(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 802 426**

(51) Int. CI.:

***G06F 21/10*** (2013.01)
***H04L 9/06*** (2006.01)
***H04L 29/06*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.12.2015 PCT/IL2015/051177**

(87) Fecha y número de publicación internacional: **08.06.2017 WO17093990**

(96) Fecha de presentación y número de la solicitud europea: **03.12.2015 E 15823204 (1)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2020 EP 3384417**

(54) Título: **Método y sistema para asegurar un acceso de un cliente a servicios de agente DRM para un reproductor de video**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**19.01.2021**

(73) Titular/es:

**ORCA INTERACTIVE LTD. (100.0%)**
**P.O. Box 2220 22 Zarhin Street**
**4366248 Ra'anana, IL**

(72) Inventor/es:

**TOUEG, YAACOV**

(74) Agente/Representante:

**ELZABURU, S.L.P**

## DESCRIPCIÓN

Método y sistema para asegurar un acceso de un cliente a servicios de agente DRM para un reproductor de video

**1. Campo técnico**

La presente invención se refiere al campo de asegurar el acceso de un cliente a los servicios de un agente DRM y más particularmente de asegurar el acceso de un cliente a un servicio de servicios de un agente DRM de un reproductor de video.

**2. Técnica relacionada**

Una solución conocida de Adobe, se describe en el número de documento de patente US90271A3 que describe un proceso de autenticación de un reproductor de video (llamado Componente de tiempo de ejecución) por un agente de CA-DRM. Este proceso incluye recibir contenido cifrado y un componente de autenticación dado de un sistema informático remoto. El componente de autenticación se puede configurar para autenticar un componente de tiempo de ejecución descifrando al menos una parte del contenido cifrado. De esta manera, el sistema cliente puede garantizar que el descifrado del contenido cifrado solo se produzca si varios componentes autentican el componente de tiempo de ejecución, según algunas realizaciones.

Otra solución es propuesta por Trusted Logic en la solicitud de patente No. US2009165148. Esta invención se refiere a un método para autenticar aplicaciones de un sistema informático que incluye: un microprocesador, una pluralidad de aplicaciones, un sistema operativo general (OS2) que puede ejecutar y administrar las aplicaciones y que puede asociar cada identificador de aplicación (3) con la información de identificación requerida para su ejecución, y un entorno de confianza (EC) que ofrece servicios a dichas aplicaciones. Según la invención, antes de que una aplicación pueda acceder a los servicios del entorno de confianza (EC), se realiza una operación de hash sobre la información de identificación de dicha aplicación y el entorno de confianza (EC) verifica la autenticidad del resultado de la operación de hash.

La solicitud internacional WO2007077362 describe un servicio OS para autenticar las aplicaciones y bibliotecas. La invención se refiere a un método para autenticar aplicaciones de un sistema informático que incluye: un microprocesador, una pluralidad de aplicaciones, un sistema operativo general (OS2) que puede ejecutar y administrar las aplicaciones y que puede asociar cada identificador de aplicación (3) con la identificación de información requerida para su ejecución, y un entorno confiable (EC) que ofrece servicios a dichas aplicaciones. Según la invención, antes de que una aplicación pueda acceder a los servicios del entorno de confianza (EC), se realiza una operación de hash sobre la información de identificación de dicha aplicación y el entorno de confianza (EC) verifica la autenticidad del resultado de la operación de hash.

La invención se expone en el conjunto de reivindicaciones adjunto.

La presente invención proporciona un método para asegurar el acceso del módulo informático del cliente a los servicios de un agente DRM.

El método comprende los pasos de:

- Enviar, por parte del cliente, una solicitud obtener-token al agente DRM;

- Aplicar los siguientes pasos por el agente DRM:

  a. Recibir la solicitud obtener-token;

  b. aplicar una función para generar un identificador de solicitud de descifrado IDSolicitud y un Token de valor token, y devolver IDSolicitud y Token al cliente;

  c. insertar, en una tabla hash de valores de token con identificadores de solicitudes obtener-token como claves, registrados en una memoria del agente DRM, un registro que comprende el Token de valor de token asociado a la clave IDSolicitud;

