secreta K,

- previamente a la emisión el servidor de derecho incorpora en los datos de seguridad D(K) un criterio de selección que depende de la sintaxis de dichos datos de seguridad D(K) y que permite a uno al menos de los módulos de control de acceso (10, 46) entre los diferentes módulos de control de acceso del terminal (8) decidir tratar solo los datos D(K) para intentar obtener la clave secreta K, o transmitir al menos una parte de estos a uno de los demás módulos de control de acceso del terminal;

- al recibir dichos datos de seguridad D(K) por uno de dichos módulos de control de acceso (10, 46), dicho módulo de control de acceso:

analiza los datos D(K) para obtener dicho criterio de selección y, de acuerdo con su valor;

termina el tratamiento de los datos D(K) para obtener la clave secreta K; o

transmite una parte o todos los datos de seguridad D(K) a uno al menos de los demás módulos de control de acceso.

2. Procedimiento de acuerdo con la reivindicación 1, en el que dicho criterio de selección es un bit o un grupo de bits entre los datos de seguridad D(K).

3. Procedimiento de acuerdo con la reivindicación 1, en el que el contenido aleatorizado y los datos de seguridad se transmiten al terminal respectivamente por el servidor de contenido (2) y por el servidor de derecho (6) simultáneamente o de forma escalonada en el tiempo.

4. Procedimiento de acuerdo con la reivindicación 1, en el que los datos de seguridad D(K) comprenden al menos un ECM y/o al menos una licencia de DRM.

5. Procedimiento de acuerdo con la reivindicación 4, en el que el mensaje ECM está encapsulado en la licencia de DRM.

6. Procedimiento de acuerdo con la reivindicación 1, en el que dicho conjunto de datos de seguridad D(K) comprende, además, un mensaje EMM destinado a actualizar o a inscribir una clave o un título de acceso en una memoria no volátil de dicho terminal.

7. Procedimiento de acuerdo con la reivindicación 1, en el que los datos de seguridad D(K) están cifrados total o parcialmente.

8. Sistema de control de acceso a un contenido digital aleatorizado suministrado por un operador a un terminal (8) de recepción que comprende una multitud de módulos de control de acceso (10, 46) distintos, aplicando cada módulo de control de acceso una técnica específica de determinación de la clave secreta K, comprendiendo dicho sistema:

- un servidor de contenido (2) que comprende unos medios para aleatorizar el contenido por una clave secreta K;

- un servidor de derecho que comprende unos medios para calcular unos datos de seguridad D(K) en función de la clave secreta K,

y comprendiendo, además, unos medios para incorporar en los datos de seguridad D(K) un criterio de selección que depende de la sintaxis de dichos datos de seguridad D(K) y que permite a uno al menos de los módulos de control de acceso del terminal (8) decidir tratar solo los datos D(K) para intentar obtener la clave secreta K, o transmitir al menos una parte de estos a uno de los demás módulos de control de acceso del terminal.

9. Terminal (8) de recepción de un contenido aleatorizado por una clave secreta K suministrada por un operador, comprendiendo dicho terminal una multitud de módulos de control de acceso (10, 46) distintos aplicando cada uno una técnica específica de determinación de dicha clave secreta K, recibiendo dicho terminal, además, de dicho

operador unos datos de seguridad D(K) que comprenden un criterio de selección de un módulo de control de acceso entre la multitud de módulos de control de acceso del terminal (8), dependiendo dicho criterio de selección de la sintaxis de dichos datos de seguridad D(K), y comprendiendo uno de dichos módulos de control de acceso unos medios para analizar dicho criterio de selección de manera que decida tratar solo los datos D(K) para intentar obtener la clave secreta K, o transmitir al menos una parte de estos a uno de los demás módulos de control de acceso del terminal.

10. Terminal de acuerdo con la reivindicación 9, que comprende dos módulos de control de acceso (10, 46), en el que el primer módulo (10) es un agente DRM (*Digital Rights Management*) y el segundo modulo (46) es un módulo de acceso condicional.

11. Terminal de acuerdo con la reivindicación 10, que comprende una tarjeta con chip como procesador de seguridad.

12. Programa de ordenador grabado en un soporte y destinado, cuando lo ejecuta un ordenador, a aplicar el procedimiento de acuerdo con una de las reivindicaciones 1 a 7 en un terminal de acuerdo con una de las reivindicaciones 9 a 11.

