(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 417 141**

(51) Int. CI.:

H04N 21/4623 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.08.2006 E 06792902 (6)**

(97) Fecha y número de publicación de la concesión europea: **27.03.2013 EP 1961223**

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

(30) Prioridad:

13.12.2005 FR 0553852
31.03.2006 FR 0651130

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.08.2013

(73) Titular/es:

VIACCESS (100.0%)
LES COLLINES DE L'ARCHE, TOUR OPERA C
92057 PARIS LA DEFENSE CEDEX, FR

(72) Inventor/es:

CHEVALLIER, ANTHONY;
LANFRANCHI, STÉPHANE y
MAGIS, ERWANN

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DESCRIPCIÓN

Procedimiento de control de acceso a un contenido aleatorizado

Campo técnico

La invención se sitúa en el campo de la distribución de contenidos y se refiere más específicamente a un procedimiento de control de acceso a un contenido aleatorizado suministrado a un terminal de recepción por un operador al que está asociada una unidad de gestión de acceso, estando dotado el terminal de recepción de al menos un módulo de control de acceso, comprendiendo dicho procedimiento las siguientes etapas:

- asociar al contenido una pluralidad de informaciones necesarias en la desaleatorización de dicho contenido,

- transmitir dicho contenido con dicha pluralidad de informaciones a dicho terminal, y,

a la recepción de dicha pluralidad de informaciones por el terminal,

- reenviar sistemáticamente u ocasionalmente al menos una información entre dicha pluralidad de informaciones a la unidad de gestión de acceso vía una conexión punto a punto,

- verificar mediante la unidad de gestión de acceso si la información reenviada es compatible con unos derechos de acceso previamente concedidos a dicho terminal,

- transmitir al terminal al menos un parámetro de mando para permitir la utilización del contenido si la información renviada es compatible con los derechos de acceso previamente concedidos a dicho terminal,

- si no, la unidad de gestión no transmite dicho parámetro al terminal.

La invención se refiere igualmente a un sistema de control de acceso que comprende un dispositivo de emisión que comprende un servidor de contenido aleatorizado, una unidad de gestión de acceso asociada a dichos dispositivos, un terminal de recepción dotado al menos de un módulo de control de acceso al contenido aleatorizado suministrado por dicho servidor y al que está asociada una condición de acceso que comprende una pluralidad de informaciones necesarias en la desaleatorización de dicho contenido.

La invención se refiere igualmente a un programa de ordenador que comprende un módulo de tratamiento memorizado primero en el terminal que coopera con un módulo de tratamiento memorizado segundo en la unidad de gestión de acceso, estando destinado dicho programa a la puesta en marcha de un procedimiento de control de acceso conforme a la invención.

La invención se aplica igualmente cuando el contenido digital aleatorizado es distribuido en un parque de terminales receptores que comprenden un terminal maestro y una pluralidad de terminales esclavos que dependen de dicho terminal maestro, este último cumpliendo la función de una unidad de gestión de acceso.

Estado de la técnica anterior

En un contexto de difusión en multidifusión, es difícil reaccionar a ciertas formas de pirateo tales como por ejemplo la generación fraudulenta de derechos o claves requeridas para acceder a contenidos o incluso las tentativas de impedir la toma en cuenta por el sistema de recepción de mensajes de contramedidas emitidas por el operador.

Esta situación requiere entonces que el operador efectúe modificaciones del sistema de recepción del conjunto de los abonados para cambiar su señal de forma tal que ya no sea explotable por los dispositivos piratas. Las modificaciones a realizar deben por lo tanto ser suficientemente profundas, y su despliegue es entonces una operación pesada y costosa.

Estos inconvenientes provienen, particularmente, del hecho de que los sistemas de control de acceso conocidos presentan generalmente una arquitectura sin vía de retorno. En este tipo de arquitectura, el terminal funciona de forma autónoma con respecto a la cabeza de red. De hecho, el operador ya no dispone de ningún medio que le permita controlar, en tiempo real, los derechos de los abonados determinados en cuanto que todo el control de acceso es efectuado al nivel del terminal de recepción.

Una forma de desvío de contenido digital consiste en utilizar un mismo procesador de seguridad, típicamente una tarjeta inteligente válida, por varios terminales con el fin de tratar varías vías ECM. En este caso, un solo abonado es conocido del operador para varios usuarios efectivos de la misma tarjeta.

Esta forma de desvío permite a los decodificadores incriminados acceder a tantos programas diferentes en el límite de los derechos efectivamente presentes en la tarjeta compartida y en el límite del número de ECM que la tarjeta

puede tratar durante el periodo de renovación de las palabras de control. Este desvío de la tarjeta del abonado por varios decodificadores se hace sin ningún control del operador que no puede prohibirlo, ni tampoco limitarlo.

Otro problema se plantea igualmente cuando un abonado dispones de varios terminales de recepción de datos y/o servicios aleatorizados. En efecto, a menos que se consideren los terminales del mismo abonado como tantos terminales independientes conectados a tantas "copias" de este abonado, el operador no dispone de solución simple que le permita controlar la atribución de derechos de acceso independientes o comunes a los diferentes terminales del abonado.

La invención tiene por objeto paliar estos inconvenientes.

Más específicamente, la invención concierne a repartir las operaciones de control de acceso entre la parte aguas arriba del sistema, y la parte aguas abajo, es decir entre, por una parte, los equipamientos instalados en casa del operador, cuyas operaciones están directamente bajo el control de este último, y, por otra parte, el terminal de recepción que efectúa de forma clásica la verificación de los derechos de los abonados por medio del módulo de control de acceso. Este reparto permite limitar, incluso suprimir, la autonomía del terminal con respecto al operador en el transcurso de los tratamientos del control de acceso.

Otro objeto de la invención es tener en cuenta configuraciones en las que el terminal de recepción no dispone de una gran potencia de tratamiento. Esto puede ser el caso cuando los terminales de recepción son terminales móviles (teléfono móvil, PDA, ordenador portátil…) con una autonomía limitada en términos de energía y de potencia de tratamiento.

La invención tiene igualmente por objeto suministrar a los operadores una solución simple que permite atribuir de forma controlada unos derechos de acceso independientes o comunes a diferentes terminales de un mismo abonado.

La invención se aplica en los casos clásicos en los que el terminal está dotado de un módulo físico de control de acceso, típicamente una tarjeta inteligente, pero se aplica ventajosamente cuando el módulo de control de acceso no es un módulo físico sino un módulo de software almacenado preferentemente de forma asegurada en una memoria del terminal.

El documento US 2002114465 describe un sistema de transmisión de contenidos digitales a un usuario final en el que dicho terminal de usuario segundo transmite un contenido digital aleatorizado a un terminal de usuario primero de manera que dicho terminal de usuario segundo no pueda reutilizar dicho contenido y de manera que sea obligado a conectarse a un centro de control para obtener la autorización de usar dicho contenido.

El documento WO 0971692 describe un sistema de control de acceso a unos datos aleatorizados por una palabra CW de control y memorizados en un soporte de registro, comprendiendo dicho sistema unos medios para suministrar a dicho soporte de registro datos de regeneración de la palabra CW de control diferente a esta última, y unos medios para encontrar palabra CW de control a partir de dichos datos de regeneración.

Exposición de la invención

La invención preconiza un procedimiento de control de acceso a un contenido aleatorizado suministrado a un terminal de recepción por un operador al que está asociada una unidad de gestión de acceso, estando dotado dicho terminal de al menos un módulo de control de acceso.

Este procedimiento comprende las siguientes etapas:

- asociar al contenido una pluralidad de informaciones necesarias en la desaleatorización de dicho contenido,

- transmitir dicho contenido con dicha pluralidad de informaciones a dicho terminal, y,

a la recepción de dicha pluralidad de informaciones por el terminal,

- reenviar sistemáticamente u ocasionalmente al menos una información entre dicha pluralidad de informaciones a la unidad de gestión de acceso vía una conexión punto a punto,

- verificar mediante la unidad de gestión de acceso si la información reenviada es compatible con unos derechos de acceso previamente concedidos a dicho terminal,

- transmitir al terminal al menos un parámetro de mando para permitir la utilización del contenido si la información renviada es compatible con los derechos de acceso previamente concedidos a dicho terminal,

- si no, la unidad de gestión no transmite dicho parámetro al terminal.

Según la invención, el parámetro de mando enviado por la unidad de gestión de acceso al terminal es un mensaje ECM_R destinado a ser registrado con el contenido y que comprende unos criterios de acceso destinados al control de la reutilización de dicho contenido.

Así, cuando el terminal de recepción establece una comunicación con la unidad de gestión de acceso vía la conexión punto a punto, este último "toma la mano" para controlar los derechos de dicho terminal a acceder al contenido solicitado y permite o impide la utilización del contenido por el terminal en función del resultado de este control. En un modo preferido de puesta en marcha del procedimiento, el tratamiento de la información recibida por la unidad de gestión de acceso comprende una primera etapa que consiste en verificar si esta información es compatible con datos de acceso memorizados en el terminal, y una segunda etapa que consiste en transmitir al terminal al menos un parámetro de mando para permitir o impedir la utilización del contenido en función del resultado de la primera etapa.

Gracias al procedimiento según la invención, el control de acceso ya no es efectuado exclusivamente al nivel del terminal de recepción. Esto refuerza la protección del contenido.

Según la invención, la pluralidad de informaciones necesarias en la desaleatorización del contenido es transmitida al terminal en un mensaje ECM que comprende al menos un criterio de acceso CA, un criptograma CW^*_{kecm} de una palabra CW de control cifrada por una clave K_{ecm}.

El contenido aleatorizado es distribuido a un parque de terminales receptores y en el que la unidad de gestión de acceso es un terminal maestro entre los terminales del parque de terminales receptores y el terminal de recepción es un terminal esclavo entre los terminales del parque de terminales receptores.

El terminal esclavo reenvía al menos el criptograma CW^*_{Kecm} al terminal maestro.

El sistema de control de acceso destinado a poner en marcha el procedimiento según la invención comprende un dispositivo de emisión que comprende un servidor de contenido, una unidad de gestión de acceso asociada a dicho dispositivo de emisión, un terminal de recepción dotado de al menos un módulo de control de acceso a un contenido aleatorizado transmitido por dicho servidor y al que está asociada una pluralidad de informaciones necesarias en la desaleatorización de dicho contenido, estando unido dicho terminal de recepción a dicha unidad de acceso por una conexión punto a punto, estando adaptado dicho módulo de control de acceso para reenviar, sistemáticamente u ocasionalmente a dicha unidad de gestión de acceso al menos una información contenida en la pluralidad de informaciones necesarias en la desaleatorización del contenido, y dicha unidad de gestión de acceso es adaptada para verificar si la información reenviada es compatible con unos derechos de acceso previamente concedidos a dicho terminal, y para transmitir al terminal al menos un parámetro de mando para permitir la utilización del contenido si la información reenviada es compatible con los derechos de acceso previamente concedidos a dicho terminal, para no transmitir dicho parámetro al terminal si la información reenviada no es compatible con los derechos de acceso previamente concedidos en dicho terminal.

Según la invención, el parámetro de mando enviado por la unidad de gestión de acceso al terminal es un mensaje ECM_R destinado a ser registrado con el contenido y que comprende criterios de acceso destinados al control de la reutilización de dicho contenido.

En una primera variante de realización del sistema según la invención, dicha unidad de gestión de acceso es distinta del dispositivo de emisión.

En una segunda variante de realización del sistema según la invención, dicha unidad de gestión de acceso está integrada en el dispositivo de emisión.

En un modo particular de realización del sistema de la invención, el contenido aleatorizado es distribuido en un parque de terminales receptores y en el que la unidad de gestión de acceso es un terminal maestro entre los terminales del parque de terminales receptores y el terminal de recepción es un terminal esclavo entre los terminales del parque de terminales receptores.