- aplicar los siguientes pasos por el cliente:

  d. recibir IDSolicitud y Token del agente DRM;

  e. calcular un resumen de un fragmento cifrado de contenido multimedia usando el Token y una clave privada;

  f. calcular una solicitud de descifrado del fragmento cifrado de contenido multimedia, que comprende IDSolicitud, el fragmento cifrado y el resumen del fragmento cifrado;

  g. enviando al agente DRM, la solicitud de descifrado del fragmento cifrado;

y aplicar los siguientes pasos por el agente DRM:

h. recibir, la solicitud de descifrado;

i. recuperar el token, de la tabla hash, basado en IDSolicitud;

j. procesar el resumen utilizando una clave pública y token;

k. comprobar la coincidencia entre el resumen procesado y al menos parte del fragmento cifrado;

l. solo en caso de coincidencia: descifrar el fragmento cifrado y devolver el fragmento descifrado al cliente;

i. en donde al menos un paso de recepción, procesamiento, descifrado informático es realizado por un procesador.

Según algunas realizaciones de la invención, se aplica lo siguiente:

- la solicitud obtener-token comprende un identificador IDCliente del cliente;

- la función usa IDCliente como entrada;

- el registro de la tabla hash incluye además el IDCliente asociado con la clave IDSolicitud;

- la solicitud de descifrado comprende además un identificador ID2Cliente del cliente;

- la recuperación del Token se realiza conjuntamente con la recuperación del IDCliente, y el procesamiento posterior del resumen y el descifrado de fragmentos cifrados solo se realizan en caso de coincidencia entre el IDCliente y el ID2Cliente.

Según algunas realizaciones de la invención, la coincidencia de comprobación entre el resumen procesado y al menos parte del fragmento cifrado incluye realizar una operación XOR entre el Token y la al menos parte del fragmento cifrado.

Según con algunas realizaciones de la invención, en caso de no coincidencia, la aplicación del cliente finaliza.

Según algunas realizaciones de la invención, el método comprende además la etapa de eliminar el registro que comprende el Token de valor de token asociado a la clave IDSolicitud de la tabla hash después de que se maneje la solicitud de descifrado.

Según algunas realizaciones de la invención, el proceso de gestión de la tabla hash y el proceso de comunicación con el cliente están protegidos en términos de exclusión mutua dentro del agente DRM, para evitar que el cliente obtenga acceso a la tabla hash.

Según algunas realizaciones de la invención, el método utiliza además múltiples claves públicas como una lista blanca de clientes autorizados para soportar múltiples fuentes de clientes.

El presente documento proporciona un método para asegurar el acceso del módulo informático de un cliente a los servicios de un agente DRM. El método comprende los pasos de:

recibir la solicitud de obtención-token del cliente;

aplicar una función para generar un identificador de solicitud de descifrado IDSolicitud y un Token de valor token, y devolver IDSolicitud y Token al cliente;

insertar, en una tabla hash de valores de token con identificadores de solicitudes obtener-token como claves, registradas en una memoria del agente DRM, un registro que comprende el Token de valor de token asociado al ID de Solicitud de clave;

recibir, la solicitud de descifrado de un fragmento cifrado de contenido multimedia, que comprende el IDSolicitud, el fragmento cifrado y un resumen del fragmento cifrado;

recuperar el Token, de la tabla hash, en base al IDSolicitud;

procesar el resumen utilizando una clave pública y el token;

comprobar la coincidencia entre el resumen procesado y al menos parte del fragmento cifrado;

solo en caso de coincidencia: descifrar el fragmento cifrado y devolver el fragmento descifrado al cliente.

En donde al menos un paso de recepción, procesamiento, descifrado informático es realizado por un procesador.

El presente documento proporciona un método de un sistema para asegurar el acceso de un cliente a los servicios de un agente DRM, dicho sistema está compuesto por:

un módulo de algoritmo de cliente para recibir el IDSolicitud y el Token del agente DRM, calcular un resumen de un fragmento cifrado de contenido multimedia usando el Token y una clave privada, calcular una solicitud de descifrado del fragmento cifrado de contenido multimedia, que comprende el IDSolicitud, el fragmento cifrado y el resumen del fragmento cifrado y enviar al agente DRM, la solicitud de descifrado del fragmento cifrado;

