(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 647 907**

(51) Int. CI.:

H04N 7/167 (2011.01)
H04N 7/16 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.08.2007 PCT/EP2007/058689**

(87) Fecha y número de publicación internacional: **28.02.2008 WO08023023**

(96) Fecha de presentación y número de la solicitud europea: **21.08.2007 E 07802764 (6)**

(97) Fecha y número de publicación de la concesión europea: **16.08.2017 EP 2055102**

(54) Título: **Procedimiento de transmisión de un dato complementario a un terminal de recepción**

(30) Prioridad:

23.08.2006 FR 0653433

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.12.2017

(73) Titular/es:

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

(72) Inventor/es:

CHIEZE, QUENTIN;
NEAU, LOUIS y
TRONEL, BRUNO

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Procedimiento de transmisión de un dato complementario a un terminal de recepción

Campo técnico

La invención corresponde al campo del control de acceso a servicios multimedia y se refiere más específicamente a un procedimiento de transmisión de al menos un dato complementario D en una lista de palabras de control CW_i de acceso a un contenido aleatorizado transmitido por un servidor de contenido de un operador a un equipo de usuario que consta de un terminal de recepción asociado a un procesador de seguridad, estando cada palabra de control CW_i de dicha lista destinada a desaleatorizar dicho contenido durante un criptoperiodo determinado.

La invención se refiere igualmente a un procesador de seguridad y a un terminal de recepción que cooperan en un equipo de usuario destinado a recibir dicho contenido con una lista de palabras de control CW_i en la que se transmite un dato complementario D.

La invención se refiere además a un servidor de contenido destinado a transmitir a un equipo de usuario un contenido aleatorizado con el que está asociada una lista de palabras de control CW_i destinadas cada una a desaleatorizar dicho contenido durante un criptoperiodo determinado, lista en la que se transmite un dato complementario D.

La invención se refiere igualmente a un terminal de recepción destinado a recibir un contenido aleatorizado transmitido por un servidor, estando dicho contenido acompañado de una lista de palabras de control CW_i, estando cada palabra de control destinada a desaleatorizar dicho contenido durante un criptoperiodo determinado, lista en la que al menos una de las palabras de control se ha sustituido por una magnitud X como resultado del tratamiento de un dato complementario D con una función G que tiene una función dual H.

La invención se aplica independientemente de la naturaleza de la red de soporte o del tipo de servicio ofrecido (TV en directo, PVR, VOD).

Estado de la técnica anterior

Se pueden proporcionar a un usuario contenidos protegidos por un sistema de control de acceso CAS (por sus siglas en inglés de Conditional Access System, sistema de acceso condicional) según diferentes tipos de servicios, como la difusión en directo (TV en directo), la distribución bajo demanda (VoD, por sus siglas en inglés de Video on Demand) o la relectura de contenidos registrados (PVR, por sus siglas en inglés de Personal Video Recorder (grabador de vídeo personal), o NPVR, por sus siglas en inglés de Network Personal Video Recorder, (grabador de vídeo en red)).

En cualquier caso, los contenidos proporcionados al usuario se aleatorizan primero mediante palabras de control CW_i y el operador controla el acceso a un contenido condicionando la obtención de las palabras de control a que el usuario ostente una autorización “comercial”. A tal efecto, el operador adjunta al contenido una condición de acceso que debe cumplir el abonado o su equipo para poder desaleatorizar este contenido.

La transmisión de las palabras de control y la descripción de la condición de acceso se realizan mediante mensajes de control de acceso específicos, denominados mensajes ECM (Entitlement Control Message, mensaje de control de habilitación). Las palabras de control CW_i se cifran mediante una clave de servicio antes de transmitirse en los mensajes ECM. Como resulta conocido para el experto en la materia, la condición de acceso consta de uno o varios criterios (referencia a un abono, número del programa, coste del programa, umbral de nivel moral, ...) que deben cumplirse mediante títulos de acceso (abono, billete, ...) memorizados en el procesador de seguridad o mediante acuerdos dados por el usuario (acuerdo de Pay Per View (pago por visión), acuerdo moral, ...). La transmisión de la clave de servicio y de los títulos de acceso se realiza mediante mensajes de control de acceso específicos, denominados mensajes EMM (por sus siglas en inglés de Entitlement Management Message, mensaje de gestión de habilitación).

A nivel del equipo del usuario, el procesador de seguridad trata los mensajes ECM, concretamente con el fin de verificar los parámetros de seguridad y comparar la condición de acceso a los títulos de acceso previamente inscritos en una memoria no volátil del procesador de seguridad. Si los títulos de acceso cumplen la condición de acceso, el procesador de seguridad restituye, por descifrado, cada palabra de control que proporciona al terminal de recepción, permitiendo así la desaleatorización.

El procesador de seguridad intercambia de este modo datos con el terminal de recepción: en concreto, recibe y trata los mensajes EMM y ECM, y proporciona las palabras de control que permiten la desaleatorización de los contenidos. En un ejemplo bien conocido, el procesador de seguridad es una tarjeta con chip y estos intercambios de datos entre terminal de recepción y procesador de seguridad se hacen a través de una interfaz conforme a la norma ISO 7816.

Este principio de arquitectura, en el que se sitúa la invención, se aplica igualmente cuando el procesador de seguridad está integrado en el terminal de recepción, o cuando funciona con, o está integrado en, un módulo de control de acceso y de desaleatorización externo al terminal de recepción, como un módulo conforme a la norma EN 50221 (“Common Interface Specification for Conditional Access”, Especificación de interfaz común para acceso condicional).

Un equipo de usuario que implementa el control de acceso según este principio de arquitectura puede ser objeto de un uso fraudulento. Un uso fraudulento particular consiste en explotar los recursos de acceso condicional del equipo del usuario fuera del uso “normal” del mismo por parte del usuario, es decir, compartiendo sin autorización el uso del procesador de seguridad (o “card sharing”), es decir, redistribuyendo fraudulentamente las palabras de control proporcionadas por el procesador de seguridad (o “CW sharing”).