Dicho terminal maestro es integrado en el dispositivo de emisión o en una antena de recepción colectiva.

En el sistema según un modo particular de realización, el terminal maestro cumple una función de pasarela entre el servidor de contenido y los terminales esclavos del parque.

El terminal de recepción del contenido aleatorizado transmitido con una pluralidad de informaciones necesarias en la desaleatorización de dicho contenido está unido a una unidad de gestión de acceso vía una conexión punto a punto y comprende un módulo de control de acceso que comprende unos medios para reenviar sistemáticamente u ocasionalmente al menos una información de dicha pluralidad de informaciones necesarias en la desaleatorización de dicho contenido a la unidad de gestión de acceso vía la conexión punto a punto de manera que permite a dicha

unidad de gestión de acceso verificar si la información reenviada es compatible con unos derechos de acceso previamente concedidos a dicho terminal, y transmitir al terminal al menos un parámetro de mando para permitir la utilización del contenido si la información reenviada es compatible con los derechos de acceso previamente concedidos a dicho terminal, o para no transmitir dicho parámetro al terminal si la información reenviada no es compatible con los derechos de acceso previamente concedidos a dicho terminal.

Según la invención, dicho parámetro de mando transmitido, por la unidad de gestión de acceso al módulo de control de acceso es un mensaje ECM_R destinado a ser registrado con el contenido y que comprende criterios de acceso destinados al control de la reutilización de dicho contenido.

El programa de ordenador memorizado en un soporte de registro comprende instrucciones destinadas a la puesta en marcha de un procedimiento de control de acceso según la invención cuando es ejecutado en un ordenador.

En un ejemplo de realización, la primera etapa de tratamiento de la información recibida por la unidad de gestión de acceso y el control de la condición de acceso por el terminal de recepción son efectuados independientemente uno del otro, sistemáticamente u ocasionalmente, según una cadencia definida por el operador.

El operador está así en condiciones de modular finamente el reparto espacial y temporal del control de acceso entre el operador y el terminal de recepción.

En otro ejemplo de realización, la cadencia definida por el operador es imprevisible para el terminal de recepción.

En la realización del procedimiento el terminal reenvía hacia la unidad de gestión de acceso al menos el criptograma CW^*_{Kecm} si el módulo de control de acceso no dispone de la clave K_{ecm} para descifrar dicho criptograma CW^*_{Kecm}. El parámetro enviado, después, por la unidad de gestión de acceso al terminal es una palabra CW de control descifrada con la clave K_{ecm} y recifrada por una clave K_{ter} conocida específicamente del terminal.

En un segundo ejemplo de aplicación, el procedimiento es puesto en marcha para controlar el acceso a un contenido protegido por una licencia DRM.

En este caso, la información reenviada por el terminal a la unidad de gestión de acceso es la licencia DRM.

Breve descripción de los dibujos

Otras características y ventajas de la invención surgirán de la descripción que va a seguir, tomada a título de ejemplo no limitativo, en referencia a las figuras adjuntas en las que:

- la figura 1 representa un esquema general de un sistema de control de acceso;

- la figura 2 representa esquemáticamente un primer ejemplo del sistema de la figura 1;

- la figura 3 es un esquema de bloque que ilustra una aplicación particular del procedimiento;

- las figuras 4 a 6 representan un cronograma que ilustra la cadencia del procedimiento;

- la figura 7 es un organigrama que ilustra las etapas de un modo de puesta en marcha del procedimiento;

- la figura 8 ilustra esquemáticamente una segunda aplicación del procedimiento en la que el control de acceso es gestionado por un terminal maestro al que están asociados varios terminales esclavos;

- la figura 9 ilustra esquemáticamente un procedimiento de control de la habilitación de un terminal esclavo para explotar el contenido digital.

Exposición detallada de modos de realización particulares

Un procedimiento para controlar el acceso a unos programas o unos contenidos multimedia difundidos a unos abonados dotados de derechos de acceso va ser descrito.

En la descripción que sigue, unas referencias idénticas designarán los elementos de las diferentes figuras que cumplen funciones idénticas o equivalentes. Nótese que el procedimiento puede ser puesto en marcha en cualquier red conectada dotada de una vía de retorno con caudal suficiente, tal como una red cableada tipo DSL (de *Digital Subscriber Line*), o una red sin hilo del tipo Wi-Fi o Wi-Wax (o ASFI, de *Accés Sans Fil à Internet*), o incluso una red móvil 3G.

La figura 1 ilustra un esquema general de un sistema de distribución de contenido en el que el procedimiento es susceptible de ser puesto en marcha.

Este sistema comprende un dispositivo 2 de emisión asociado a una unidad 4 de gestión de acceso, y un terminal 6 de recepción.

El dispositivo 2 de emisión comprende un servidor 8 de contenido que distribuye contenidos aleatorizados hacia el terminal 6 vía una red 7 de transporte, tal como una red cableada o una red de difusión hertziana, o incluso vía una línea DSL, y el terminal 6 comprende un módulo 10 de control de acceso que puede ser una tarjeta inteligente o, preferentemente, un módulo de software que realiza las funciones de control.

El terminal 6 es unido a la unidad 4 de gestión de acceso por una conexión punto a punto bidireccional 12.

En referencia a la figura 2, que ilustra esquemáticamente un ejemplo particular de sistema de la figura 1, el terminal 6 de recepción es un decodificador digital instalado en casa del abonado y la conexión entre el operador y los abonados es realizada por una línea DSL vía un equipo intermediario 14 que comprende un multiplexor DS-LAM 15 (de *Digital Subscriber Line Access Multiplexer* en inglés o multiplexor de acceso para líneas de abonados digitales) que comunica con una unidad 4 de gestión de acceso (o UGA). Este último está integrado en el equipo 14.

Nótese que la unidad 4 de gestión de acceso puede ser instalada en casa de un tercero de confianza que tenga por función controlar los derechos de los abonados bajo la supervisión del operador sin salir del marco de la invención.

El dispositivo 2 de emisión comprende un módulo ECM-G 16 (de *Entitlement Control Message Generator*) destinado a calcular y a difundir mensajes de explotación ECM, un módulo SAS 18 (de *Subscriber Authorization System*), destinado a calcular y a difundir mensajes EMM (de *Entitlement Management Message*) necesarios entre otros en el envío de los derechos y de las claves a los abonados y un multiplexor MUX 20 destinado a constituir un paquete de contenidos a partir de programas y/o servicios suministrados por el operador.

El terminal 6 está constituido por ejemplo por un decodificador/desaleatorizador de contenidos multimedia, conocido en la técnica anterior como Set Top Box en inglés (o STB). Dispones de un procesador 10 de seguridad especialmente concebido para tratar el control de acceso a los contenidos y la gestión de los derechos y de los secretos criptográficos (claves). Un ejemplo bien conocido de tal procesador de seguridad es la tarjeta inteligente conectada al terminal. Otro ejemplo del procesador 10 de seguridad puede igualmente ser realizado por una función de software dedicada e integrada en el terminal.

El procedimiento va a ser ahora descrito por referencia a las figura 3 a 7.

Los contenidos suministrados que representan programas multimedia difundidos en forma aleatorizado por una palabra CW de control.

El terminal 6 dispone de una clave K_{Diff} común a los terminales dirigidos por el operador, de una clave K_{Ter} específica a este terminal y de un derecho D_{Oper}. Estas claves y este derecho han sido cargados previamente en el procesador de seguridad, típicamente por mensaje EMM. Además, en caso de acción ilícita del abonado, el procesador de seguridad contiene un derecho D_{Fraud} adquirido fraudulentamente.

La unidad 4 de gestión de acceso dispone previamente de la clave T_{Oper}, de la clave K_{Ter} de cada terminal y sabe de qué derecho D_{Oper} dispone cada terminal.

En referencia a la figura 3, la condición de acceso es transmitida al terminal (flecha 22) en un mensaje ECM generado por el ECM-G 16 del dispositivo 2 de emisión. Este mensaje ECM comprende un criterio CA_{Oper} de acceso y el criptograma CW^*_{Kecm} de la palabra CW de control cifrada por una clave K_{ecm} que es ya sea la clave K_{Oper} conocida solamente del operador, ya sea la clave K_{Diff} conocida de todos los terminales del operador. Así, el acceso a un programa al que el mensaje ECM está asociado es posible en cuanto que el terminal dispone de al menos un derecho D_{Oper} que satisface el criterio CA_{Oper} de acceso y de la clave K_{ecm} que permite obtener la palabra CW de control por desciframiento del criptograma CW^*_{Kecm} que es el caso en este ejemplo si la clave K_{ecm} es la clave K_{Diff}.

En la recepción de los programas, el terminal 6 reenvía (flecha 24) el ECM recibido en la unidad 4 de gestión de acceso.

En una primera variante de puesta en marcha del procedimiento, en la que el operador quiere controlar sistemáticamente la desaleatorización del contenido por el terminal, la clave K_{ecm} es la clave K_{oper} que no es transmitida al terminal 6. En este caso, el terminal reenvía sistemáticamente el ECM a la unidad 4 de gestión de acceso.

En otra variante de puesta en marcha donde el control de la desaleatorización del contenido es compartido entre el terminal y el operador, el terminal reenvía ocasionalmente el ECM a la unidad 4 de gestión de acceso después de la verificación previa del criterio de acceso por el módulo 10.

En esta variante, el terminal reenvía el ECM si, por ejemplo, el abonado no dispone del derecho D_{oper} que permitiría verificar el criterio de acceso o si el terminal no dispone de la clave K_{ecm} de desciframiento del criptograma CW^*_{Kecm}. Si al contrario el terminal dispone del derecho que verifica el criterio de acceso y si el criptograma CW^*_{Kecm} puede ser descifrado con la clave K_{Diff}, el terminal accede al programa como en la técnica anterior.

Cuando la unidad 4 de gestión de acceso recibe el ECM del terminal 6, esta verifica si el terminal 6 dispone de los derechos necesarios para acceder a los programas recibidos.

En un primer modo de realización, la unidad de gestión de acceso dispone de una base de datos en la que se memorizan las descripciones de los derechos que el operador ha enviado al terminal del abonado. La unidad de gestión de acceso efectúa así la verificación del criterio de acceso con respecto a los derechos cuyo abonado dispone oficialmente. Este modo inhibe toda verificación del criterio de acceso con respecto a unos derechos ilícitos que el abonado habría podido cargar fraudulentamente en su terminal.

En un segundo modo de realización, la unidad de gestión de acceso lee a distancia el contenido del procesador de seguridad del terminal y efectúa la verificación del criterio de acceso con respecto a los derechos efectivamente presentes en el terminal. Este modo dispensa a la unidad de gestión de acceso de soportar una base de datos de los derechos de todos los abonados y permite además verificar el contenido de los procesadores de seguridad por control de suma de control u otro procedimiento análogo.

Cuando la verificación de los derechos del terminal por la unidad de gestión de acceso es positiva, esta reenvía al terminal un parámetro de mando para permitir el acceso al contenido.

En el caso contrario, no reenvía este parámetro al terminal impidiendo así el acceso al contenido.

Cuando el criterio de acceso es verificado positivamente por la unidad 4 de gestión de acceso, está descifra el criptograma CW^*_{Kecm} con la clave K_{ecm}, recifra la palabra CW de control con la clave K_{ter} conocida específicamente del terminal y reenvía al terminal (flecha 26) el criptograma CW_{Kter} de la palabra de control así recifrada. La clave K_{Ter} es determinada según la identificación del terminal hecha por la unidad de gestión de acceso durante el establecimiento de la conexión punto a punto 12 según un método cualquiera de autentificación del estado de la técnica y exterior al procedimiento.

En una variante particular del procedimiento, el terminal envía (24) a la unidad de gestión de acceso solamente el criptograma CW^*_{Kecm} que entra del ECM. En este caso, la unidad 4 de gestión de acceso considera que el criterio de acceso es implícitamente siempre verificado y efectúa solamente el desciframiento/reciframeinto de la palabra CW de control. Así el operador continúa para controlar la desaleatorización por el terminal por la utilización de la clave específica K_{Ter}.