un módulo de manejo de solicitudes obtener-token para recibir una solicitud obtener-token, aplicar una función para generar un identificador de solicitud de descifrado IDSolicitud y un Token de valor de token, devolver el IDSolicitud y el Token al cliente e insertar en una tabla hash de valores de token con identificadores de solicitudes obtener-token como claves, un registro que comprende el Token de valor token asociado a la clave IDSolicitud;

un módulo de manejo de solicitudes de descifrado para recibir una solicitud de descifrado de un fragmento cifrado de contenido multimedia que comprende el IDSolicitud, el fragmento cifrado y un resumen del fragmento cifrado, recuperar el Token, de la tabla hash en base al IDSolicitud, procesar el resumen utilizando una clave pública y el Token, comprobar la coincidencia entre el resumen procesado y al menos parte del fragmento cifrado y, solo en caso de coincidencia: descifrar el fragmento cifrado y devolver el fragmento descifrado al cliente.

m. El presente documento proporciona un método del sistema:

la solicitud obtener-token comprende un identificador IDCliente del cliente;

la función usa el IDCliente como entrada;

el registro de la tabla hash incluye además el IDCliente asociado con la clave IDSolicitud;

la solicitud de descifrado comprende además un identificador ID2Cliente del cliente.

Según algunas realizaciones de la presente invención, la comprobación de la coincidencia entre el resumen procesado y al menos parte del fragmento cifrado incluye realizar una operación XOR entre el Token y la al menos parte del fragmento cifrado.

Según algunas realizaciones de la presente invención, en caso de no coincidencia, la aplicación del cliente finaliza.

Según algunas realizaciones de la presente invención que comprende además medios para proteger, en términos de exclusión mutua dentro del agente DRM, el proceso de gestión de la tabla hash y el proceso de comunicación con el cliente para evitar que el cliente obtenga acceso a la tabla hash.

Según algunas realizaciones de la presente invención, un método de solicitud de descifrado para llevar. Comprendiendo el método de solicitud de descifrado, realizar por el cliente los pasos de:

Enviar una solicitud obtener-token al agente DRM;

recibir el IDSolicitud y el Token del agente DRM;

calcular un resumen de un fragmento cifrado de contenido multimedia usando el Token y una clave privada;

calcular una solicitud de descifrado del fragmento cifrado de contenido multimedia, que comprende el IDSolicitud, el fragmento cifrado y el resumen del fragmento cifrado;

enviar al agente DRM, la solicitud de descifrado del fragmento cifrado;

en donde al menos un paso de recepción, procesamiento, descifrado informático es realizado por un procesador.

Según algunas realizaciones de la presente invención, un cliente para implementar el método de solicitud de descifrado de la reivindicación 14, dicho cliente está compuesto por un módulo de firma para calcular un resumen de un fragmento cifrado de contenido multimedia usando el Token y una clave privada.

**Breve descripción de los dibujos**

Para una mejor comprensión de la invención y para mostrar cómo puede llevarse a cabo la misma, ahora se hará referencia, simplemente a modo de ejemplo, a los dibujos adjuntos en los que números similares designan elementos o secciones correspondientes en todas partes.

En los dibujos adjuntos:

La Figura 1 es un diagrama de bloques esquemático de alto nivel del agente DRM con el reproductor de video, según con la presente invención;

La Figura 2 es un diagrama de bloques esquemático de alto nivel del agente DRM, según la presente invención;

La Figura 3 es un diagrama de flujo de alto nivel que ilustra el algoritmo global del agente DRM, según algunas realizaciones de la presente invención.

La Figura 4 es un diagrama de flujo de alto nivel que ilustra el algoritmo del cliente implementado por el reproductor de video, según algunas realizaciones de la presente invención.

La Figura 5 es un diagrama de flujo de alto nivel que ilustra el algoritmo del módulo de manejo de solicitudes Obtener-token, según algunas realizaciones de la presente invención.

La Figura 6 es un diagrama de flujo de alto nivel que ilustra el módulo de manejo de solicitudes de descifrado, según algunas realizaciones de la presente invención.

**Descripción detallada**

Con referencia específica ahora a los dibujos en detalle, se enfatiza que los detalles mostrados son a modo de ejemplo y para propósitos de discusión ilustrativa de las realizaciones preferidas de la presente invención solamente, y se presentan con la causa de proporcionar lo que se cree ser la descripción más útil y fácil de entender de los principios y aspectos conceptuales de la invención. A este respecto, no se intenta mostrar detalles estructurales de la invención con más detalle del necesario para una comprensión fundamental de la invención, la descripción tomada con los dibujos hace evidente a los expertos en la técnica cómo las diversas formas de la invención pueden ser incorporadas en la práctica.