El uso compartido del procesador de seguridad de un equipo de usuario consiste en que varios terminales de recepción soliciten el mismo a través de una red de comunicación bidireccional. Este uso se traduce en concreto en someter al procesador de seguridad mensajes sintácticamente correctos, pero cuyo número o diversidad son excesivos con respecto a lo que serían generalmente debido a un uso “normal” del sistema.

La redistribución de palabras de control consiste en hacer que varios terminales de recepción se beneficien de las palabras de control CW_i obtenidas por uno de ellos, a través de una red de comunicación. Esta forma de pirateo es aplicable, en concreto, cuando las palabras de control CW_i transitan sin cifrar entre el procesador de seguridad y el terminal de recepción. La escucha de la interfaz del procesador de seguridad y del terminal de recepción permite de este modo interceptar las palabras de control y redistribuirlas de forma fraudulenta hacia otros terminales de recepción (“MacCormac Hack”), redistribución que puede realizarse por medio de un servidor que difunde las palabras de control CW_i o las proporciona en respuesta a la sumisión de los ECM asociados con el contenido considerado.

La figura 1 ilustra esquemáticamente una situación de redistribución fraudulenta de palabras de control de este tipo.

Con referencia a esta figura 1, un equipo 2 de usuario consta de un terminal de recepción 4 asociado con un procesador de seguridad 6 como una tarjeta con chip. El terminal de recepción 4 recibe una ECM desde la cabecera de la red y transmite (flecha 5) estos ECM al procesador de seguridad 6. El procesador de seguridad 6 trata los ECM recibidos para verificar las condiciones de acceso y descifra las palabras de control contenidas en estos ECM, luego transmite (flecha 8) las palabras de control descifradas al terminal de recepción 4. Estas palabras de control son susceptibles de interceptarse fraudulentamente en la interfaz del procesador de seguridad/terminal de recepción y luego ser distribuidas fraudulentamente (flechas 12) por un servidor pirata 10 a terminales de recepción 14.

Se conocen soluciones para luchar contra los usos fraudulentos de tipo “card sharing” o “CW sharing”. Por ejemplo, se puede activar un emparejamiento entre el procesador de seguridad y el terminal de recepción, como se describe en las patentes francesas FR 2.866.772 y FR 2.866.773; el procesador de seguridad puede enviar las palabras de control en forma cifrada al terminal de recepción como se describe en la solicitud de patente FR 2.882.208; el procesador de seguridad puede proporcionar al terminal de recepción, no ya las palabras control, sino datos que le permitan al terminal reconstituirlos, como se describe en la solicitud de patente FR 2.876.858. Sin embargo, estas diversas soluciones necesitan, como complemento a la adaptación del procesador de seguridad, una adaptación de los terminales de recepción. Si bien es relativamente fácil cambiar una tarjeta con chip, resulta más difícil y costoso cambiar un parque existente de terminales de recepción para soportar estas nuevas funcionalidades.

El objetivo de la invención es permitir “rastrear” los equipos de usuario, típicamente sus procesadores de seguridad, que contribuyen en un dispositivo de reparto de tarjetas o de redistribución de palabras de control y permitir así que el operador en cuestión identifique, por medios externos al sistema, al cliente titular de tal equipo de usuario que contribuye a este pirateo. La implementación de esta invención solo implica la adaptación del procesador de seguridad sin tener que modificar los terminales de recepción existentes.

La solución propuesta se aplica principalmente en caso de que las palabras de control transiten en forma no cifrada en la interfaz entre el procesador de seguridad y el terminal de recepción. Puede implementarse también cuando esta interfaz está protegida por cifrado, pero permanecer latente para volver a activarse en el caso en que esta protección de interfaz se viera comprometida.

Descripción de la invención

La invención preconiza un procedimiento de transmisión de al menos un dato complementario D en una lista de palabras de control CW_i de acceso a un contenido aleatorizado transmitido por un servidor de contenido de un operador a un equipo de usuario que consta de un terminal de recepción asociado a un procesador de seguridad, estando cada palabra de control CW_i de dicha lista destinada a desaleatorizar dicho contenido durante un criptoperiodo determinado.

El procedimiento según la invención consta de las siguientes etapas:

a) sustituir previamente al menos una de las palabras de control de dicha lista por una magnitud X que resulta del tratamiento de dicho dato complementario D mediante una función G que tiene una función dual H, y a la recepción de dicha lista en el terminal,
b) recuperar dicho dato complementario D mediante el tratamiento de dicha magnitud X con la función dual H.

Según una característica de la invención, la magnitud X presenta un formato idéntico al de la palabra de control sustituida.

Preferentemente, la función dual H además restituye la palabra de control sustituida durante la etapa a).

En una primera variante de implementación del procedimiento, según la invención, la lista de palabras de control CW_i consta de una primera palabra de control CW_c destinada a descifrar el contenido durante el criptoperiodo actual y de una segunda palabra de control CW_s destinada a descifrar el contenido durante el criptoperiodo siguiente, y dicha magnitud X sustituye a la segunda palabra de control CW_s.

En una aplicación particular del procedimiento, según la invención, el dato complementario D representa un identificador del usuario o un identificador único UA del procesador de seguridad.

En otra aplicación del procedimiento, según la invención, dicho dato complementario D es un comando destinado al terminal de recepción.

Durante la aplicación del procedimiento a un contenido dado, la función G y la sustitución de la palabra de control se ejecutan en el servidor de contenido del operador.

En otra variante, la función G y la sustitución de la palabra de control se ejecutan en el procesador de seguridad asociado con el terminal de recepción.

En este último caso, la ejecución de la función G y de la sustitución de la palabra de control está controlada por el operador y consta de una etapa de armado y de una etapa de activación, consistiendo la etapa de armado en definir, para el contenido dado y para un procesador de seguridad seleccionado, un periodo de armado durante el cual la función G y la sustitución de la palabra de control son ejecutables, y consistiendo la etapa de activación en ordenar la ejecución, por parte de dicho procesador de seguridad seleccionado, de la función G y de la sustitución de una palabra de control particular por la magnitud X conforme a las condiciones definidas en la etapa de armado.