Según una característica ventajosa del procedimiento, la verificación del criterio de acceso por el módulo de 10 de control de acceso del terminal 6 de recepción y el tratamiento del ECM por la unidad 4 de gestión de acceso son efectuados independientemente la una del otro según una cadencia definida por el operador.

Esta cadencia será descrita después mediante referencia a las figuras 4 a 6.

Como se ha descrito precedentemente, el terminal 6 dispone típicamente:

- de la clave K_{Diff} que representa una instancia de K_{ecm} que le permite obtener el CW cuando el ECM transporta el criptograma CW^*_{KDiff}. Esta clave es común a un conjunto de terminales.

- de la clave K_{Ter}, dedicada a este terminal 6, que permite obtener la palabra CW de control a partir del criptograma CW^*_{KTer} enviado al terminal por la unidad 4 de gestión de acceso.

- de un título de acceso D_{Oper} recibido oficialmente de la unidad 4 de gestión de acceso que conoce la existencia en el terminal 6.

- de un título de acceso D_{Fraud} obtenido fraudulentamente por el usuario del terminal. La detención de este título de acceso por el terminal no es por lo tanto conocido de la unidad 4 de gestión de acceso.

La unidad 4 de gestión de acceso dispone típicamente:

- de la clave K_{Oper} que representa otra instancia de K_{ecm} que le permite obtener la palabra CW de control cuando el ECM transporta el criptograma CW^*_{KOper}. Esta clave es conocida únicamente de la unidad 4 de gestión de acceso.

- de la clave K_{Ter}, dedicada al terminal 6 considerado, que permite suministrar a este terminal 6 la palabra CW de control en forma de un criptograma CW_{KTer}.

- del título de acceso Doper que la unidad 4 de gestión de acceso ha enviado oficialmente al terminal 6.

Con el fin de ilustrar las diferentes situaciones, se definen tres valores distintos para la condición de acceso CA:

- CA_{Oper}: esta condición es satisfecha por la detención (lícita) del derecho D_{Oper} por el terminal,

- CA_{Fraud}: esta condición es satisfecha por la detención fraudulenta de un derecho D_{Fraud} por el terminal 6,

- CA_{Autre}: esta condición no es satisfecha por el terminal que no posee ningún derecho correspondiente.

Las fases A, B y C ilustran el efecto de la cadencia del control de la condición de acceso por el terminal en el acceso al programa.

En A: el ECM es reenviado a la unidad 4 de gestión de acceso por el terminal 6 ya sea porque este último no controla el ECM, ya sea porque ha encontrado un derecho que satisface la condición de acceso pero que la palabra de control es cifrada por la clave K_{Oper} de la que no dispone. Durante este periodo, hay acceso al programa ya que la unidad 4 de gestión de acceso constata que la condición de acceso es satisfactoria. Envía al terminal el criptograma CW^*_{KTer} de la palabra de control cifrada con la clave del terminal.

En B: el ECM es reenviado a la unidad 4 de gestión de acceso ya sea porque el terminal no controla el ECM, ya sea porque ha encontrado un derecho ilícito que satisface la condición de acceso mientras que no tiene la clave K_{Oper}. Durante este periodo, el acceso al programa es prohibido ya que la unidad 4 de gestión de acceso constata que la condición de acceso no puede ser satisfecha por los derechos oficiales del terminal 6. No envía criptograma de la palabra CW de control.

En C: el ECM no es enviado a la unidad 4 de gestión de acceso ya que el terminal dispone de la clave K_{Diff} que permite descifrar el criptograma CW^*_{Kecm}. Si el terminal está en una fase de la cadencia donde debe controlar el criterio de acceso (C1), no hay acceso al programa ya que el criterio de acceso CA_{Autre} no puede ser satisfecho por un derecho disponible en el terminal. Si por el hecho de la cadencia el terminal no controla el criterio de acceso (C2), hay acceso al programa por el solo desciframiento de la palabra de control. Es evidente que este último caso C2 debe ser evitado en la puesta en marcha del procedimiento, por ejemplo forzando el control del criterio del acceso independientemente de la cadencia en cuanto que el criptograma CW^*_{Kecm} puede ser descifrado por el terminal.

Las fases D y E ilustran el efecto de la cadencia del control de la condición de acceso por la unidad 4 de gestión de acceso en el acceso al programa.

En D: hay acceso al programa ya sea porque la unidad 4 de gestión de acceso no controla la condición de acceso y la considera por defecto como satisfactoria, ya sea porque esta unidad 4 de gestión de acceso verifica la condición de acceso y la constata satisfactoria.

En E: hay acceso al programa porque la unidad 4 de gestión de acceso no verifica la condición de acceso y la considera por defecto como satisfactoria mientras que el terminal 6 explota un derecho ilícito.

Las fases K a P ilustran el efecto, en el acceso al programa, de la cadencia del control de la condición de acceso conjuntamente por el terminal y por la unidad 4 de gestión de acceso.

En K: el acceso al programa es autorizado ya que la condición de acceso es constatada satisfactoria por el terminal 6 y/o por la unidad 4 de gestión de acceso y eventualmente estimada satisfactoria por defecto por uno solo de estos dos módulos.

En L: el acceso al programa es autorizado ya que la condición de acceso es constatada satisfactoria por defecto por el terminal 6 y por la unidad 4 de gestión de acceso. Las dos decisiones por defecto son aquí conformadas en la combinación condición de acceso/derecho oficial.

En M: el acceso al programa es autorizado ya que la condición de acceso es constatada satisfactoria efectivamente por el terminal 6 y por defecto por la unidad 4 de gestión de acceso. En este caso, la unidad 4 de gestión de acceso no detecta que el terminal 6 explota un derecho ilícito.

En N: no hay acceso al programa ya que la condición de acceso es constatada como no satisfactoria por la unidad 4 de gestión de acceso que no conoce el derecho ilícito que explota el terminal.

En la primera parte de este caso, la unidad 4 de gestión de acceso detecta que el terminal 6 dispone de un derecho ilícito si el terminal 6 lo precisa que disponga de un derecho válido.

En O: el acceso al programa es autorizado ya que la condición de acceso es estimada satisfactoria por defecto por el terminal 6 y por la unidad 4 de gestión de acceso.

En P: el ECM no es enviado a la unidad 4 de gestión de acceso ya que el terminal dispone de la clave K_{Diff} utilizada para cifrar la palabra CW de control. El control por la unidad de gestión de acceso es inefectivo. Esta fase es similar a la fase C descrita más arriba y debe beneficiar de la misma implementación particular para evitar que, fuera del control por el terminal, pueda tener acceso al programa.

Las etapas del procedimiento van ahora a ser descritas en referencia a la figura 7.

En esta figura 7, las etapas representadas en la parte izquierda corresponden a los tratamientos realizados por el terminal 6, y las de la parte derecha en los tratamientos realizados por la unidad 4 de gestión de acceso.

Cuando el abonado quiere acceder a un programa, el terminal 6 adquiere los flujos digitales que contienen los componentes video, audio y otros del programa así como los mensajes ECM.

En cada mensaje ECM recibido (etapa 30), el terminal verifica si está en un periodo en el que debe controlar la condición de acceso (etapa 32). El test efectuado en la etapa 32 materializa la cadencia del procedimiento al nivel del terminal 6. Si este último debe efectuar este control (flecha 34), la condición de acceso contenido en el ECM es comparada a los derechos presentes en el terminal (etapa 36).

Si ningún derecho satisface la condición de acceso (flecha 38), el tratamiento del ECM se termina, no hay acceso al programa y el terminal 6 espera el mensaje ECM siguiente (etapa 30). Si la condición de acceso es satisfactoria por un derecho presente en el terminal (flecha 40), el terminal 6 verifica (etapa 42) si dispone de la clave K_{ecm} permitiéndole descifrar la palabra CW de control. Esta etapa materializa la activación del procedimiento por el operador.

Si el terminal 6 dispone de la clave K_{ecm} (flecha 44), descifra la palabra CW de control (etapa 46) y puede acceder al programa por desaleatorización (etapa 48).

Si no, envía el mensaje ECM a la unidad 4 de gestión de acceso (etapa 52).

En el caso de que el terminal 6 no esté en un periodo en el que debe controlar la condición de acceso (flecha 54), dos escenarios son a considerar:

- o bien verifica (etapa 42) si puede obtener él mismo la palabra CW de control sin recurrir a la unidad 4 de gestión de acceso,

- o bien envía sistemáticamente (etapa 52) el ECM a la unidad 4 de gestión de acceso.

En el primer caso, como se describe anteriormente, descifra (etapa 46) la palabra CW de control si la verificación es positiva. El tratamiento del control de acceso es entonces efectuado por el terminal 6.

En el segundo caso, el terminal 6 debe sistemáticamente solicitar la unidad 4 de gestión de acceso. En este caso, no puede haber un acceso al programa sin control de la condición de acceso por la unidad 4 de gestión de acceso.

Cuando el terminal envía (etapa 52) un ECM a la unidad 4 de gestión de acceso, esta verifica (etapa 60) si está en un periodo en el que debe controlar la condición de acceso del ECM.

La etapa 60 materializa la cadencia del procedimiento al nivel de la unidad 4 de gestión de acceso.

Si la unidad 4 de gestión de acceso debe controlar la condición de acceso (flecha 62), compara (etapa 64) esta condición de acceso con los derechos del terminal 6.

Como ha sido descrito más arriba, la unidad 4 de gestión de acceso efectúa esta comparación a partir de su propia base de datos de los derechos de los terminales de abonados sin consultar explícitamente al terminal 6. Solo los derechos lícitos se consideran en este tratamiento para otorgar o rechazar el acceso a los programas. En la variante puede igualmente efectuar esta comparación consultando a distancia al procesador de seguridad del terminal. En este caso la presencia de derechos ilícitos puede ser detectada por ejemplo por controles de suma de control en los derechos constatados en este procesador.

Si la condición de acceso es satisfactoria (flecha 66) o si la unidad 4 de gestión de acceso no tiene que controlar la condición de acceso (flecha 68), la unidad 4 de gestión de acceso descifra la palaba CW de control de la ECM (etapa 70), cifra la palabra CW de control (etapa 72) obtenida con una clave K_{ter} dedicada al terminal 6 y envía (etapa 74) el criptograma obtenido al terminal 6. Este último descifra (etapa 76) con su clave dedicada la palabra CW de control y desaleatorizar (48) el programa.

Si la unidad 4 de gestión de acceso considera que, conforme a los derechos del terminal 6, la condición de acceso

no es satisfactoria (flecha 78), no suministra al terminal 6 la palabra CW de control que permite la desaletorización del programa.

En una variante de puesta en marcha del procedimiento ilustrado por los trazos de puntos, (flecha 80), en la que el terminal 6 ha precisado vía el ECM, durante la etapa 52, que dispone de un derecho que satisface la condición de acceso, la unidad 4 de gestión de acceso correlaciona entonces (etapa 84) esta información con su propia conclusión y puede detectar (flecha 86) que el terminal 6 está tentado de acceder ilícitamente al contenido y activar (etapa 88) un tratamiento apropiado de tal tentativa de fraude.

El procedimiento cuando es puesto en marcha en un contexto de reutilización de un contenido previamente obtenido según el procedimiento, para la relectura o la redistribución de un contenido registrado, representa la invención.

En este caso, el parámetro enviado por la unidad 4 de gestión de acceso al terminal 6 es un mensaje ECM_R destinado a ser registrado en el terminal con el contenido y que comprende unos criterios de acceso destinados al control de la reutilización de dicho contenido, relectura o redistribución, por ejemplo. Durante la relectura del contenido o de su reutilización, el mensaje ECM_R será, según su constitución, tratado según el procedimiento, haciendo referencia a la unidad 4 de gestión de acceso, o según la técnica anterior por el terminal solo.