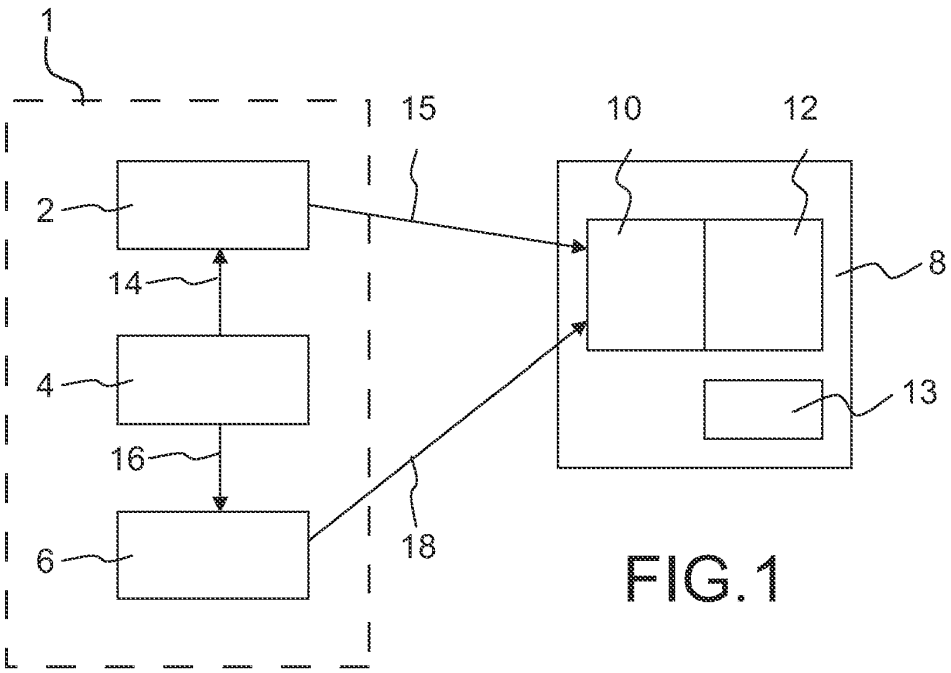

FIG.1

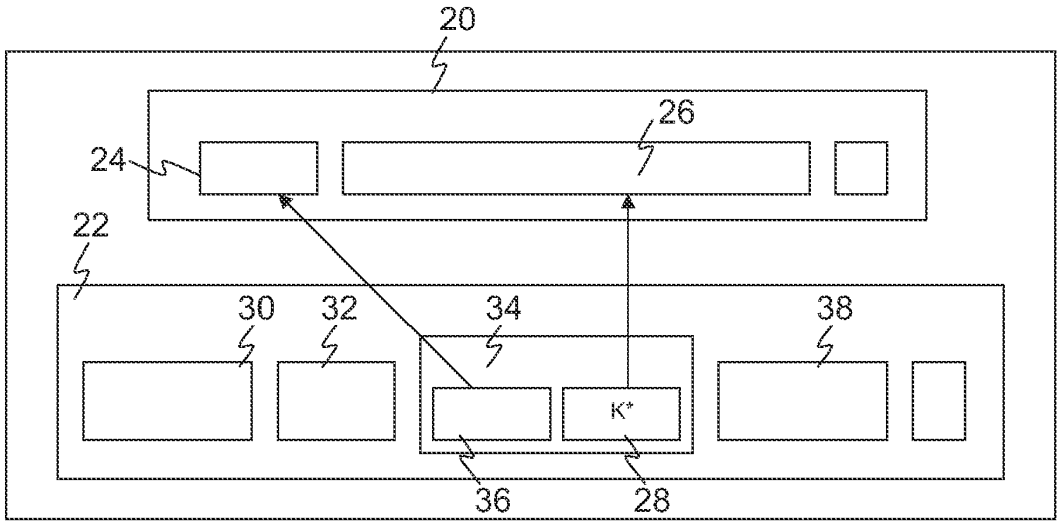

FIG.2

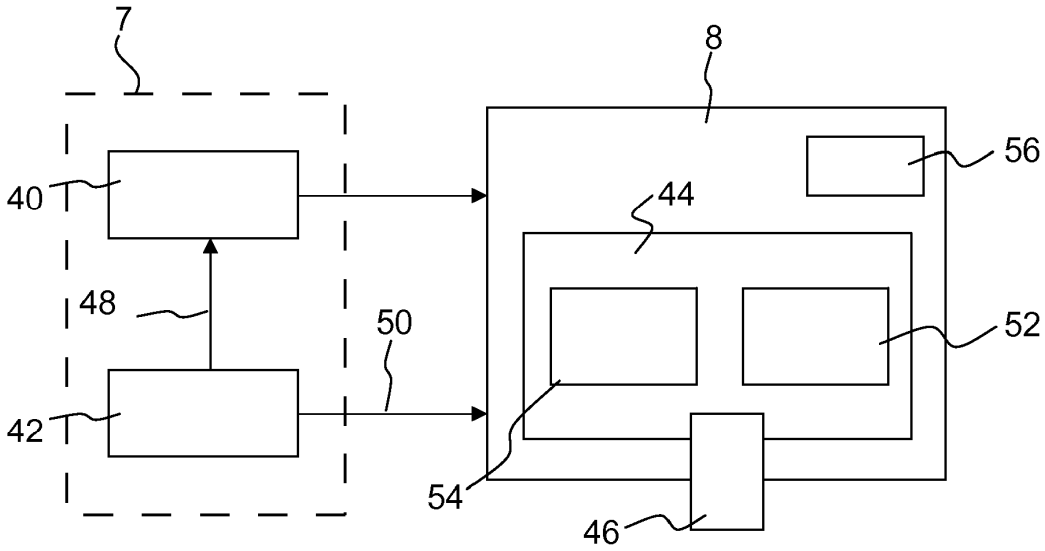

FIG.3

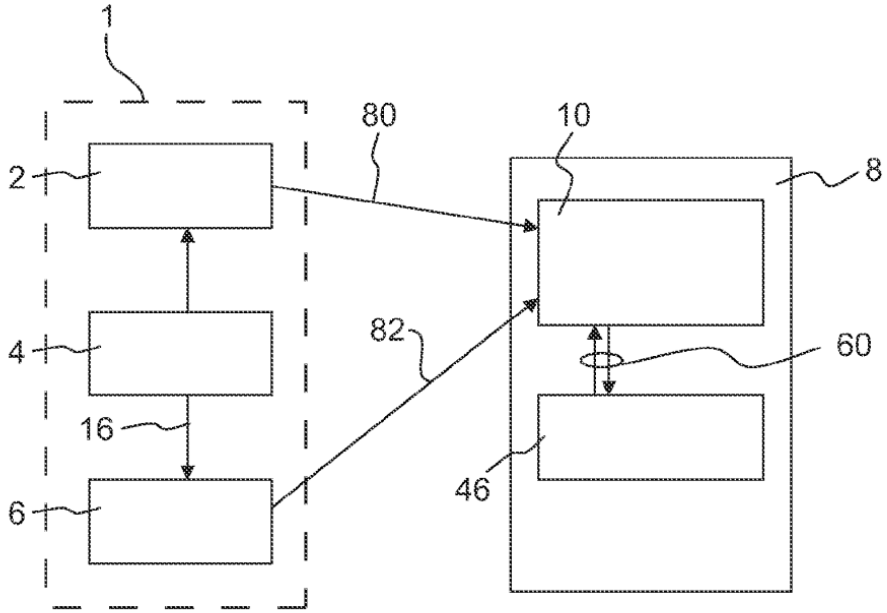