Preferentemente, el periodo de armado y la designación del contenido para los que se pueden ejecutar dicha función G y la sustitución de la palabra de control se transmiten de manera oculta en un mensaje EMM a los procesadores de seguridad seleccionados y la ejecución de la función G y la sustitución de la palabra de control particular por la magnitud X las activa el operador por medio de un comando específico transmitido de manera oculta en un mensaje EMM o en un mensaje ECM.

En una segunda variante, el procesador de seguridad activa de manera autónoma la ejecución de la función G y de la sustitución de la palabra de control particular por la magnitud X.

En una tercera variante, la ejecución de la función G y de la sustitución de una palabra de control particular por la magnitud X se activa de forma aleatoria.

En un modo particular de realización de la invención, la designación de la palabra de control particular que hay que sustituir por la magnitud X se realiza mediante un generador de ECM (ECM-G) asociado al servidor de contenido. Esta designación de la palabra de control y la identificación del contenido en curso se transmiten de manera oculta a los procesadores de seguridad en mensajes ECM asociados a dicho contenido.

Los procesadores de seguridad que implementan el procedimiento según la invención constan de un módulo que permite sustituir en la lista de palabras de control CW_i al menos una de las palabras de control por una magnitud X que es el resultado del tratamiento con una función G de un dato complementario D que hay que transmitir al terminal de recepción, recuperándose dicho dato complementario D por dicho terminal de recepción por medio de una función H dual de la función G.

El servidor de contenido destinado a transmitir a un equipo de un usuario un contenido aleatorizado consta de un módulo que permite sustituir en dicha lista de palabras de control CW_i al menos una de las palabras de control por una magnitud X que es el resultado del tratamiento de un dato complementario D que hay que transmitir al terminal de recepción con una función G, recuperándose dicho dato complementario D por dicho terminal de recepción por medio de una función H dual de la función G.

El terminal de recepción, destinado a recibir el contenido aleatorizado transmitido por dicho servidor y acompañado de una lista de palabras de control en la que al menos una de las palabras de control se ha sustituido por una magnitud X que es el resultado del tratamiento de un dato complementario D con una función G que tiene una

función dual H, consta de un módulo que permite recuperar, mediante la aplicación de la función H al dato X, la palabra de control sustituida y/o el dato D.

En un modo de realización de la invención, este módulo del terminal es un módulo de software.

En otro modo de realización de la invención, este terminal constituye un módulo observador que consta de unos medios para volver a enviar dicho dato complementario al operador.

Breve descripción de los dibujos

Otras características y ventajas de la invención se pondrán de manifiesto a partir de la siguiente descripción, aportada a modo de ejemplo no limitativo, con referencia a las figuras adjuntas, en las que:

- la figura 1, descrita anteriormente, ilustra esquemáticamente un dispositivo de redistribución fraudulenta de palabras de control de acceso a un contenido aleatorizado;
- la figura 2 ilustra esquemáticamente la implementación del procedimiento según la invención en el contexto del dispositivo de la figura 1.
- las figuras 3 y 4 ilustran un ejemplo de determinación por parte del equipo del operador de la palabra de control que hay que marcar.

Exposición detallada de modos de realización particulares

La invención se describirá en un contexto de distribución de programas audiovisuales aleatorizados.

Esta distribución puede ser:

- en el marco de un servicio de difusión en directo en el que el contenido se difunde en tiempo real hacia un gran número de usuarios, por medio de una red de difusión (satélite, cable, hertziana terrestre, IP en modo broadcast/multicast (difusión/multidifusión)...).
- en el marco de un servicio VOD (por sus siglas en inglés de Video On Demand) en el que, bajo petición, un contenido se envía a un usuario particular a través de una red de distribución que permite el direccionamiento individual del usuario (generalmente red IP en modo unicast (unidifusión)).
- en el marco de un servicio PVR (por sus siglas en inglés de Personal Video Recorder) en el que un contenido (difundido o en VOD) está grabado por el usuario en su equipo terminal o por una función similar propuesta por el operador de la red, pudiendo el usuario acceder posteriormente al contenido grabado.

Sea cual sea el servicio proporcionado, el procedimiento según la invención consta de una etapa de configuración que consiste en designar el contenido (o servicio) en cuestión y la palabra de control que debe ser modificada por el procesador de seguridad.

En esta descripción, en lo sucesivo, se designará con la expresión “marcado de una palabra de control” la sustitución de esta palabra de control por un dato mediante la aplicación del procedimiento según la invención.

Unas referencias idénticas designarán los elementos comunes de las diferentes figuras.

La figura 2 ilustra esquemáticamente la implementación del procedimiento en la arquitectura descrita en la figura 1.

En el ejemplo ilustrado por esta figura 2, un terminal de recepción 4 de un usuario recibe desde la cabecera de la red cuatro ECM sucesivos ECM(1-CWp/CWf), ECM(2-CWp/CWf), ECM(3-CWp/CWf) y ECM(4-CWp/CWf), cada uno de los cuales consta de un par de palabras de control CW_p, CW_f que representan respectivamente la palabra de control actual CW_p (p de “present”) y la palabra de control siguiente CW_f (f de “following”). Se entiende que la palabra de control siguiente CW_f en un ECM, por ejemplo, ECM(2-CW_p / CW_f), es la palabra de control actual CW_p en el ECM siguiente, en este ejemplo ECM(3-CW_p / CW_f).

Esta arquitectura consta además de un terminal observador 20 programado para intercambiar información con la cabecera de la red a través de un canal seguro.