Antes de explicar al menos una realización de la invención en detalle, debe entenderse que la invención no está limitada en su aplicación a los detalles de construcción y a la disposición de los componentes establecidos en la siguiente descripción o ilustrados en los dibujos. La invención es aplicable a otras realizaciones y puede practicarse o llevarse a cabo de varias maneras. Además, debe entenderse que la fraseología y la terminología empleadas en este documento tienen fines descriptivos y no deben considerarse como limitantes.

Antes de exponer los antecedentes de la técnica relacionada, puede ser útil establecer definiciones de ciertos términos que se utilizarán más adelante.

El objetivo de la invención es optimizar los recursos utilizados para proporcionar esta seguridad, y en particular para minimizar su huella de CPU, utilizando un mínimo de memoria de CPU. Otra ventaja de la invención es que la invención proporciona autenticación de cliente asíncrona para cada fragmento de contenido multimedia enviado al Agente DRM.

La Figura 1 es un diagrama de bloques esquemático de alto nivel del agente DRM con el reproductor de video, según la presente invención. La presente invención proporciona una solución para autenticar la comunicación de un reproductor de video 2, que tiene un módulo de firma 3, con un agente 1 DRM.

La Figura 2 es un diagrama de bloques esquemático de alto nivel del agente DRM, según la presente invención. El agente DRM se compone del módulo 10 de manejo de solicitudes de token para manejar las solicitudes de token recibidas del reproductor de video, un módulo 20 de manejo de solicitudes de descifrado para manejar las solicitudes de descifrado del reproductor de video y proporcionar contenido descifrado usando el módulo 40 de descifrado, y un módulo 25 de gestión de tabla hash para gestionar la tabla 30 hash. El módulo de descifrado puede usar cualquier método de descifrado conocido en la técnica.

La Figura 3 es un diagrama de flujo de alto nivel que ilustra el algoritmo global del agente DRM, de acuerdo con algunas realizaciones de la presente invención. El algoritmo global del agente DRM realiza al menos uno de los siguientes pasos:

- recibir de un reproductor de video una solicitud obtener-token para el Agente DRM (paso 110),

- aplicar una función de devolución de llamada obtener-token () que devuelve dos parámetros de salida: un identificador de solicitud de descifrado IDSolicitud y un Token de valor de token (paso 115),

- insertar en una tabla 30 hash (ver Figura 2) de valores de token con identificadores de solicitudes de descifrado como claves (paso 120), un registro compuesto por IDSolicitud y Token,

- recibir una solicitud de descifrado de fragmentos cifrados de contenido multimedia junto con un identificador de solicitud de descifrado, el fragmento cifrado y un resumen del fragmento cifrado (paso 130),

- procesar el resumen y recuperar el valor del token según el identificador de solicitud de descifrado recibido de la tabla hash (paso 140), y autenticar la solicitud de descifrado (paso 150),

- descifrar el fragmento cifrado y devolver el fragmento descifrado resultante (solo si la solicitud de descifrado se autenticó) (paso 155),

- eliminar el registro compuesto por el IDSolicitud y el Token de la tabla 30 hash.

La tabla hash es un conjunto desordenado de registros, cada uno asociado a un identificador de solicitud de descifrado IDSolicitud, un Token de valor de token y un identificador de cliente (IDCliente). El mantenimiento de la tabla hash consiste esencialmente en agregar y/o eliminar un registro a la tabla hash.

Según algunas realizaciones de la presente invención, un valor de token es un valor aleatorio suficientemente fuerte.

La autenticación de la solicitud de obtención de token consiste en realizar la operación XOR entre el Token de valor token recuperado y los primeros 16 bytes del fragmento y comparar el resultado obtenido con el fragmento cifrado enviado para el descifrado (paso 150). Si hay una coincidencia, la solicitud se autentica como emitida por un cliente autorizado, el fragmento cifrado se descifra, el fragmento transparente resultante se transmite al reproductor de video (paso 160) y el registro que comprende el IDSolicitud y el Token se elimina de la tabla hash. Si no hay coincidencia, la aplicación del reproductor de video se bloquea o finaliza (etapa 170), y no se necesita descifrar el fragmento.