El procedimiento puede igualmente aplicarse para reforzar el control de acceso en un sistema DRM.

En este caso, una única clave es generalmente requerida para desaleatorizar el conjunto de un contenido. Esta clave es puesta a disposición independientemente del contenido mismo, encapsulada en una licencia específica en el sistema de recepción destinatario.

En este contexto, el procedimiento propuesto se aplica constituyendo la licencia de forma específica al sistema aguas arriba, de forma que el sistema de recepción no pueda explotar esta licencia sin recurrir al sistema aguas arriba, pudiendo el sistema aguas arriba entonces verificar el derecho del sistema de recepción a acceder al contenido considerado, y después reconstituir llegado el caso la licencia de forma específica en este sistema de recepción.

La figura 8 ilustra esquemáticamente una arquitectura de distribución de contenidos y/o de servicios, designados a continuación como “contenidos”, en la que un operador 100 suministra un contenido aleatorizado en un conjunto de terminales (102, 104, 106, 108) de una misma entidad, tal como una misma residencia familiar, que reagrupa varios terminales para permitir a un abonado visualizar en varios receptores audiovisuales contenidos diferentes, en función de diversos derechos atribuidos a este abonado por el operador.

En el ejemplo ilustrado por esta figura 8, el terminal maestro 102 y los terminales esclavos están dotados de dispositivos de demodulación (demodulador DVB-S, DVB-C, DVB-T, módem IP,…) adaptados a las redes de distribución a las que están conectados. Además, en este ejemplo, el terminal maestro 102 está dotado de un procesador de seguridad, tal como una tarjeta inteligente 109 y los terminales esclavos (104, 106, 108) no disponen de tarjeta inteligente sino que permiten acceder a los contenidos del operador conectándose al terminal maestro 102 por el que podrán obtener el acceso a dichos contenidos.

Nótese que el terminal maestro 102 puede ser utilizado por el abonado para acceder a los contenidos de forma clásica.

El terminal maestro 102 y el terminal esclavo 104 reciben directamente (flechas 105) del operador 100 un contenido aleatorizado, el terminal esclavo 106 recibe (flecha 107) un contenido vía el terminal maestro 102, el terminal esclavo 108 recibe (flecha 110) un contenido registrado en una memoria local 111 del terminal maestro 102 o en una memoria local del terminal esclavo 106 (flecha 112).

Nótese, no obstante, que un terminal esclavo (104, 106, 108) puede estar dotado sin embargo de una tarjeta inteligente que permite efectuar el control de acceso a los contenidos parcialmente mediante el terminal esclavo y parcialmente mediante el terminal maestro, según una cadencia controlada por el operador tal como la descrita precedentemente.

La arquitectura descrita en la figura 8 se aplica igualmente a otras entidades tales como un servidor pasarela (*home gateway*) o una antena colectiva sin salir del marco de la invención.

En cualquier caso, los terminales esclavos 104, 106 y 108 disponen cada uno de una conexión punto a punto (flecha 115) con el terminal maestro 102, y reenvían a dicho terminal maestro 102 vía esta conexión punto a punto una información extraída de la condición de acceso asociada al contenido para permitir al terminal maestro 102 gestionar el control de acceso a este contenido.

Esta arquitectura además puede ser extendida a una organización en cascada de los terminales. En efecto, un terminal esclavo puede ser el terminal maestro de otros terminales esclavos que le son conectados. Esta capacidad

de extensión permite construir topologías funcionales particulares de terminales. La limitación de tal extensión de arquitectura procede de los tiempos de respuesta inducidos por las cascadas múltiples de terminales.

En un modo preferido de realización, los terminales esclavos están equipados con un chip electrónico asegurado con el que proceden al desciframiento del criptograma de la palabra de control suministrado por el terminal maestro.

En este caso, la seguridad del acceso al contenido por uno de los terminales esclavos 104, 106 y 108 se obtiene gracias a la utilización conjunta de la única tarjeta inteligente en cada uno de los terminales esclavos 104, 106 y 108. En otro modo de realización esta función de desciframiento se efectúa mediante un módulo de software dedicado asegurado del terminal esclavo.

La solución se aplica tanto a los contenidos difundidos en directo como a los contenidos previamente registrados por el terminal maestro 102 o por otro terminal esclavo 106.

El operador puede definir desde su sistema aguas arriba los terminales esclavos autorizados a ser registrados por el terminal maestro, introduciendo así una noción de dominio. Así, un terminal esclavo no autorizado no podrá descifrar los contenidos resultantes del terminal maestro.

En un modo preferido de realización, el operador controla los terminales esclavos habilitados para funcionar con un terminal maestro controlando la distribución de la clave de sesión, como será descrito más adelante.

En la variante, el operador puede igualmente limitar el número de terminales esclavos que pueden hacer referencia a un mismo terminal maestro creando una lista explícita que contiene los identificadores de los terminales autorizados o prohibidos. En este caso el control de un terminal esclavo resulta de su habilitación para disponer de una conexión punto a punto establecida con el terminal maestro. El número de terminales autorizados en la lista puede entonces ser elegido por el operador.

En cualquier caso, solo los terminales esclavos autorizados reciben una clave de sesión compatible con el terminal maestro al que están unidos.

La eliminación de un terminal esclavo de la lista de los terminales autorizados es igualmente controlada por el operador típicamente excluyendo este terminal de la lista de terminales esclavos a los que es enviada una nueva clave de sesión.

Recepción y registro de los contenidos por el terminal “maestro”

El acceso a los contenidos por el terminal maestro, para su utilización, su registro o su lectura, es controlado conforme al procedimiento de la figura 1 descrita precedentemente, por solicitación de su tarjeta inteligente si el terminal está dotado y/o de la unidad 4 de gestión de acceso del operador. En la recepción de la condición de acceso, el terminal maestro 102 reenvía al menos una información de dicha condición de acceso a la unidad 4 de gestión de acceso vía la conexión punto a punto 12. Esta última trata dicha información para autorizar o impedir la utilización del contenido por el terminal maestro 102. Este tratamiento de los contenidos por el terminal maestro no es modificado por el hecho de que los terminales esclavos puedan solicitarlo por otro lado.

Por el contrario, por su estatus de maestro, el terminal maestro 102 dispone de la funcionalidad suplementaria que le permite ser solicitado por unos terminales esclavos 104, 106, 108 para controlar su acceso a unos contenidos. Puede además estar dotado de la capacidad de transmitir a unos terminales esclavos los contenidos que recibe (terminal 106) o unos contenidos que ha registrado (terminal 108). Esta operación es controlada por el operador programando, en el terminal maestro 102, los flujos/servicios que pueden ser redirigidos hacia uno (o los) de los terminales esclavos 104, 106 ó 108.

Utilización de un contenido por un terminal esclavo

Un terminal esclavo recibe los contenidos/servicios directamente (terminal 104) de la fuente aguas arriba, vía una conexión satélite por ejemplo, a través (terminal 106) del terminal maestro, o después de su registro (terminal 108) en otro terminal maestro o esclavo.

En la recepción del contenido y de la condición de acceso asociado (ECM), el terminal esclavo 104, 106 ó 108 se conecta al terminal maestro 102 vía el canal 115 de comunicación, y transmite el mensaje ECM al terminal maestro 102 para tratamiento. En la medida en que los datos enviados al terminal maestro 102 por el terminal esclavo 104, 106 y 108 son cifrados, el canal 115 de comunicación puede no estar asegurado.

El terminal maestro 102 somete después al ECM a la tarjeta inteligente 109 que descifra la palabra CW de control si las condiciones de acceso son remplazadas, y la recifra localmente con una clave de sesión K_S.

La palabra CW de control así recifrada localmente es enviada por el terminal maestro 102 al terminal esclavo 104,

106 ó 108.

En la recepción de la palabra CW de control así recifrada, el terminal esclavo 104, 106 ó 108 somete al criptograma del CW al chip electrónico asegurado que efectúa el desciframiento con la clave de sesión K_S y aplica la palabra CW de control descifrada en el desaleatorizador.

Nótese que el operador puede controlar si un terminal esclavo 104, 106 ó 108 está asociado al terminal maestro 102 controlando la presencia de la clave de sesión K_S en este terminal esclavo. Así solo un terminal esclavo que dispone de la buena clave de sesión K_S está en condiciones de obtener la palabra CW de control, y por lo tanto de descifrar los contenidos redistribuidos por el terminal maestro 102 o recibidos directamente.

Nótese igualmente que la función del chip electrónico asegurada puede ser reemplazada por un procesador de seguridad, tal como una tarjeta inteligente, o un módulo de software sin salir del marco de la invención.

El procedimiento según la invención se aplica igualmente cuando el terminal esclavo 106, en lugar de explotar directamente (típicamente visualizar) el contenido, lo registra en una memoria local 120. En este caso, si las condiciones de acceso son satisfactorias, el terminal maestro 102 suministra al terminal esclavo 106 mensajes ECM para registrar con el flujo.

En la relectura de un contenido registrado, el terminal esclavo 106 ó 108 hace referencia, como para un contenido tratado en su recepción, al terminal maestro 102 para tratar las condiciones de acceso.

Gestión de la clave de sesión

La clave de sesión destinada a cifrar la palabra CW de control que el terminal maestro 102 envía al terminal esclavo 104, 106 ó 108 es conocida del terminal maestro 102 y unos terminales esclavos 104, 106 y 108 de un mismo parque.

Esta clave de sesión es cargada en los terminales 102, 104, 106, 108 en la constitución del parque, durante una etapa de inicialización de estos terminales. En un modo preferido de realización esta clave de sesión es cargada por el operador en la tarjeta inteligente del terminal maestro 102 mediante un mensaje de gestión (EMM). Es enviada igualmente por el operador al terminal esclavo 104, 106 ó 108, por ejemplo por mensaje EMM, para ser registrada en el chip electrónico asegurado. Estos cargos mediante EMM pueden referirse a la clave de sesión misma o a un dato, típicamente secreto, que sirve a las dos partes para calcular la clave de sesión.

La figura 9 ilustra esquemáticamente un procedimiento de control de la habilitación de un terminal esclavo para explotar el contenido digital.

En el ejemplo ilustrado por esta figura 9, una dirección @i es atribuida a cada terminal del parque. Los terminales 102 y 104, de direcciones respectivas @0 y @1, disponen de la misma clave de sesión K1 cargada por el operador mientras que el terminal 106 de dirección @2 dispone de otra clave de sesión K2. El terminal esclavo 104 puede cooperar con el terminal maestro 102, ya que puede descifrar el criptograma CW^*_{K1} con la clave K1 para obtener la palabra CW de control.

Por el contrario, el terminal esclavo 106 que dispone de la clave de sesión K2 no puede descifrar el criptograma CM^*_{K1} que le sería enviado por el terminal maestro 102 que utiliza la clave de sesión K1.

Resulta que el operador controla enteramente el reparto de tarjeta entre los terminales por el control de la clave de sesión compartida por el terminal maestro 102 y los terminales esclavos (104, 106).

Control del uso normal de un terminal

El procedimiento puede ser utilizado por un mismo terminal maestro para tratar uno o varios ECM. En efecto, un terminal puede solicitar la unidad 4 de gestión de acceso (figura 1) para tratar la vía ECM que le permite acceder a un contenido. Puede igualmente solicitar esta unidad 4 de gestión de acceso para tratar simultáneamente varios contenidos, lo que se traduce por tantas vías ECM a tratar.

El acceso simultaneado en varios contenidos por el mismo terminal maestro 102 puede ser normal. Es el caso en el que un programa es constituido de varios componentes tales como por ejemplo una condición de acceso en la imagen y el sonido original, otra para una lengua diferente, otra incluso para los subtítulos para sordos. Es igualmente el caso cuando el terminal es un terminal pasarela, es decir un equipo servidor de punto de entrada en una misma entidad (un mismo foco por ejemplo) y que federa los accesos de varios terminales a los contenidos distribuidos.