El terminal de recepción 4 recibe mensajes ECM junto con el contenido y los transmite al procesador de seguridad 6 (flecha 5). Para cada ECM recibido el procesador de seguridad 6 verifica las condiciones de acceso, descifra las palabras de control contenidas en estos ECM y luego transmite (flecha 8) las palabras de control descifradas al terminal de recepción 4. En el caso particular del ECM (2-CW_p/CW_f), la palabra de control CW_f que debería volver a enviarse al terminal de recepción se sustituye por el dato $CW_{f\text{-}UA}$ (igual a G (UA)), o palabra de control marcada, calculada en función del identificador único UA del procesador de seguridad 6.

La captura y el análisis, por parte del terminal observador 20, del dato $CW_{f\text{-}UA}$ transmitido fraudulentamente por el servidor pirata 10 a los terminales piratas 14 permite determinar el UA del procesador de seguridad proveedor de la

palabra de control marcada y, por tanto, contribuidor del pirateo.

Cabe destacar que el terminal observador está controlado por el operador y está configurado para distinguir un valor de palabra de control de un valor procedente del marcado, es decir, un resultado X de la función G. Esta distinción se realiza, por ejemplo, comparando los valores recibidos del dispositivo pirata con las palabras de control usadas efectivamente por el operador. Se mejora esta comparación efectuándola en correlación con los momentos de activación del procedimiento que define el propio operador.

El terminal observador aplica entonces la función dual H al dato recibido para extraer del mismo el identificador del procesador de seguridad UA (igual a $H(CW_{f\text{-}UA})$) mediante la aplicación de la función H

El terminal observador 20 transmite a continuación, a la cabecera de la red, a través del canal seguro, dicho UA de dicho procesador de seguridad.

El operador puede aplicar entonces una contramedida al dispositivo pirata identificado de este modo.

Se observa que la palabra de control marcada que sustituye la palabra de control CW_f puede calcularse en función de un identificador propio del usuario 2 sin desviarse del ámbito de la invención.

En las normas en vigor relativas a la implementación de la aleatorización, del transporte y de la desaleatorización en un contexto como DVB, las palabras de control CW no se designan como “actual” y “siguiente” sino como “par” e “impar” con referencia a las fases “par” e “impar” de la aleatorización. Cuando la aleatorización está en la fase “par”, la palabra de control “par” es la palabra de control “actual” y la palabra de control “impar” es la palabra de control “siguiente”. Esto se invierte cuando la aleatorización está en fase “impar”. También, con el fin de permitir que el procesador de seguridad 6 detecte a lo largo del tiempo la palabra de control “siguiente” entre las palabras de control transportadas en los ECM, se asocia un atributo de paridad de la aleatorización con el contenido aleatorizado en cada criptoperiodo. Este atributo permite determinar cuál de las palabras de control “par” o “impar” se usa para aleatorizar el contenido durante el criptoperiodo actual. Se observa que ya existe una indicación de la paridad de aleatorización en los contenidos aleatorizados (vídeo, sonido), pero un sistema de acceso condicional en un equipo de usuario no puede utilizarla en tiempo real, esa es la razón por la que se introduce un atributo de paridad específicamente en los mensajes ECM. Este atributo se determina en la emisión del contenido y de los mensajes ECM asociados.

Las figuras 3 y 4 ilustran un ejemplo de determinación por parte del equipo del operador de la palabra de control que hay que marcar.

Con referencia a la figura 3, el equipo del operador comprende, en concreto, un multiplexador/aleatorizador 30 encargado de combinar en un multiplexor 31, por ejemplo, conforme a la norma ISO 13818 “MPEG2”, los flujos 32 digitales vídeo, audio o datos diversos que constituyen los contenidos, y aleatorizarlos. Un generador ECMG 34 proporciona al multiplexador 30 mensajes ECM que hay que asociar con los contenidos en el multiplexor 31.

El generador ECMG 34 comprende además una memoria 36 que contiene una variable CW_{par} a la que afecta el último valor de la palabra de control recibida del multiplexador 30 que este identificó como palabra de control par y de una segunda memoria 38 en la que memoriza la paridad de la palabra de control que ha determinado como la palabra de control que hay que marcar. Por defecto, la variable CW_{par} no es significativa.

Entre otras realizaciones posibles, un protocolo 40 de diálogo entre el multiplexador 30 y el generador ECMG 34 es conforme a la norma TS 103197 “DVB SimulCrypt”. La implementación de este protocolo se describe en este documento para el caso de mensajes ECM que transportan dos palabras de control. Según este protocolo, el establecimiento de un canal de intercambio entre el multiplexador 30 y el generador ECLG 34 es conocido y se da por supuesto que se ha efectuado.

La figura 4 es un ejemplo de diagrama temporal ejecutado por el multiplexador 30 y el generador ECMG 34 en cada criptoperiodo para determinar la palabra de control que hay que marcar.

Durante una etapa 100, el multiplexador 30 envía al generador ECMG 34 una solicitud de mensaje ECM cuyos parámetros son, en concreto, las dos palabras de control par CW_{2k} e impar CW_{2k+1} que hay que insertar en el ECM solicitado. Una de estas palabras de control es la palabra de control actual utilizada por la aleatorización en curso, la otra es la palabra de control siguiente. En efecto, el protocolo “DVB SimulCrypt” identifica la paridad de las palabras de control enviadas por el multiplexador al generador ECMG 34, pero no precisa cuál de estas palabras de control es la usada por la aleatorización en curso.

Durante una etapa 110, el generador ECMG 34 extrae de la solicitud que ha recibido las dos palabras de control y los otros parámetros. Estos otros parámetros normalmente le sirven al generador ECMG 34 para construir la condición de acceso que hay que insertar en el ECM; sin embargo, no intervienen en el proceso descrito en este documento.

Durante una etapa 120, el generador ECMG 34 compara el valor de la palabra de control par recibida CW_{2k} al valor de su variable CW_{par}. Si estos dos valores son idénticos, concluye que esta palabra de control CW_{2k}, inalterada desde el criptoperiodo anterior, es la palabra de control actual usada por el aleatorizador 30. En ese caso, durante una etapa 140, el generador ECMG 34 memoriza en la segunda memoria 38 que la paridad de la palabra de control que hay que marcar es impar. Si los dos valores comparados en la etapa 120 no son idénticos, el generador ECMG 34 memoriza, durante una etapa 160, en la segunda memoria 38 que la paridad de la palabra de control que hay que marcar es par.