La Figura 4 es un diagrama de flujo de alto nivel que ilustra el algoritmo del reproductor de video, según algunas realizaciones de la presente invención.

De manera preliminar, al reproductor de video se le asigna un par de claves privadas y públicas en una infraestructura de clave pública. La clave privada solo es registrada por el módulo de firma. La clave pública está disponible públicamente y, por lo tanto, para el agente DRM.

El reproductor de video realiza al menos uno de los siguientes pasos: enviar al agente DRM una solicitud de obtención de token, recibir en respuesta el identificador de solicitud de descifrado IDSolicitud y el Token de valor de token, calcular, mediante el módulo de firma, un resumen del fragmento cifrado mediante cifrado, utilizando los siguientes parámetros: Clave-Privada, el resultado de una operación XOR realizada en el valor del token recibido y los primeros 16 bytes del fragmento cifrado (en caso de que el fragmento cifrado sea más corto que 16 bytes, debe ser completado con ceros) (210); una vez que se calcula el resumen, se envía al agente DRM una solicitud de descifrado, el resumen y el fragmento cifrado (220). Al final del proceso, el fragmento descifrado se recibe del agente DRM (230).

La Figura 5 es un diagrama de flujo de alto nivel que ilustra el algoritmo del módulo de manejo de solicitudes obtener-token, según algunas realizaciones de la presente invención. El algoritmo del módulo de manejo de solicitudes obtener-token, incluye al menos uno de los siguientes pasos: lanzar el Agente DRM (310), esperar la solicitud 320 obtener-token, identificar el evento de solicitud obtener-token con el identificador de cliente IDCliente (paso 330), si IDCliente es conocido por el agente DRM (paso 340), generar un Token de valor token y un identificador de solicitud de descifrado IDSolicitud (paso 360), enviar la llamada obtener-token (IDSolicitud, Token) (paso 370) y almacenar el IDSolicitud, el IDCliente y el Token en la tabla hash (paso 380). Si el agente DRM desconoce el IDCliente, enviar un error de devolución de llamada obtener-token (0,0) (paso 350). En caso de que solo se espere un cliente, no se necesita el identificador de cliente IDCliente.

La Figura 6 es un diagrama de flujo de alto nivel que ilustra el algoritmo del módulo de manejo de solicitudes de descifrado, según algunas realizaciones de la presente invención. El algoritmo del módulo de manejo de solicitudes de descifrado incluye los siguientes pasos:

- Lanzar el Agente DRM (paso 410) y esperar la solicitud de descifrado (paso 420),

- recibir una solicitud de descifrado junto con el IDCliente, el IDSolicitud, un resumen del fragmento cifrado y el fragmento cifrado (paso 430), y comprobar si IDSolicitud está disponible en la tabla hash (paso 440). En caso afirmativo, obtener el IDCliente y el Token asociados de la tabla hash (paso 450), y luego verificar si el IDCliente recuperado de la tabla hash coincide con el IDCliente recibido con la solicitud (paso 460). En caso afirmativo, calcular el parámetro temporal Temp procesando el resumen utilizando una clave pública, aplicar la función XOR con el Token (paso 470) y luego hacer corresponder Temp con el fragmento cifrado que comienza (paso 480). En caso de coincidencia, realizar las siguientes operaciones: descifrar el fragmento cifrado (paso 482) para obtener el fragmento limpio, eliminar el registro IDSolicitud de la tabla hash (paso 484) y enviar la llamada de descifrado que incluye el fragmento claro (fragmento descifrado) al cliente. En caso de no coincidencia, finalizar el agente DRM (paso 490) sin descifrar el fragmento (cifrado).

Según algunas realizaciones de la presente invención, el dispositivo cliente no es un reproductor de video, sino otro tipo de dispositivo. Por ejemplo, el dispositivo cliente es un decodificador de video, o es otro tipo de reproductor multimedia como un reproductor de audio.

Según algunas realizaciones de la presente invención, se usa una función ordinaria en lugar de una función de devolución de llamada.