Por el contrario, el acceso simultáneo a varios contenidos por el mismo terminal maestro 102 puede ser utilizado para desviar un acceso oficial y multiplicar el acceso a unos contenidos sin autorización.

Una solución para detectar este desvío consiste en observar, durante un periodo dado, el número y el tipo de peticiones formuladas a la unidad 4 de gestión de acceso por un mismo terminal maestro 102, y diagnosticar, según el contexto, si este terminal es o no utilizado fraudulentamente.

La observación del tipo de petición permite determinar, particularmente, si el terminal maestro 102 somete a tratamiento la misma vía ECM o varías vías ECM, y en este último caso si estas vías ECM están correlacionadas, es decir, son relativas al mismo programa, o independientes, es decir, relativas a programas diferentes. Se constata igualmente que el terminal maestro repita unas peticiones de acceso en un contenido del cual no tiene normalmente los derechos de acceso.

El número de peticiones así reveladas, según su tipo, es comparado con un umbral más allá del cual la unidad 4 de gestión de acceso diagnostica que se trata de una tentativa de pirateo y toma las medidas en consecuencia, tales como el paro de transmisión, a este terminal, de los datos que permiten el acceso a los contenidos.

La contabilización de las peticiones, la toma en cuenta de los tipos de peticiones, la determinación del periodo de observación, el ajuste del umbral son modulables en función de la permisibilidad o la severidad que quiera darse a este control.

El control por el terminal maestro del uso normal de un terminal esclavo puede igualmente ser efectuado según el mismo procedimiento.

En los modos de realización descritos anteriormente, ya que el terminal no puede tratar un ECM para extraer las palabras de control, este envía este ECM a la unidad 4 de gestión o al terminal maestro 102 para obtener estas palabras de control que permiten descifrar el contenido. Como ha sido descrito precedentemente, esta transferencia/tratamiento de ECM se efectúa ocasionalmente o en cada criptoperiodo.

Para que el terminal disponga de las palabras de control a tiempo para desaleatorizar el contenido, la duración global de la transferencia/tratamiento de ECM por la unidad 4 de gestión o por el terminal maestro 102, visto desde el terminal de recepción, debe ser inferior a la longitud de un criptoperiodo.

Esta condición en la duración global de la transferencia/tratamiento permite el funcionamiento correcto del conjunto del sistema durante el acceso “simple” a un contenido, es decir a velocidad normal con un criptoperiodo del orden de una decena de segundos tal como se practica usualmente.

No obstante hay otros casos de utilización en los que esta condición en la duración global de transferencia/tratamiento puede no ser técnicamente satisfecha, lo que conduce a una discontinuidad, incluso una imposibilidad de desaleatorización.

En un primer ejemplo, funciones tales como la relectura de un contenido registrado en el terminal (PVR) o en la red (nPVR), o servicios tales como la VOD (*Video on Demand*) pueden ofrecer al usuario la posibilidad de recibir un contenido a velocidades más elevadas que la normal, antes o después (*trick modes*). Durante un acceso rápido delantero o trasero, la frecuencia aparente de los ECM en el contenido aumenta y la duración de criptoperiodo aparente disminuye. Resulta que el intervalo de tiempo entre dos sumisiones de ECM por el terminal de recepción en la unidad de gestión o en el terminal maestro disminuye. Más allá de una cierta velocidad de acceso al contenido, la duración entre dos sumisiones de ECM puede ser más corta que la cura global de transferencia/tratamiento de un ECM. El sistema diverge y ya no funciona.

En otro ejemplo, con el fin de reforzar la protección del contenido, el operador puede disminuir la longitud del criptoperiodo para acelerar la renovación de las palabras de control y así aumentar la dificultad de un ataque por fuerza bruta en los criptogramas de las palabras de control o en el contenido aleatorizado. Más allá de una cierta disminución del criptoperiodo, la duración entre dos sumisiones de ECM se hace más corta que la duración global de transferencia/tratamiento de un ECM. Como en el ejemplo precedente, el sistema diverge y ya no funciona.

Utilización del procedimiento en acceso rápido delantero o trasero

Con el fin de paliar este inconveniente de divergencia y de disfuncionamiento del sistema en utilizaciones particulares, una solución consiste en reducir la frecuencia de sumisión de los ECM por el terminal de recepción en la unidad 4 de gestión de acceso o en el terminal maestro 102, conservando una parte del control del acceso por estos. Se explota así la característica del procedimiento según la cual los ECM son enviados ocasionalmente por el terminal de recepción a la unidad de gestión o al terminal maestro.

El principio de esta solución consiste en recortar la duración del contenido en segmentos temporales durante cada uno de los cuales el terminal de recepción puede tratar los ECM sin hacer referencia a la unidad de gestión o al terminal maestro. No obstante, durante el paso de un segmento a otro, el terminal de recepción debe hacer referencia a la unidad de gestión o al terminal maestro para disponer de las informaciones, típicamente la clave

necesaria en el desciframiento de las palabras de control o los títulos de acceso que satisfacen el criterio de acceso al contenido, permitiéndole tratar los ECM durante este nuevo segmento.

Preferentemente, el terminal debe hacer referencia a la unidad de gestión o al terminal maestro para obtener la clave de desciframiento de las palabras de control para el segmento temporal que viene, lo que conduce a que satisfaga siempre la condición de acceso, ya sea disponiendo de los títulos de acceso necesarios, ya sea no controlando esta condición.

Esta solución es aplicable en diversas utilizaciones tales como las presentadas más arriba y es descrita después en el caso de los accesos delantero y trasero rápidos a un contenido por un terminal de recepción conectado a una unidad (4) de gestión.

A este efecto, cuando el contenido es suministrado en el terminal 6 de recepción por un operador al que está asociada una unidad 4 de gestión de acceso, el procedimiento comprende una fase de condicionamiento del contenido por el operador y una fase de explotación de dicho contenido por el terminal de recepción.

La fase de condicionamiento del contenido comprende las siguientes etapas:

a) la duración de dicho contenido es recortada en N segmentos temporales a cada uno de los cuales están asociados un identificador S_j, una clave K_j y un dato D_j relativo a esta clave, comprendiendo cada segmento S_j un número entero M_j de criptoperiodos CP_i para i=1 en M_j,

b) el contenido es aleatorizado utilizando palabras de control $CW_{i, j}$ para i=1 en M_j y j=1 en N,

c) cada palabra $CW_{i, j}$ de control es cifrada por la clave K_j,

d) después el contenido, durante cada segmento temporal S_j, es transmitido aleatorizado al terminal, a cada criptoperiodo CP_i, con un mensaje EMC que comprende al menos el criptograma de la palabra $CW_{i, j}$ de control cifrada con la clave actual K_j, el dato D_j relativo a la clave actual K_j, el dato D_{j-1} relativo a la clave precedente K_{j-1} y el dato D_{j+1} relativo a la clave siguiente K_{j+1}.

Se designa con “segmento actual” el segmento S_j en curso de recepción por el terminal; la clave K_j asociada es señalada “clave actual”. Se comprende que en acceso al contenido delantero el terminal recibe los segmentos sucesivos en la orden… S_j, S_{j+1}, S_{j+2}…, siendo el segmento 3_{j+1} el “segmento siguiente” del segmento S_j en el contenido y utilizando la “clave siguiente” K_{j+1}, mientras que en acceso al contenido trasero el terminal recibe los segmentos sucesivos en el orden… S_j, S_{j-1}, S_{j-2}…siendo el segmento S_{j-1} el “segmento precedente” del segmento S_j en el contenido y que utiliza la “clave precedente” K_{j-1}.

La fase de explotación del contenido pone en marcha tres dobletes para la memorización de los cuales el terminal ha sido previamente configurado. Estos dobletes (K_c, D_c), K_p, D_p), (K_s, D_s) están constituidos respectivamente por una clave actual K_c y por un dato D_c relativo a esta clave, de una clave precedente K_p y de un dato relativo D_p, y de una clave siguiente K_S y de un dato relativo D_s.

La fase de explotación comprende las siguientes etapas, en la recepción de cada mensaje ECM:

e) El terminal analiza el dato D_j contenido en el mensaje ECM y evalúa la correspondencia con los datos de los cuales dispone en los dobletes.

f) Si el dato D_j contenido en el mensaje ECM corresponde al dato D_c previamente memorizado en el terminal, el terminal descifra las palabras $CW_{i, j}$ de control con la clave K_c asociada, en el doblete correspondiente, a este dato D_c. En este caso ningún tratamiento complementario del ECM es para solicitar por el terminal a la unidad de gestión.

g) Si el dato D_j contenido en el mensaje ECM corresponde al dato D_p, previamente memorizado en el terminal, el terminal descifra las palabras $CW_{i, j}$ de control con la clave K_p asociada, en el doblete correspondiente, al dato D_p. Esto se produce en lectura trasera de un contenido durante el paso al segmento precedente. De la misma forma si el dato D_j contenido en el mensaje ECM corresponde al dato D_s, el terminal descifra las palabras $CW_{i, j}$ de control con la clave K_s. Esto se produce en lectura delantera de un contenido durante el paso al segmento siguiente.

h) En definitiva, si el dato D_j contenido en el mensaje ECM no corresponde al dato D_c previamente memorizado en el terminal, el terminal envía el mensaje ECM recibido en la unidad (4) de gestión de acceso que determina la clave actual K_j a partir del dato D_j, la clave precedente K_{j-1} a partir del dato D_{j-1} y la clave siguiente K_{j+1} a partir del dato D_{j+1} y envía estas claves y sus datos relativos al terminal, que memoriza sus valores respectivamente como nuevos valores de las claves K_c, K_p y K_s y unos datos D_c, D_p y D_s relativos a estas claves. Esto se produce en cada paso de un segmento al otro de un mismo contenido, en lectura delantera como en lectura trasera, durante el paso de un contenido a otro y cuando el terminal acaba de ser inicializado y que los tres dobletes no han sido todavía puestos al día.

Conforme al problema planteado, la combinación de las etapas f), g) y h) permite compensar una duración global de transferencia/tratamiento excesivo en relación con el criptoperiodo, conservando un control del acceso al contenido mediante la unidad de gestión. En efecto, la presencia en el terminal de la clave actual K_c le permite descifrar las palabras de control si hacer referencia a la unidad de gestión. No obstante, esta clave no es válida más que durante la duración del segmento actual (etapa f, utilización de la clave actual). Al final del segmento el terminal debe tener en cuenta otra clave de desciframiento. Para poder desaleatorizar el contenido sin discontinuidad, el terminal dispone ya de esta nueva clave (etapa g, utilización de la clave precedente o de la clave siguiente). No obstante, para que al final de este nuevo segmento el terminal pueda siempre desaleatorizar sin discontinuidad, debe hacer referencia a la unidad de gestión para tratar el ECM que le permitirá poner su sistema de claves al día (etapa h). En la recepción del ECM que sigue a esta puesta al día, se volverá a centrar entonces en su nueva clave actual (vuelta a la etapa f). Así, la desaleatorización se persigue aunque el suministro de claves por la unidad de gestión tenga una duración superior al criptoperiodo, y la unidad de gestión conserva el control del acceso al contenido ya que el terminal debe hacer referencia una vez en el curso de cada uno de los segmentos.

Se comprende así que el terminal debe satisfacer la condición de acceso, ya sea disponiendo de títulos de acceso, ya sea ignorando esta condición, ya que en el caso contrario solicitaría la unidad de gestión a cada ECM lo que conduciría a la divergencia del sistema citado anteriormente. Se señala además que la unidad de gestión, cuando recibe un ECM para determinar las claves del terminal, puede verificar como en el procedimiento de base que el terminal disponga efectivamente de los títulos de acceso que satisfacen los criterios de acceso y no de los títulos de acceso ilícitos.