Después, durante una etapa 180, el generador ECMG 34 memoriza el valor de la palabra de control par recibida CW_{2k} en la primera memoria 36.

Finalmente, el generador ECMG 34 construye durante una etapa 200 el mensaje ECM solicitado por el multiplexador en la etapa 110. Para generar este mensaje ECM, el generador ECMG 34 cifra las dos palabras de control CW_{2k} y CW_{2k+1} recibidas y las combina, concretamente según la condición de acceso elegida. Cuando se activa la función de marcado, como se describirá a continuación, el generador ECMG 34 inserta, asimismo, en el mensaje ECM el valor contenido en la segunda memoria que designa la palabra de control que hay que marcar. Este mensaje, una vez constituido, se envía al multiplexador 30 durante una etapa 220 para insertarse en el multiplexor digital 32.

Las etapas 100 a 220 se repiten en cada criptoperiodo.

Control del marcado de la palabra de control por el operador

El operador controla la función de marcado en dos fases: una fase de armado durante la cual un procesador de seguridad puede aplicar el marcado a una palabra de control y una fase de activación durante la cual, bajo reserva de armado, un procesador de seguridad debe aplicar el marcado a una palabra de control. Según la implementación, la una y/o la otra de estas fases son implícitas o están controladas explícitamente por el operador.

En un modo preferido de realización, el operador controla explícitamente los parámetros de estas dos fases. El procedimiento según la invención se aplica, para un procesador de seguridad dado, a un servicio (programa o cadena) dado o al conjunto de los servicios proporcionados por el operador.

Durante la fase de armado, el operador define para un procesador de seguridad dado:

- El periodo para el que se arma la función de marcado. Fuera de este periodo, no se efectúa ningún marcado, y durante este periodo, dicho procesador de seguridad puede efectuar un marcado. Por lo tanto, este periodo es una ventana de aplicación del marcado de las palabras de control.
- El identificador de un servicio para el que se debe efectuar el marcado. El operador selecciona de este modo el servicio que prevé observar para identificar a un pirata. Preferentemente, el operador puede designar un servicio particular o todos los servicios.

El armado del marcado de las palabras de control lo realiza el operador mediante la transmisión de un EMM confidencial al procesador de seguridad de un usuario.

Un EMM confidencial de este tipo contiene un parámetro específico, denominado de armado del marcado de las palabras de control PDTCW, que comprende:

- la fecha de armado del marcado de las palabras de control DDTCW;
- la duración del periodo de armado del marcado de las palabras de control PPCW, preferentemente igual a la duración del criptoperiodo usado por el multiplexador.
- un identificador SERVICE_ID del servicio para el que hay que armar el marcador, del que un valor particular permite armar el marcado de las palabras de control para el conjunto de los servicios del operador.

El parámetro de armado del marcado de las palabras de control se transmite al procesador de seguridad 6 con una fecha de difusión para impedir una reproducción del mensaje EMM correspondiente.

El procesador de seguridad 6 está programado para tratar este parámetro solo si va fechado y si su fecha de difusión es superior a la del último parámetro de la misma naturaleza ya tratado.

Al aprovechar las capacidades de direccionamiento de los mensajes EMM, el operador puede armar la función de marcado en un procesador de seguridad particular, en un grupo de procesadores de seguridad o en todos los procesadores de seguridad.

De manera análoga, la función de marcado de las palabras de control puede desarmarse por mensaje EMM, por ejemplo, si el operador desea suspender esta función en un subconjunto del parque, cuando el mensaje de armado se ha enviado inicialmente a todos los terminales de recepción del parque.

El procesador de seguridad 6 está programado para usar igualmente esta función de desarme tras haber enviado una palabra de control marcada. Esto le permite al procesador de seguridad 6 aplicar una sola vez el procesamiento de marcado de la palabra de control CW a partir de la fecha de inicio del marcado de las palabras de control.

Como variante, el parámetro de armado PDTCW se transmite a los procesadores de seguridad 6 de manera confidencial en un ECM.

La fase de activación es durante la cual un procesador de seguridad aplica el marcado a una palabra de control particular. La activación del marcado se realiza mediante un parámetro específico CWTAT introducido en un ECM por el generador de ECM 32.

Este parámetro caracteriza las condiciones de aplicación del marcado de las palabras de control. Consta de:

- un identificador ECM_SERVICE_ID del servicio al que se refiere el ECM,
- un parámetro PARITY que designa cuál de las dos palabras de control presentes en el ECM debe marcarse. Este parámetro retoma el valor del indicador 38. Preferentemente, además de los valores “par” e “impar”, este parámetro puede tomar el valor “no marcado” para inhibir la activación.

Este parámetro CWTAT además está asociado con una fecha del mensaje ECM. Esta fecha está explicita en el mensaje ECM o, preferentemente, establecida por el procesador de seguridad en el momento de llegada del ECM. Se conocen varias soluciones técnicas para que un procesador de seguridad pueda gestionar el tiempo y conocer la fecha de llegada de un ECM.

Preferentemente, el parámetro CWTAT se transmite en un mensaje ECM de manera confidencial.

Se entiende que todos los procesadores de seguridad contemplados durante la fase de armado son susceptibles de activar el procedimiento a la recepción el mensaje ECM.

Como variante, la fase de activación puede desencadenarse en una parte de los procesadores de seguridad en los que se ha armado el procedimiento de marcado. La activación implementa entonces un mensaje ECM y un mensaje EMM. El mensaje ECM transporta el parámetro CWTAT que prepara el procesador de seguridad para aplicar el procedimiento, pero no lo activa. El mensaje EMM transporta un comando específico para que el(los) procesador(es) de seguridad contemplado(s) por este mensaje EMM active(n) efectivamente el procedimiento de marcado.