Según algunas realizaciones de la presente invención, el proceso de gestión de la tabla hash dentro del agente DRM y la comunicación del reproductor de video al agente DRM están protegidos en términos de exclusión mutua, para evitar que el reproductor de video obtenga acceso a la tabla hash. Esta protección tiene como objetivo garantizar que estos procesos concurrentes no se ejecuten simultáneamente. Se pueden usar varias soluciones de hardware y software para asegurar la comunicación y el procesamiento de la tabla hash que se conocen en el campo del control de concurrencia. Ejemplos de soluciones de hardware son: interrupciones de desactivación y de espera ocupada.

Entre las soluciones de software, varios algoritmos también dependen de la espera ocupada, mientras que otros utilizan las capacidades de sincronización de sistemas operativos. (Véase por ejemplo https://en.wikipedia.org/wiki/Mutual_exclusion # cite note-6 para obtener más información sobre este tema)

Según algunas realizaciones de la presente invención, las llamadas del reproductor de video, que se envían durante la reproducción cada vez que el reproductor de video recibe o lee un fragmento de contenido multimedia cifrado y tienen que ser procesadas por el reproductor de video, aparecen en pares: la solicitud obtener-token se enviará primero y luego la solicitud de descifrado de fragmentos.

Según algunas realizaciones de la presente invención, un identificador de solicitud de descifrado IDSolicitud es un número de recuento entero simple. También puede ser cualquier otro tipo de número de valor fijo o cadena de caracteres, por ejemplo, calculado al azar.

Según algunas realizaciones de la presente invención, el token generado es aleatorio suficientemente fuerte, calculado por medio de un generador de números pseudoaleatorios.

Según algunas realizaciones de la presente invención, admite múltiples fuentes de reproductores de video mediante el uso de múltiples claves públicas como una lista blanca de reproductores de video autorizados.

Según algunas realizaciones de la presente invención, los 16 bytes del fragmento encriptado utilizado para calcular su resumen no son los primeros 16. Por ejemplo, son los últimos 16. En otro ejemplo, los 16 bytes usados del fragmento encriptado usado para calcular su resumen, no son bytes consecutivos.

Según algunas realizaciones de la presente invención, se usa un índice basado en el token para seleccionar los 16 bytes dentro del fragmento de video enviado para descifrado. Por ejemplo, si un bit de peso dado del token tiene un valor 0, respectivamente 1, entonces se utilizan los primeros, respectivamente los últimos, 16 bytes.

Según algunas realizaciones de la presente invención, se utiliza un índice de cada bit el cual corresponde a un byte de un fragmento cifrado de manera similar: dependiendo de cada valor de bit del índice, se tiene en cuenta el byte correspondiente del fragmento cifrado o no. Por ejemplo, el índice se calcula de forma pseudoaleatoria. En otro ejemplo, el índice se renueva con una frecuencia predeterminada.

Según algunas realizaciones de la presente invención, se usa otro número de bytes del fragmento cifrado para calcular su resumen. Por ejemplo, se utilizan 8 o 32 bytes.

Según algunas realizaciones de la invención, en caso de que el fragmento cifrado sea más corto que 16 bytes, debe rellenarse con unos, o mediante otra secuencia predeterminada de valores de bit.

Según algunas realizaciones de la presente invención, se sugiere definir un límite de tamaño de ventanas, para limitar el número de solicitudes pendientes simultáneas para el descifrado de fragmentos.

Según algunas realizaciones de la presente invención, se sugiere agregar una lista blanca de reproductores autorizados que usan el sistema de mensajería DRM para soportar la gestión de la tabla hash.

Según algunas realizaciones de la presente invención, se sugiere reemplazar la función XOR básica por cualquier función biyectiva F (Token, primeros 16 bytes)/$F^{-1}$(Token, primeros 16 bytes), como un algoritmo de cifrado simétrico como el Algoritmo de Cifrado Mínimo (TEA) que usa el Token como clave

La principal ventaja de esta invención es que la huella de CPU utilizada se optimiza utilizando una memoria de CPU mínima. Otra ventaja es que el sistema según la presente invención proporciona autenticación de cliente asíncrona para cada fragmento enviado al Agente DRM.