Según una característica de la invención, el terminal reenvía dicho mensaje ECM recibido a la unidad 4 de gestión de acceso vía una conexión punto a punto.

Las claves actual K_j, precedente K_{j-1} y siguiente K_{j+1} cuyo terminal debe disponer en sus dobletes según la solución son determinados a partir de los datos relativos a estas claves presentes en el ECM.

En un primer modo de realización, los datos relativos a las claves transmitidas en el ECM comprenden al menos los criptogramas respectivos de dichas claves K_j, K_{j-1} y K_{j+1} que pueden ser descifrados por una clave de gestión conocida exclusivamente de la unidad 4 de gestión de acceso.

En un segundo modo de realización, los datos relativos a las claves transmitidas en el ECM comprenden al menos los identificadores S_j, S_{j-1} y S_{j+1} de los segmentos correspondientes. Cuando los datos relativos no comprenden los criptogramas de dichas claves, las claves K_j, K_{j-1} y K_{j+1} son respectivamente determinadas por la unidad 4 de gestión a partir de estos identificadores de segmentos.

En una primera puesta en marcha de este modo de realización, la unidad 4 de gestión de acceso determina las nuevas claves K_j, K_{j-1} y K_{j+1} por búsqueda en una base de datos predefinida a partir de los identificadores de segmentos.

En otro modo de puesta en marcha, la unidad 4 de gestión de acceso determina las nuevas claves K_j, K_{j-1} y K_{j+1} por diversificación de una clave raíz a partir de los identificadores de segmentos.

Durante las etapas e) a h), el terminal evalúa la correspondencia entre el dato relativo recibido D_j y los datos D_c, D_p y D_s de los cuales dispone en sus dobletes. Preferentemente, esta correspondencia se refiere a la igualdad de los identificadores de segmentos. Cuando los identificadores de segmentos no son puestos en marcha, la búsqueda de correspondencia consiste en comparar los criptogramas de las claves.

En un tercer modo de realización solo el dato D_j relativo a la clave actual K_j está presente en el mensaje ECM, y la unidad 4 de gestión de acceso deducida de este dato los dos otros datos D_{j-1} y D_{j+1} relativos a las claves precedentes K_{j-1}, y siguiente K_{j+1}. En un primer ejemplo, los datos relativos a las claves son unos identificadores de segmentos de valores digitales sucesivos… X-2, X-1, X, X+1, X+2… En otro ejemplo, los datos relativos a las claves son los criptogramas de estas claves y la unidad de gestión dispone con antelación de la lista de estos criptogramas ordenados según la orden de sucesión de los segmentos. Cuando el criptograma de la clave K_j se encuentra en esta lista, el criptograma que le precede es el de la clave K_{j-1} y el criptograma que le sigue es el de la clave K_{j+1}.

En la variante, si la lectura trasera de un contenido no es puesta en marcha, el dato D_{j-1} relativo a la clave precedente K_{j-1} no es puesto en marcha en los mensaje ECM y el doblete (K_p, D_p) que corresponde al segmento precedente puede ser suprimido permaneciendo en el marco de la solución.

En la variante, el doblete (K_p, D_p) que corresponde al segmento precedente puede ser remplazado por varios dobletes asociados a los n_p segmentos precedentes sucesivos y el doblete (K_s, D_s) que corresponde al segmento siguiente puede ser remplazado por varios dobletes asociados a los n_s segmentos siguientes sucesivos, permaneciendo en el marco de la invención. Esta extensión de los dobletes permite a la solución de aplicarse igual durante el acceso al contenido a una velocidad tal que el retraso global de transferencia/tratamiento del ECM es

superior a la duración aparente de uno o varios segmentos sucesivos. El número de dobletes precedentes n_p o siguientes n_s depende entonces de la velocidad máxima de acceso al contenido que se quiera poder alcanzar.

La solución descrita anteriormente puede igualmente ser puesta en marcha cuando el contenido aleatorizado es distribuido en un parque de terminales receptores que comprende un terminal maestro (102) y al menos un terminal esclavo (104, 106, 108) que depende de dicho terminal maestro (102). En este caso el terminal de recepción es remplazado por el terminal esclavo y, visto desde el terminal esclavo, la unidad de gestión es remplazada por el terminal maestro.

En un modo de realización, el tratamiento del ECM, enviado por el terminal esclavo al terminal maestro para obtener los nuevos valores de los dobletes (K_c, D_c), (K_p, D_p), (K_s, D_s), es efectuado por el terminal maestro mismo que dispone de medios similares a los de una unidad de gestión tales como, según la puesta en marcha, una función de desciframiento por una clave de gestión, una base de datos de los criptogramas.

En otro modo de realización, el terminal maestro (102) determina los nuevos valores de los dobletes (K_c, D_c), (K_p, D_p) (K_s, D_s) a enviar al terminal esclavo enviando para tratamiento el mensaje ECM que recibe en una unidad (4) de gestión o en un terminal maestro del que depende y enfrente de la que/del que se comporta como un terminal esclavo.

La solución preferida descrita más arriba consiste en asociar una clave diferente al segmento, la condición de acceso siendo siempre satisfactoria o ignorada por el terminal. Esta solución se transpone a la evidencia en el caso de que una condición de acceso diferente es asociada a cada segmento, la clave de desciframiento siendo igual y disponible en el terminal. En este caso, los datos D j son relativos a unos derechos y la unidad de gestión suministra al terminal, en lugar de las claves, los derechos necesarios para el acceso a los segmentos actual, siguiente y precedente.

REIVINDICACIONES

1.- Procedimiento de control de acceso a un contenido aleatorizado suministrado a un terminal (6) de recepción por un operador que coopera con una unidad (4) de gestión de acceso, estando dotado dicho terminal (6) de al menos un módulo (10) de control de acceso, procedimiento que comprende las etapas siguientes:

- asociar al contenido una pluralidad de informaciones necesarias en la desaleatorización de dicho contenido,

- transmitir dicho contenido con dicha pluralidad de informaciones a dicho terminal (6), y,

a la recepción de dicha pluralidad de informaciones por el terminal (6):

- reenviar sistemáticamente u ocasionalmente al menos una información entre dicha pluralidad de informaciones a la unidad (4) de gestión de acceso vía una conexión (12) punto a punto,

- verificar mediante la unidad (4) de gestión de acceso si la información reenviada es compatible con unos derechos de acceso previamente concedidos a dicho terminal (6),

- transmitir al terminal al menos un parámetro de mando para permitir la utilización del contenido si la información renviada es compatible con los derechos de acceso previamente concedidos a dicho terminal (6),

- si no, la unidad (4) de gestión no transmite dicho parámetro al terminal (6);

procedimiento en el que el parámetro de mando enviado por la unidad (4) de gestión de acceso al terminal (6) es un mensaje ECM_R destinado a ser registrado con el contenido y que comprende criterios de acceso destinados al control de la reutilización de dicho contenido.

2.- Procedimiento según la reivindicación 1, en el que la pluralidad de informaciones necesarias en la desaleatorización del contenido es transmitida al terminal (6) en un mensaje ECM que comprende al menos un criterio CA de acceso, un criptograma CW^*_{Kecm} de una palabra CW de control cifrada por una clave K_{ecm}.

3.- Procedimiento según la reivindicación 1, en el que el contenido suministrado al terminal (6) es protegido por una licencia DRM.

4.- Sistema de control de acceso que comprende un dispositivo (2) de emisión que comprende un servidor (8) de contenido aleatorizado, una unidad (4) de gestión de acceso asociada a dichos dispositivo (2) de emisión, un terminal (6) de recepción dotado al menos de un módulo (10) de control de acceso a un contenido aleatorizado transmitido por dicho servidor (8) y al que está asociada una pluralidad de informaciones necesarias en la desaleatorización de dicho contenido, estando conectada dicho terminal (6) de recepción a dicha unidad (4) de gestión de acceso por una conexión (12) punto a punto, estando adaptado dicho módulo (10) de control de acceso para reenviar, sistemáticamente u ocasionalmente a dicha unida (4) de gestión de acceso al menos una información contenida en la pluralidad de informaciones necesarias en la desaleatorización del contenido, y porque dicha unidad (4) de gestión de acceso está adaptada para verificar si la información renviada es compatible con unos derechos de acceso previamente concedidos a dicho terminal (6), y para transmitir al terminal (6) al menos un parámetro de mando para permitir la utilización del contenido si la información renviada es compatible con los derechos de acceso previamente concedidos a dicho terminal (6), o para no transmitir dicho parámetro al terminal si la información renviada no es compatible con los derechos de acceso previamente concedidos a dicho terminal (6),

sistema en el que el parámetro de mando enviado por la unidad (4) de gestión de acceso al terminal (6) es un mensaje ECM_R destinado a ser registrado con el contenido y que comprende unos criterios de acceso destinados al control de la reutilización de dicho contenido.

5.- Sistema según la reivindicación 4, en el que la pluralidad de informaciones necesarias en la desaleatorización del contenido es transmitida al terminal (6) en un mensaje ECM que comprende al menos un criterio CA de acceso, un criptograma CW^*_{Kecm} de una palabra CW de control cifrada por una clave K_{ecm}.

6.- Sistema según la reivindicación 5, en el que dicha unidad (4) de gestión de acceso es distinta del dispositivo (2) de emisión.

7.- Sistema según la reivindicación 5, en el que dicha unidad (4) de gestión de acceso está integrada en el dispositivo (2) de emisión.

8.- Terminal (6) de recepción de un contenido aleatorizado transmitido con una pluralidad de informaciones necesarias en la desaleatorización de dicho contenido, estando conectado dicho terminal a una unidad (4) de gestión de acceso vía una conexión (12) punto a punto y que comprende un módulo (10) de control de acceso que comprende unos medios para renviar sistemáticamente u ocasionalmente al menos una información de dicha

pluralidad de informaciones necesarias en la desaleatorización de dicho contenido en la unidad (4) de gestión de acceso vía la conexión (12) punto a punto de manera que permite a dicha unidad (4) de gestión de acceso verificar si la información renviada es compatible con unos derechos de acceso previamente concedidos al terminal (6), y transmitir al terminal (6) al menos un parámetro de mando para permitir la utilización del contenido si la información renviada es compatible con los derechos de acceso previamente concedidos a dicho terminal (6), o para no transmitir dicho parámetro al terminal si la información renviada no es compatible con los derechos de acceso previamente concedidos a dicho terminal (6),

dicho parámetro de mando transmitido por la unidad (4) de gestión de acceso al módulo (10) de control de acceso es un mensaje ECM_R destinado a ser registrado con el contenido y que comprende unos criterios de acceso destinados al control de la reutilización de dicho contenido.

9.- Programa de ordenador memorizado en un soporte de registro y que comprende instrucciones destinadas a la puesta en marcha de un procedimiento de control de acceso según la reivindicación 1 cuando se ejecuta en un ordenador.

10.- Procedimiento de control de acceso según la reivindicación 1, en el que el contenido aleatorizado es distribuido a un parque de terminales receptores y en el que la unidad (4) de gestión de acceso es un terminal maestro entre los terminales del parque de terminales receptores y el terminal (6) de recepción es un terminal esclavo entre los terminales del parque de terminales receptores.

11.- Procedimiento según la reivindicación 10, en el que dicha pluralidad de informaciones necesarias en la desaleatorización de dicho contenido es transmitida en un mensaje ECM que comprende al menos un criterio CA de acceso y un criptograma CW^*_{Kecm} de una palabra CW de control cifrada por una clave K_{ecm}.

12.- Procedimiento según la reivindicación 11, en el que el terminal esclavo (104, 106, 108) renvía al menos el criptograma CW^*_{Kecm} al terminal maestro (102).

13.- Sistema de control de acceso según la reivindicación 4, en el que el contenido aleatorizado es distribuido en un parque de terminales receptores y en el que la unidad (4) de gestión de acceso es un terminal maestro entre los terminales del parque de terminales receptores y el terminal (6) de recepción es un terminal esclavo entre los terminales del parque de terminales receptores.