Tratamiento del marcado de la palabra de control por el procesador de seguridad

Durante la fase de armado, el procesador de seguridad 6 recibe el parámetro PDTCW de armado del marcado de las palabras de control por EMM para un operador. Durante el tratamiento de este mensaje EMM, el procesador de seguridad verifica que este mensaje no se haya tratado ya y, en caso afirmativo, memoriza los parámetros de armado del marcado extraídos del parámetro PDTCW:

- fecha a partir de la cual la activación del marcado de las palabras de control es posible;
- duración del periodo durante el cual el marcado de las palabras de control es posible;
- identificador del servicio para el que se pueden marcar las palabras de control.

A la recepción de un mensaje ECM de un operador que contiene el parámetro CWTAT de activación del marcado, el procesador de seguridad 6 solo efectúa el marcado si se cumplen las siguientes condiciones:

- el marcado de las palabras de control está armado, es decir, el procesador de seguridad dispone de datos (periodo y servicio de armado) de un parámetro PDTCW para este operador,
- el parámetro PARITY que identifica en el ECM la palabra de control que hay marcar no tiene el valor “sin marcado”,
- el parámetro ECM_SERVICE_ID del ECM corresponde al identificador de servicio SERVICE_ID dado por el EMM de armado,
- la fecha del ECM está comprendida en la ventana de aplicación de la medida determinada por el período de armado (entre DDTCW y DDTCW + PPCW).

Si el parámetro PARITY tiene el valor “par”, se marca el CW par.

Si el parámetro PARITY tiene el valor “impar”, se marca el CW impar.

Al final de este procedimiento, preferentemente, el procesador de seguridad procede al desarme de la función de marcado con el fin de evitar la repetición del marcado de la palabra de control CW.

El procesador de marcado a efectos de identificación de un dispositivo ilícito es tanto más eficaz en tanto que su activación no sea predecible por el dispositivo que se tiene como objetivo. También, además de la confidencialidad de los parámetros en cuestión en el mensaje ECM, es preferible que la activación del procedimiento la desencadene el operador en momentos aleatorios. Además, más allá de la activación por recepción del mensaje ECM, el procesador de seguridad puede retrasar la ejecución efectiva del marcado un periodo de tiempo aleatorio.

Transmisión de un comando a un terminal de recepción

Sin salirse del ámbito de la invención, el procedimiento descrito más arriba puede usarse para transmitir un comando a un terminal de recepción. El dato D representa este comando y tiene un significado particular comprensible por el terminal de recepción para ejecutar un tratamiento específico. Es un medio para volver confidencial el envío de un comando hacia un terminal de recepción.

Un comando de este tipo al terminal representado por el dato D puede:

- generarse y activarse por el propio procesador de seguridad: por ejemplo, cuando el procesador de seguridad es capaz de detectar un funcionamiento anormal del terminal de recepción significativo de un terminal ilícito, activa él mismo el envío al terminal de un comando de invalidación del terminal transmitido como dato D según la invención.
- generarse por el procesador de seguridad al ser activado por el operador: por ejemplo, cuando un equipo de usuario ha sido identificado por el marcado por el UA de las palabras de control descrito anteriormente, el procedimiento se arma de nuevo en este equipo y luego el procesador de seguridad activa él mismo el envío al terminal de un comando de invalidación del terminal por medio del dato D; este modo de funcionamiento se le indica al procesador de seguridad durante la fase de armado o la fase de activación mediante un parámetro complementario dedicado.

- generarse y accionarse por el operador: en este ejemplo, el comando expresado por el dato D lo emite el operador, y el marcado se efectúa entonces en cuanto se generan los ECM. En este caso, el procesador de seguridad no efectúa ningún marcado complementario sobre las palabras de control que proporciona al terminal de recepción. Normalmente, un comando de este tipo es de uso general, al igual que la activación o la desactivación de ciertas salidas audiovisuales del terminal de recepción. Preferentemente, las funciones de marcado G y H se eligen de manera que el terminal de recepción pueda encontrar el valor de la palabra de control marcada y el del comando D.

REIVINDICACIONES

1. Procedimiento de transmisión de al menos un dato complementario D en una lista de palabras de control CW_i de acceso a un contenido aleatorizado transmitido por un servidor de contenido de un operador a un equipo de usuario (2) que consta de un terminal de recepción (4) asociado a un procesador de seguridad (6), estando cada palabra de control CW_i de dicha lista destinada a desaleatorizar dicho contenido durante una criptoperiodo determinado, procedimiento **caracterizado por** las siguientes etapas:

a) sustituir previamente al menos una de las palabras de control de dicha lista por una magnitud X que resulta del tratamiento de dicho dato complementario D con una función G que tiene una función dual H,
y, a la recepción de dicha lista en el terminal de recepción (4),
b) recuperar dicho dato complementario D mediante el tratamiento de dicha magnitud X con la función dual H.

2. Procedimiento según la reivindicación 1, **caracterizado por que** la magnitud X presenta un formato idéntico al de la palabra de control sustituida.

3. Procedimiento según la reivindicación 1, **caracterizado por que** dicha lista consta de una primera palabra de control CW_c destinada a descifrar el contenido durante el criptoperiodo actual y de una segunda palabra de control CW_s destinada a descifrar el contenido durante el criptoperiodo siguiente, y **por que** dicha magnitud X sustituye la segunda palabra de control CW_s.

4. Procedimiento según la reivindicación 3, **caracterizado por que** dicho dato complementario D es un identificador único UA del procesador de seguridad (6).

5. Procedimiento según la reivindicación 3, **caracterizado por que** dicho dato complementario D es un identificador del usuario.

6. Procedimiento según la reivindicación 1, **caracterizado por que** dicho dato complementario D es un comando destinado al terminal de recepción (4).

7. Procedimiento según la reivindicación 1, **caracterizado por que** dicha función G y dicha sustitución de la palabra de control se ejecutan en el servidor de contenido del operador.