El sistema de la presente invención puede incluir, según ciertas realizaciones de la invención, memoria legible por máquina que contiene o almacena un programa de instrucciones que, cuando es ejecutado por la máquina, implementa algunos o todos los aparatos, métodos, características y funcionalidades de la invención mostrada y descrita aquí. Alternativamente o además, el aparato de la presente invención puede incluir, según ciertas realizaciones de la invención, un programa como el anterior que se puede escribir en cualquier lenguaje de programación convencional, y opcionalmente una máquina para ejecutar el programa tal como, pero no limitado a una ordenador de propósito general que puede configurarse o activarse opcionalmente según las enseñanzas de la presente invención. Cualquiera de las enseñanzas incorporadas en este documento puede, siempre que sea adecuado, operar con señales representativas de objetos o sustancias físicas.

A menos que se indique específicamente lo contrario, como se desprende de las siguientes discusiones, se aprecia que a lo largo de las discusiones de la especificación, se utilizar términos como "procesamiento", "computación", "estimación", "selección", "clasificación", "calificación", "cálculo", "determinación", "generación", "reevaluación", "clasificación", "generación", "producción", "coincidencia estéreo", "registro", "detección", "asociación", "superposición", "obtención" o similar, se refieren a la acción y/o procesos de un ordenador o sistema informático, o procesador o dispositivo informático electrónico similar, que manipula y/o transforma datos representados como cantidades físicas, como electrónicas, dentro del sistema informático registros y/o memorias, en otros datos

representados de manera similar como cantidades físicas dentro de las memorias, registros u otros dispositivos de almacenamiento, transmisión o visualización de información del sistema informático. El término "ordenador" debe interpretarse en términos generales para cubrir cualquier tipo de dispositivo electrónico con capacidades de procesamiento de datos, incluidos, a modo de ejemplo no limitativo, ordenadores personales, servidores, sistemas informáticos, dispositivos de comunicación, procesadores (por ejemplo, procesador de señal digital (DSP) ), microcontroladores, matrices de puertas programables en campo (FPGA), circuito integrado de aplicación específica (ASIC), etc.) y otros dispositivos informáticos electrónicos.

La presente invención puede describirse, simplemente por claridad, en términos de terminología específica para lenguajes de programación, sistemas operativos, navegadores, versiones de sistemas, productos individuales y similares particulares. Se apreciará que esta terminología pretende transmitir principios generales de funcionamiento de manera clara y breve, a modo de ejemplo, y no pretende limitar el alcance de la invención a ningún lenguaje de programación, sistema operativo, navegador, versión de sistema o producto individual.

Se aprecia que los componentes de software de la presente invención, incluidos los programas y los datos, pueden, si se desea, implementarse en forma de ROM (memoria de solo lectura), incluyendo CD-ROM, EPROM y EEPROM, o pueden almacenarse en cualquier otro medio legible por ordenador no transitorio adecuado , tal como, pero no limitado a, discos de diversos tipos, tarjetas de diversos tipos y RAM. Los componentes descritos aquí como software pueden, de manera alternativa, implementarse total o parcialmente en hardware, si se desea, usando técnicas convencionales. Por el contrario, los componentes descritos aquí como hardware pueden, alternativamente, implementarse total o parcialmente en software, si se desea, usando técnicas convencionales.

Incluidos en el alcance de la presente invención, entre otras cosas, están las señales electromagnéticas que llevan instrucciones legibles por ordenador para realizar cualquiera o todos los pasos de cualquiera de los métodos mostrados y descritos aquí, en cualquier orden adecuado; instrucciones legibles por máquina para realizar cualquiera o todos los pasos de cualquiera de los métodos mostrados y descritos aquí, en cualquier orden adecuado; dispositivos de almacenamiento de programas legibles por máquina, que incorporan de manera tangible un programa de instrucciones ejecutables por la máquina para realizar cualquiera o todos los pasos de cualquiera de los métodos mostrados y descritos aquí, en cualquier orden adecuado; un producto de programa informático que comprende un medio utilizable por ordenador que tiene un código de programa legible por ordenador, tal como un código ejecutable, que se ha incorporado al mismo, y/o que incluye un código de programa legible por ordenador para realizar cualquiera o todos los pasos de cualquiera de los métodos mostrados y descritos en la presente memoria, en cualquier orden adecuado; cualquier efecto técnico provocado por alguno o todos los pasos de cualquiera de los métodos mostrados y descritos aquí, cuando se realiza en cualquier orden adecuado; cualquier aparato o dispositivo adecuado o combinación de los mismos, programado para realizar, solo o en combinación, cualquiera o todos los pasos de cualquiera de los métodos mostrados y descritos en la presente memoria, en cualquier orden adecuado; dispositivos electrónicos, cada uno incluyendo un procesador y un dispositivo de entrada y/o dispositivo de salida cooperativo y operativos para realizar en el software los pasos mostrados y descritos en la presente memoria; dispositivos de almacenamiento de información o registros físicos, como discos o discos duros, que hacen que se configure un ordenador u otro dispositivo para llevar a cabo cualquiera o todos los pasos de cualquiera de los métodos mostrados y descritos en la presente memoria, en cualquier orden adecuado; un programa pre-almacenado, por ejemplo en la memoria o en una red de información como Internet, antes o después de la descarga, que incluye cualquiera o todos los pasos de cualquiera de los métodos mostrados y descritos en este documento, en cualquier orden adecuado, y el método de carga o descarga, y un sistema que incluye un servidor o servidores y un cliente o clientes para usarlo; y hardware que realiza cualquiera o todos los pasos de cualquiera de los métodos mostrados y descritos aquí, en cualquier orden adecuado, ya sea solo o junto con el software. Cualquier medio legible por ordenador o legible por máquina descrito en la presente memoria está destinado a incluir medios legibles por ordenador o máquina no transitorios.