14.- Sistema según la reivindicación 13, en el que dicho terminal maestro (4, 102) está integrado en el dispositivo (2) de emisión.

15.- Sistema según la reivindicación 16 en el que dicho terminal maestro está integrado en una antena de recepción colectiva.

16.- Sistema según la reivindicación 13 en el que dicho terminal maestro cumple una función de pasarela entre el servidor (8) de contenido y los terminales esclavos (6, 104, 106, 108) del parque.

17.- Programa de ordenador según la reivindicación 9 en el que el contenido aleatorizado es distribuido en un parque de terminales receptores y en el que la unidad (4) de gestión de acceso es un terminal maestro entre los terminales del parque de terminales receptores y del terminal (6) de recepción es un terminal esclavo entre los terminales del parque de terminales receptores.

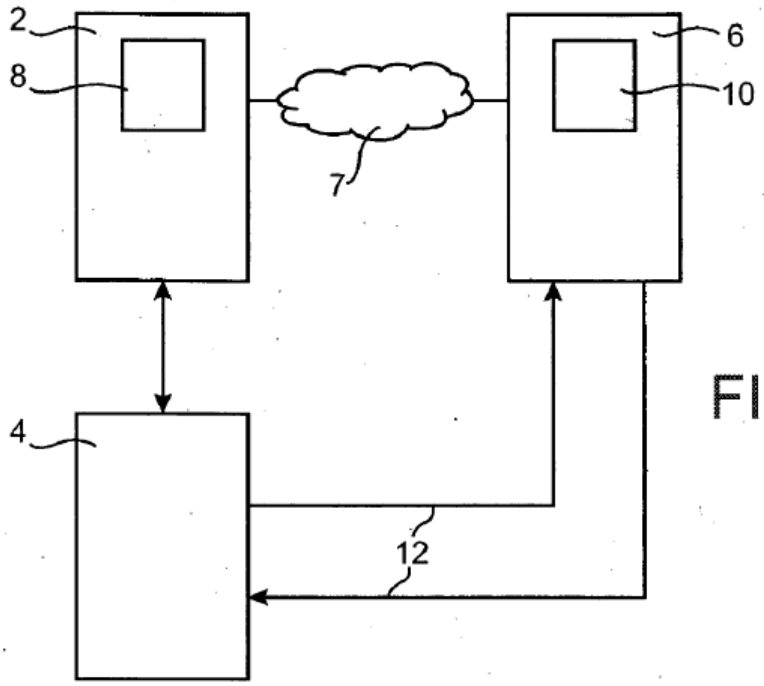

2
8
6
10
7
4
12

FIG. 1

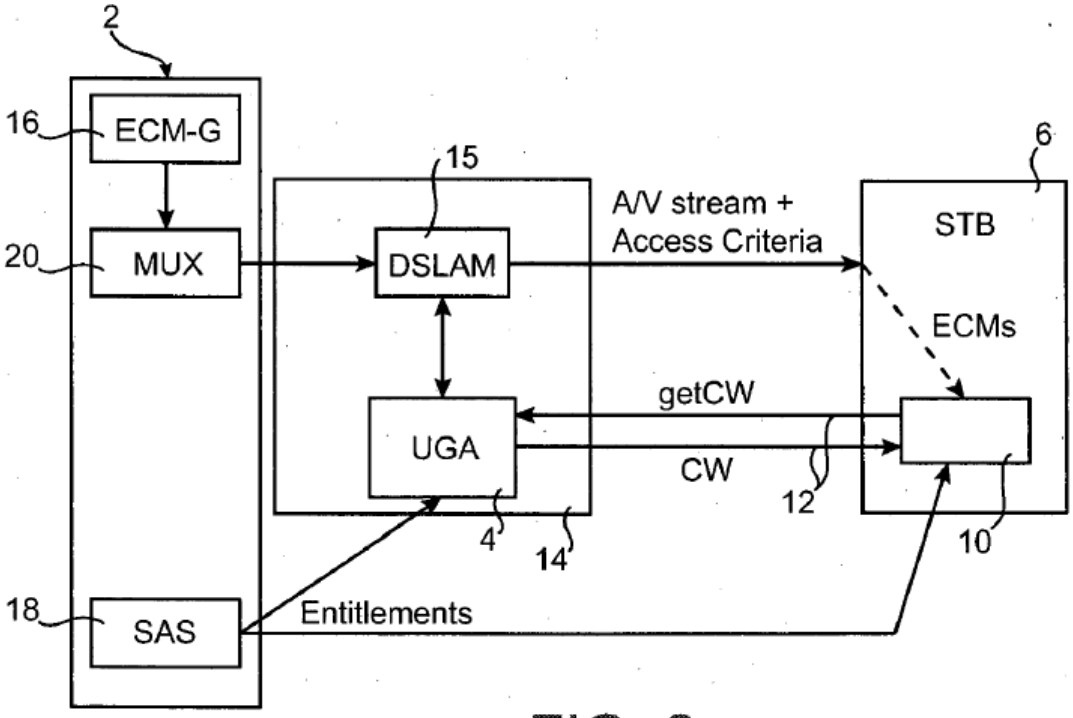

2
16
ECM-G
15
6
20
MUX
DSLAM
A/V stream +
Access Criteria
STB
ECMs
getCW
UGA
CW
12
4
14
10
18
SAS
Entitlements

FIG. 2

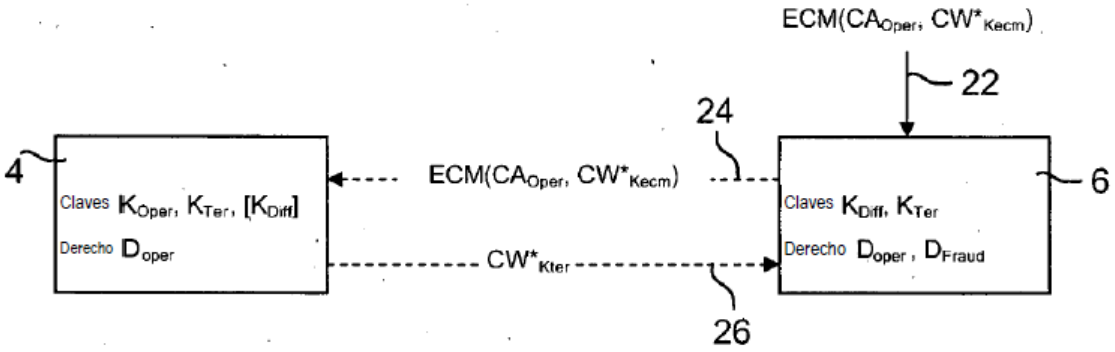

ECM(CA$_{Oper}$, CW*$_{Kecm}$)
22
24
4
ECM(CA$_{Oper}$, CW*$_{Kecm}$)
6
Claves K_{Oper}, K_{Ter}, [K_{Diff}]
Derecho D_{oper}
Claves K_{Diff}, K_{Ter}
Derecho D_{oper}, D_{Fraud}
CW*$_{Kter}$
26

FIG. 3

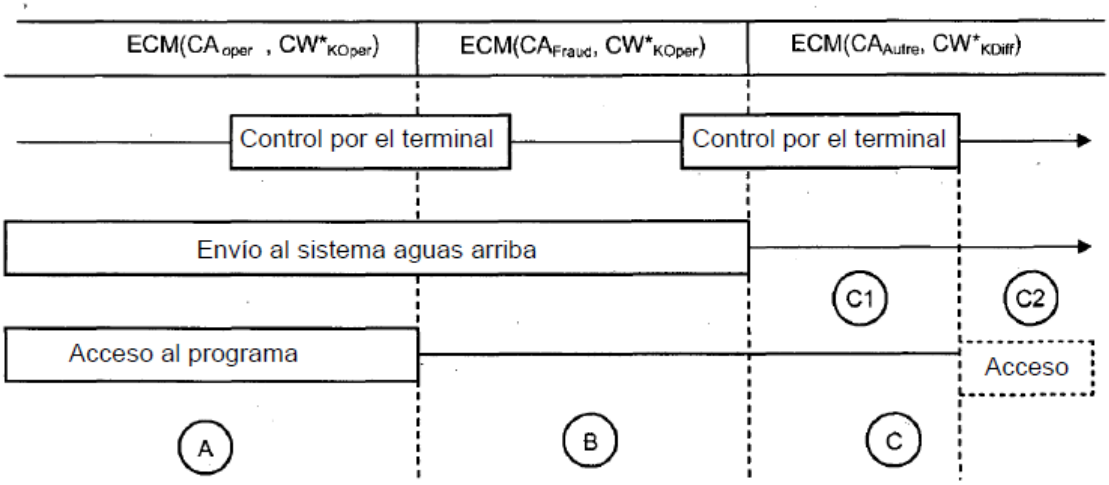

ECM(CA oper , CW*KOper)
ECM(CAFraud, CW*KOper)
ECM(CAAutre, CW*KDiff)
Control por el terminal
Control por el terminal
Envío al sistema aguas arriba
C1
C2
Acceso al programa
Acceso
A
B
C

FIG. 4

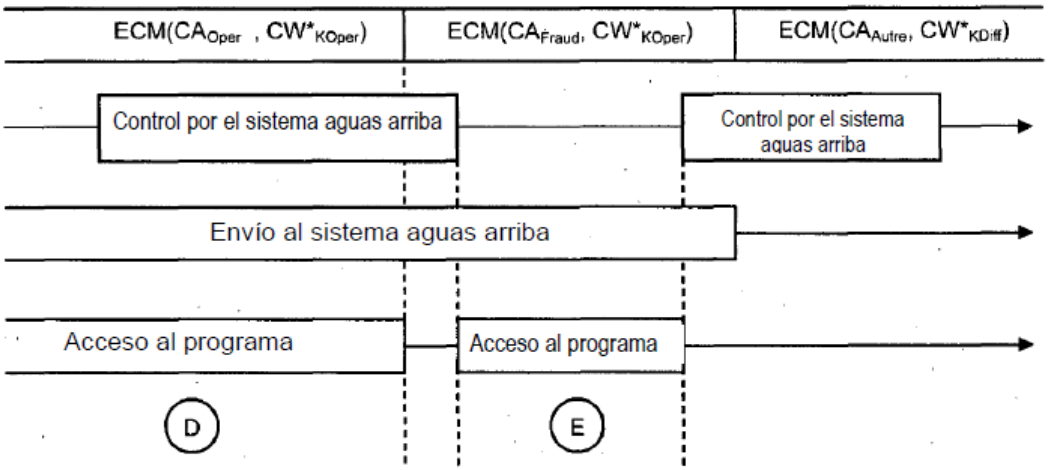

ECM(CAOper , CW*KOper)
ECM(CAFraud, CW*KOper)
ECM(CAAutre, CW*KDiff)
Control por el sistema aguas arriba
Control por el sistema aguas arriba
Envío al sistema aguas arriba
Acceso al programa
Acceso al programa
D
E