1
80
10
2
8
4
82
60
16
46
6

FIG.4

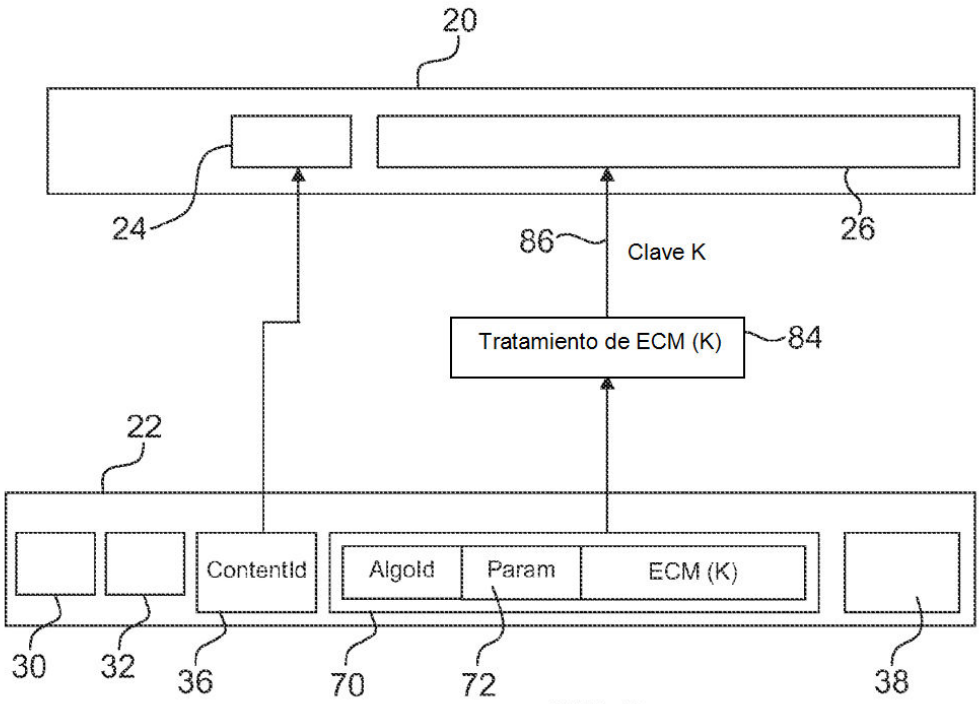
20
24
26
86
Clave K
Tratamiento de ECM (K)
84
22
ContentId
AlgoId
Param
ECM (K)
30
32
36
70
72
38