8. Procedimiento según la reivindicación 1, **caracterizado por que** dicha función G y dicha sustitución de la palabra de control se ejecutan en el procesador de seguridad (6) asociado al terminal de recepción (4).

9. Procedimiento según la reivindicación 8, en el que la ejecución en el procesador de seguridad (6) de la función G y de la sustitución de la palabra de control está dirigida por el operador y consta de una etapa de armado y de una etapa de activación,
consistiendo dicha etapa de armado en definir, para el contenido dado y para un procesador de seguridad seleccionado (6), un periodo de armado durante el cual la función G y la sustitución de la palabra de control son ejecutables,
consistiendo dicha etapa de activación en desencadenar la ejecución, por dicho procesador de seguridad seleccionado (6), de la función G y de la sustitución de una palabra de control particular por la magnitud X conforme a las condiciones definidas en la etapa de armado.

10. Procedimiento según la reivindicación 9, **caracterizado por que** el periodo de armado y la designación del contenido para los que se pueden ejecutar dicha función G y dicha sustitución de la palabra de control se transmiten de manera oculta en un mensaje EMM a los procesadores de seguridad seleccionados (6), y **por que** el operador activa la ejecución de la función G y la sustitución de la palabra de control particular por la magnitud X por medio de un comando específico transmitido de manera oculta en un mensaje EMM o en un mensaje ECM.

11. Procedimiento según la reivindicación 8, **caracterizado por que** el procesador de seguridad (6) activa de manera autónoma la ejecución de la función G y de la sustitución de la palabra de control particular por la magnitud X.

12. Procedimiento según la reivindicación 1, **caracterizado por que** la ejecución de la función G y de la sustitución de una palabra de control particular por la magnitud X se activa de forma aleatoria.

13. Procedimiento según la reivindicación 9 en el que la designación de la palabra de control particular que hay que sustituir por la magnitud X la realiza un generador de ECM (30) asociado al servidor de contenido.

14. Procedimiento según la reivindicación 9, **caracterizado por que** la designación de la palabra de control que hay que sustituir y la identificación del contenido en curso se transmiten de manera oculta a los procesadores de seguridad (6) en mensajes ECM asociados a dicho contenido.

15. Procesador de seguridad (6) asociado a un terminal de recepción (4) en un equipo de un usuario (2) destinado a recibir un contenido aleatorizado transmitido por un servidor de contenido de un operador con una lista de palabras de control CW_i destinadas cada una a desaleatorizar dicho contenido durante un criptoperiodo determinado, procesador de seguridad (6) **caracterizado por que** incluye un módulo que permite sustituir en dicha lista al menos una de las palabras de control por una magnitud X que resulta del tratamiento con una función G de un dato complementario D que hay que transmitir a dicho terminal de recepción (4), recuperándose dicho dato complementario D por dicho terminal de recepción (4) por medio de una función H dual de la función G.

16. Procesador de seguridad (6) según la reivindicación 15, **caracterizado por que** dicho dato complementario D es un identificador único UA de dicho procesador de seguridad (6).

17. Procesador de seguridad (6) según la reivindicación 15, **caracterizado por que** dicho dato complementario D es un comando destinado al terminal de recepción (4).

18. Servidor de contenido destinado a transmitir, a un equipo de un usuario (2) que consta de un terminal de recepción (4) asociado a un procesador de seguridad (6), un contenido aleatorizado al que está asociada una lista de palabras de control CW destinadas cada una a desaleatorizar dicho contenido durante un criptoperiodo determinado, servidor **caracterizado por que** consta de un módulo que permite sustituir en dicha lista al menos una de las palabras de control por una magnitud X que resulta del tratamiento de un dato complementario D que hay que transmitir al terminal de recepción (4) por una función G, recuperándose dicho dato complementario D por dicho terminal de recepción (4) por medio de una función H dual de la función G.

19. Terminal de recepción (4) destinado a recibir un contenido aleatorizado transmitido por un servidor, estando dicho contenido acompañado de una lista de palabras de control CW_i, estando cada palabra de control destinada a desaleatorizar dicho contenido durante un criptoperiodo determinado, lista en la que una de las palabras de control se ha sustituido por una magnitud X que resulta del tratamiento de dicho dato complementario D con una función G que tiene una función dual H, terminal de recepción (4) **caracterizado por que** consta de un módulo que permite recuperar mediante dicha función H dicha palabra de control y/o dicho dato complementario.

20. Terminal de recepción según la reivindicación 19, **caracterizado por que** dicho módulo es un módulo de software.

21. Terminal de recepción según la reivindicación 19, **caracterizado por que** está asociado a un procesador de seguridad (6).

22. Terminal de recepción según la reivindicación 19, **caracterizado por que** constituye un terminal observador que consta de unos medios para volver a enviar dicho dato complementario al operador.

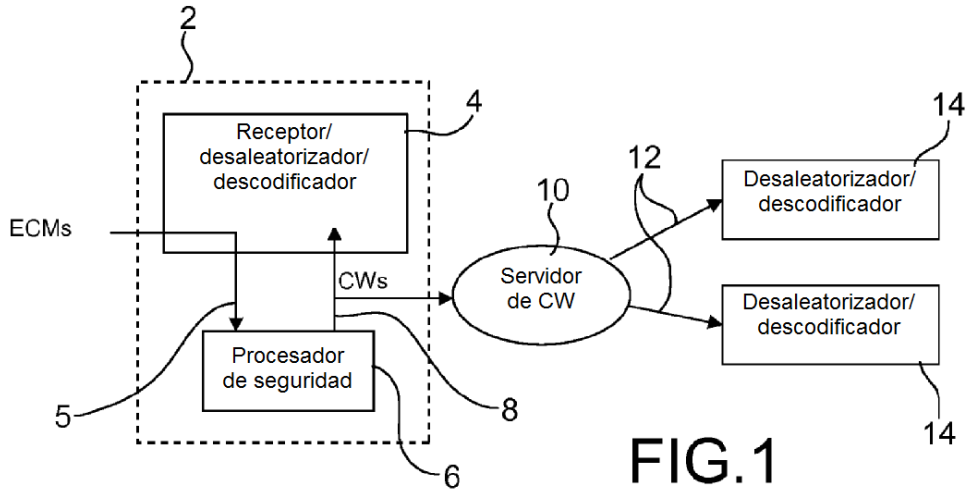
2
4
Receptor/
desaleatorizador/
descodificador
ECMs
CWs
Procesador
de seguridad
5
6
8
10
Servidor
de CW
12
14
Desaleatorizador/
descodificador
Desaleatorizador/
descodificador
14