FIG. 5

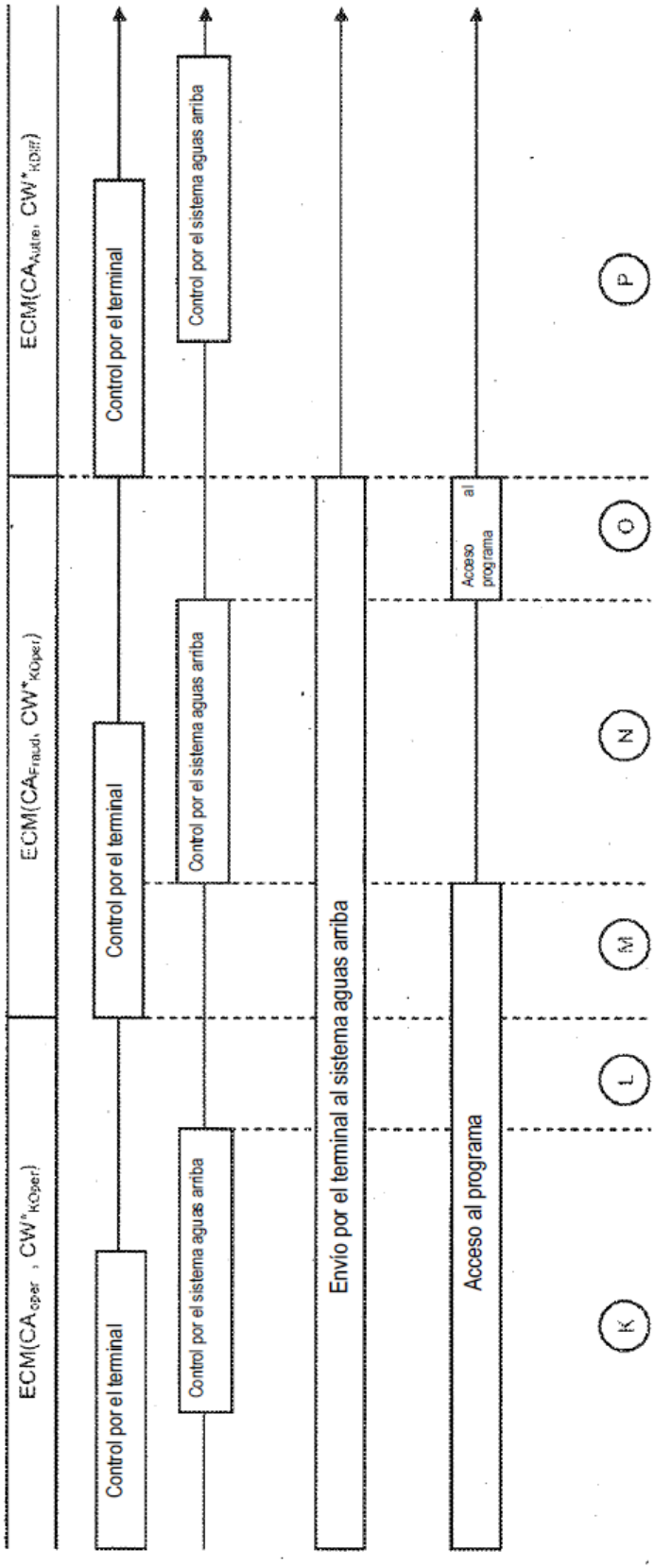
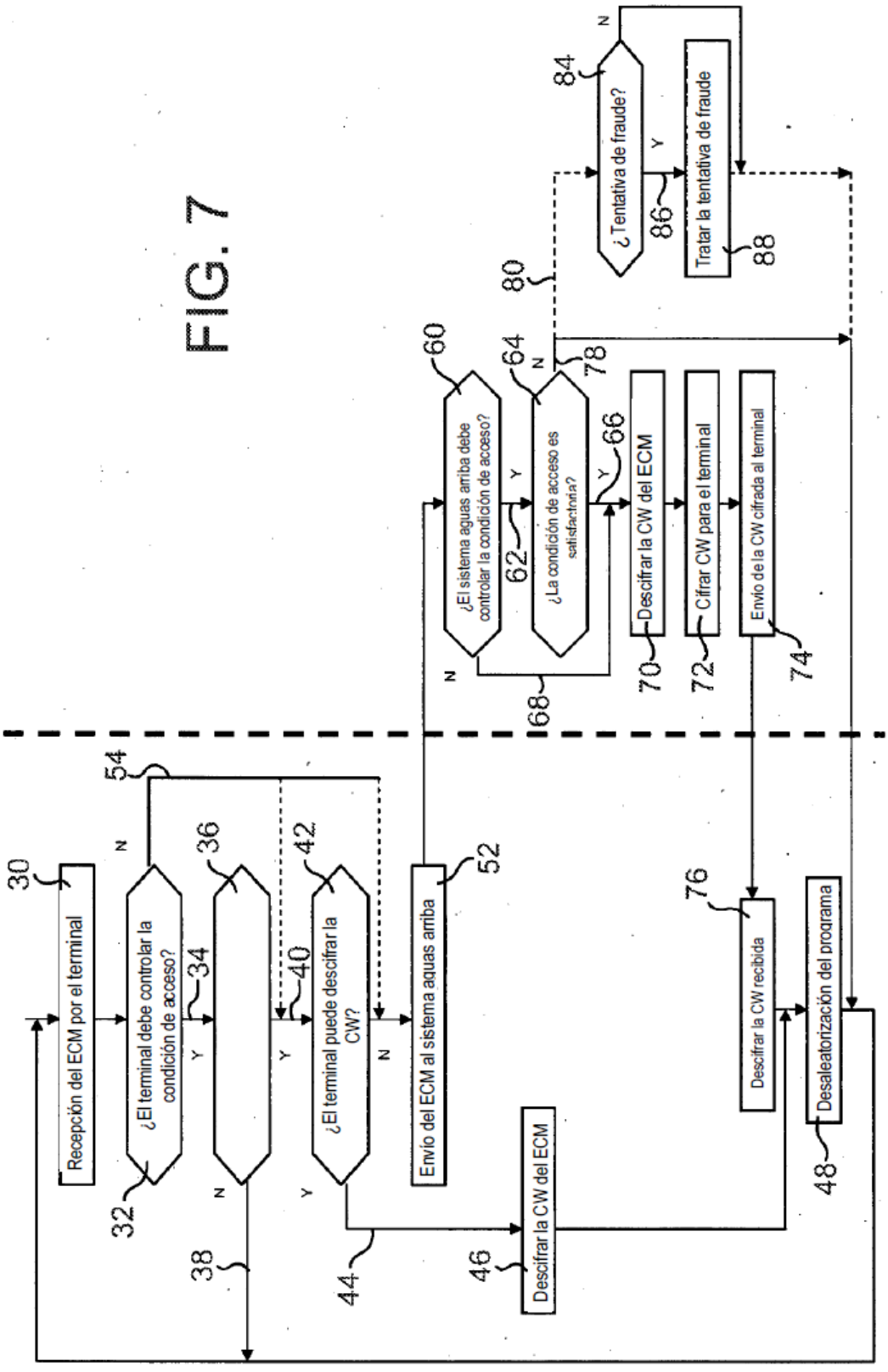

ECM(CA_Oper , CW*_KOper)
ECM(CA_Fraud, CW*_KOper)
ECM(CA_Autre, CW*_KDiff)
Control por el terminal
Control por el sistema aguas arriba
Control por el terminal
Control por el sistema aguas arriba
Control por el terminal
Envío por el terminal al sistema aguas arriba
Acceso al programa
Acceso al programa
K
L
M
N
O
P

FIG. 6

FIG. 7


Recepción del ECM por el terminal
30
¿El terminal debe controlar la condición de acceso?
32
34
36
38
¿El terminal puede descifrar la CW?
40
42
44
Envío del ECM al sistema aguas arriba
52
54
Descifrar la CW del ECM
46
¿El sistema aguas arriba debe controlar la condición de acceso?
60
62
¿La condición de acceso es satisfactoria?
64
66
68
Descifrar la CW del ECM
70
Cifrar CW para el terminal
72
Envío de la CW cifrada al terminal
74
Descifrar la CW recibida
76
Desaleatorización del programa
48
78
80
¿Tentativa de fraude?
84
86
Tratar la tentativa de fraude
88
Y
N

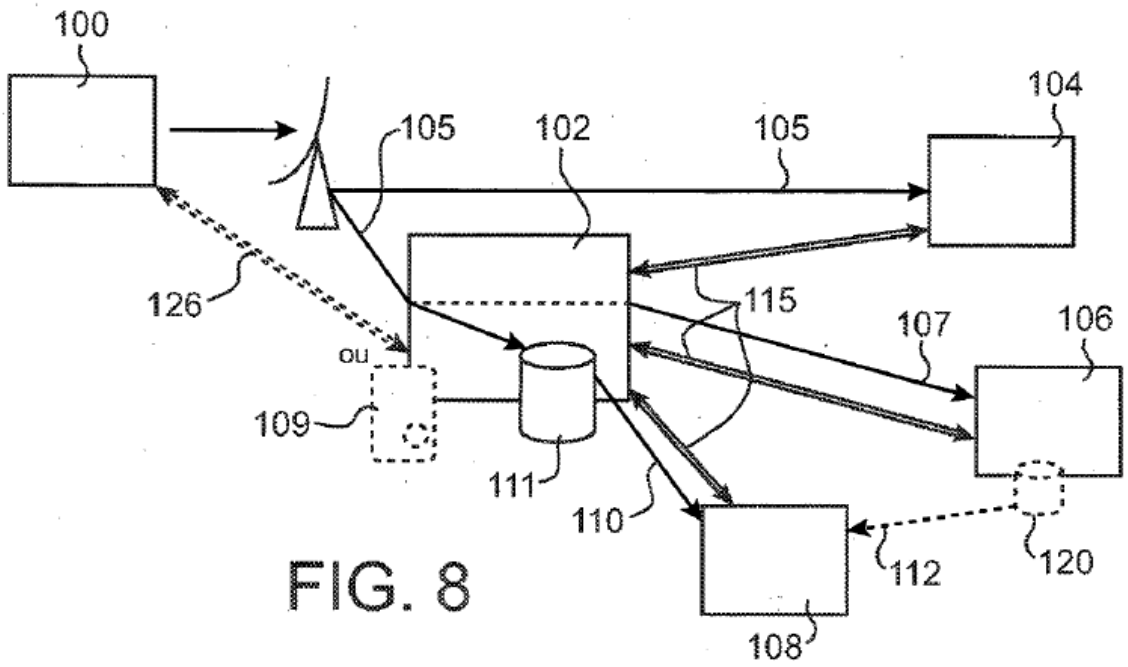

100
105
102
105
104
126
115
107
106
ou
109
111
110
112
120
108

FIG. 8

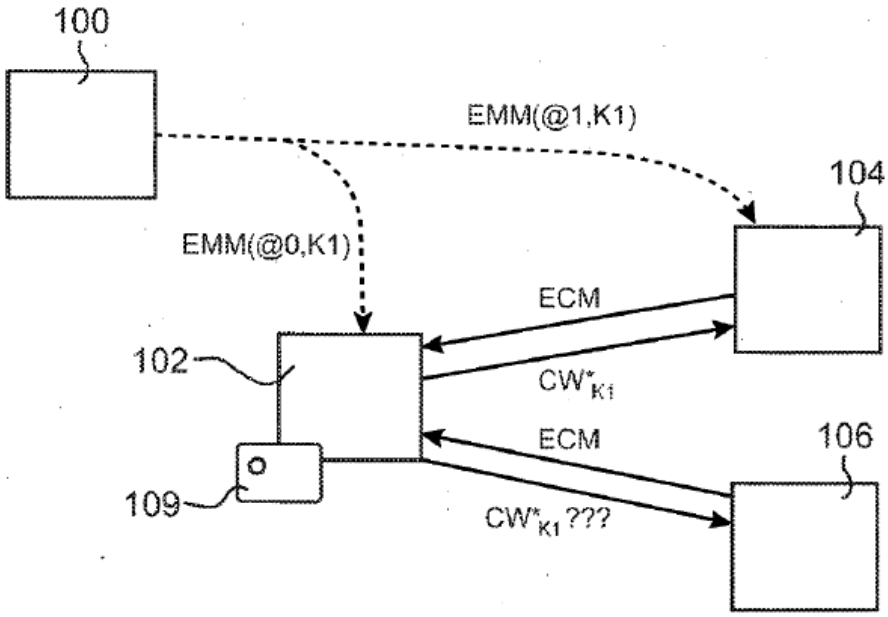

100
EMM(@1,K1)
104
EMM(@0,K1)
ECM
102
CW*K1
ECM
106
109
CW*K1 ???

FIG. 9