FIG.5

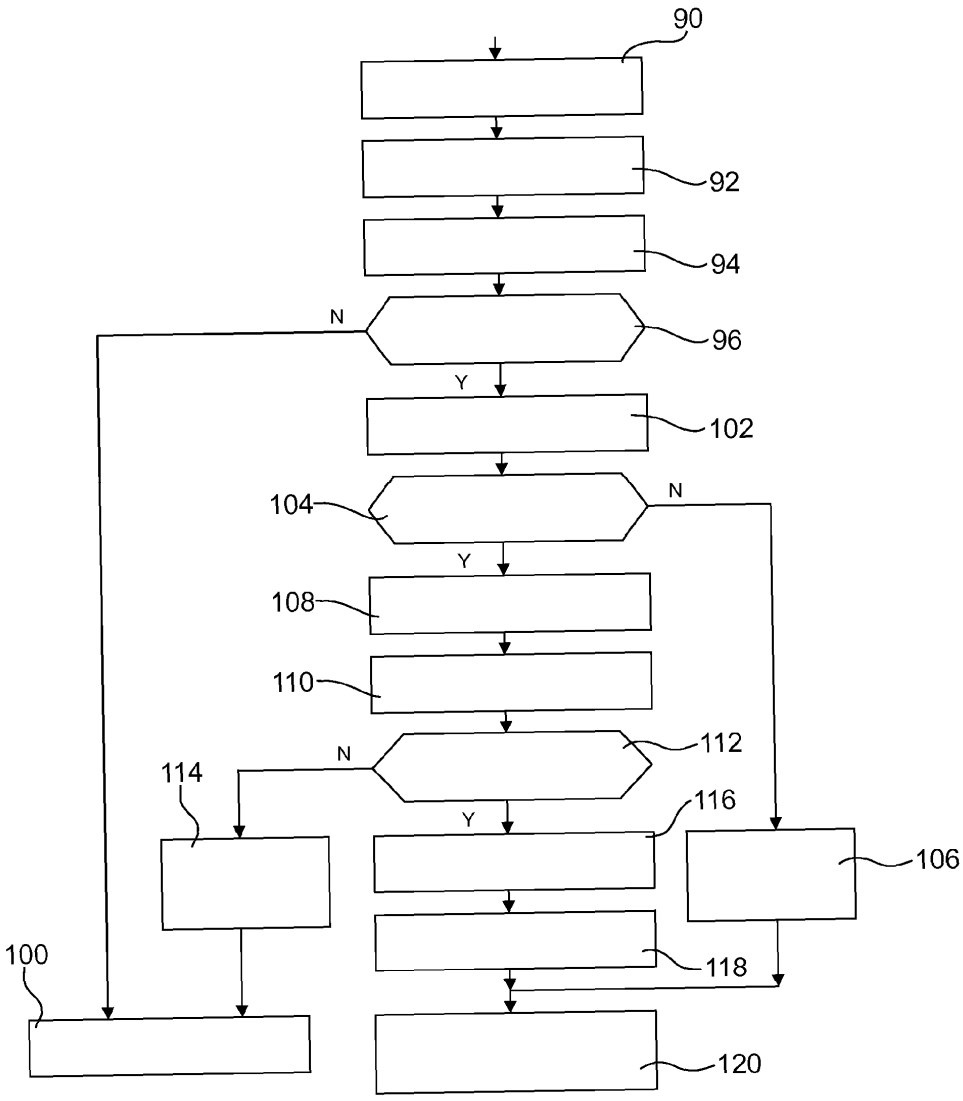

FIG.6