FIG.1

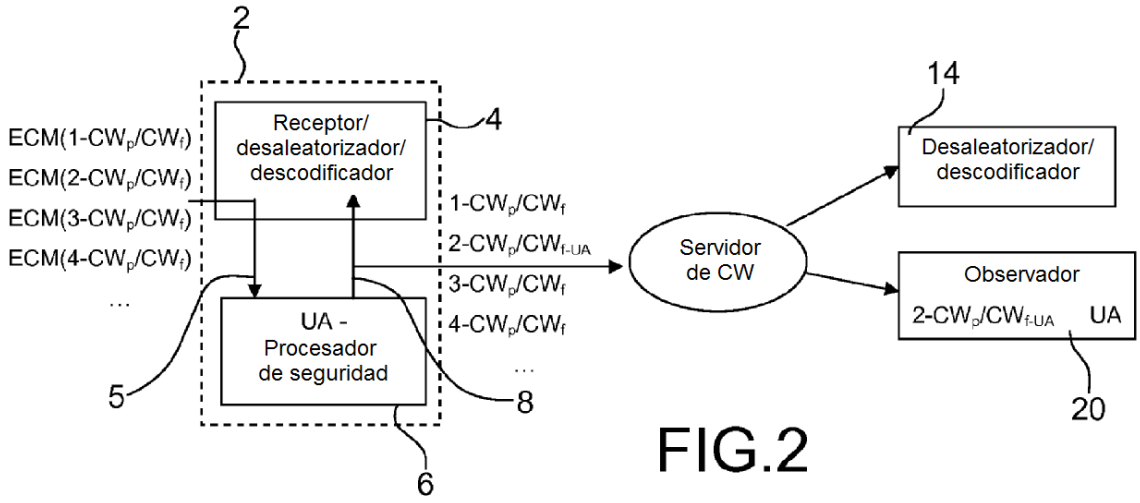
2
4
Receptor/
desaleatorizador/
descodificador
ECM(1-CWp/CWf)
ECM(2-CWp/CWf)
ECM(3-CWp/CWf)
ECM(4-CWp/CWf)
...
UA -
Procesador
de seguridad
5
6
8
1-CWp/CWf
2-CWp/CWf-UA
3-CWp/CWf
4-CWp/CWf
...
Servidor
de CW
14
Desaleatorizador/
descodificador
Observador
2-CWp/CWf-UA
UA
20

FIG.2

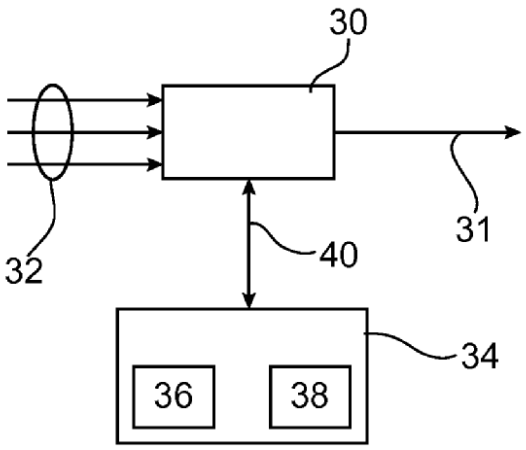

FIG.3

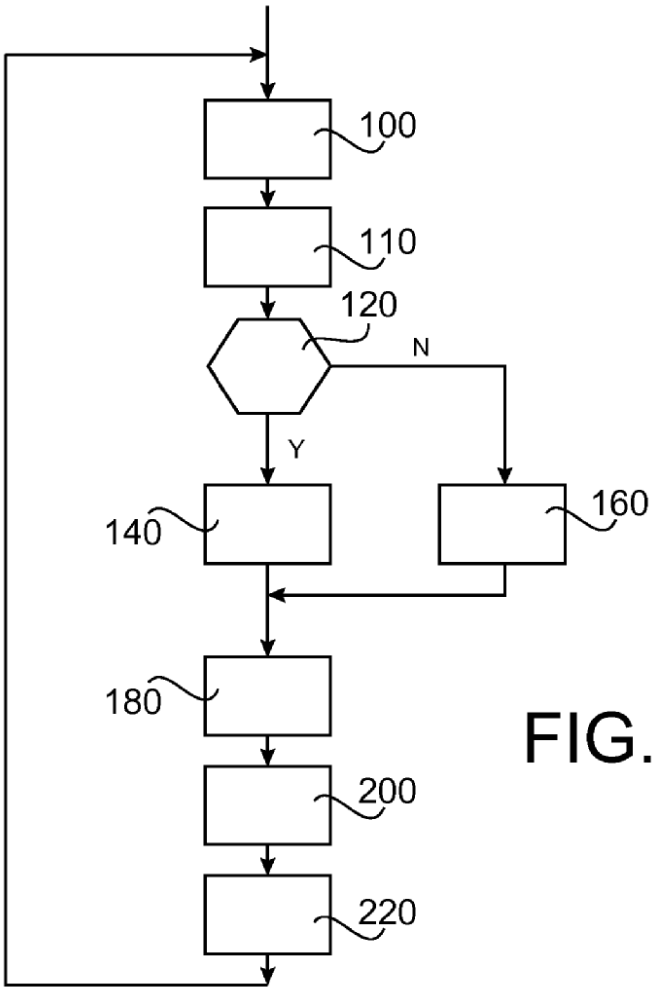

FIG.4