Cualquier cálculo u otras formas de análisis descritas en este documento pueden realizarse mediante un método informático adecuado. Cualquier paso descrito aquí puede ser implementado por ordenador. La invención mostrada y descrita en la presente memoria puede incluir (a) usar de un método informático para identificar una solución a cualquiera de los problemas o para cualquiera de los objetivos descritos en la presente memoria, la solución opcionalmente incluye al menos uno de entre una decisión, una acción, un producto, un servicio o cualquier otra información descrita en este documento que afecte, de manera positiva, a un problema o unos objetivos descritos en la presente memoria; y (b) generar la solución.

El alcance de la presente invención no se limita a las estructuras y funciones específicamente descritas en la presente memoria y también pretende incluir dispositivos que tengan la capacidad de producir una estructura, o realizar una función, descrita en la presente memoria, de modo que aunque los usuarios del dispositivo no puedan usar la capacidad, son, si así lo desean, capaces de modificar el dispositivo para obtener la estructura o función.

Las características de la presente invención que se describen en el contexto de realizaciones separadas también se pueden proporcionar en combinación en una sola realización.

Por ejemplo, una realización del sistema está destinada a incluir una realización del proceso correspondiente. Además, cada realización del sistema está destinada a incluir una "vista" centrada en el servidor o una "vista" centrada en el

cliente, o una "vista" desde cualquier otro nodo del sistema, de la funcionalidad completa del sistema, medio legible por ordenador, aparato, incluyendo solo aquellas funcionalidades realizadas en ese servidor o cliente o nodo.

**REIVINDICACIONES**

1. Un método para asegurar el acceso del módulo informático de un cliente a los servicios de un agente DRM, comprendiendo dicho método los pasos de:

- Enviar, por parte del cliente, una solicitud obtener-token (210) al agente DRM;

- Aplicar los siguientes pasos (10) por el agente DRM:

  ◦ Recibir la solicitud obtener-token;

  ◦ aplicar una función para generar un identificador de solicitud de descifrado IDSolicitud y un Token de valor de token, y devolver IDSolicitud y Token al cliente;

  ◦ insertar, en una tabla hash de valores de token con identificadores de solicitudes obtener-token como claves, registrados en una memoria del agente DRM, un registro que comprende el Token de valor de token asociado a la clave IDSolicitud;

- aplicar los siguientes pasos (220-240) por el cliente:

  ◦ recibir el IDSolicitud y el Token del agente DRM;

  ◦ calcular un resumen de un fragmento cifrado de contenido multimedia utilizando el Token y una clave privada;

  ◦ calcular una solicitud de descifrado del fragmento cifrado de contenido multimedia, que comprende el IDSolicitud, el fragmento cifrado y el resumen del fragmento cifrado;

  ◦ enviar al agente DRM, la solicitud de descifrado del fragmento cifrado;

- y aplicar los siguientes pasos (20) por el agente DRM:

  ◦ recibir, la solicitud de descifrado;

  ◦ recuperar el Token, de la tabla hash, en base al IDSolicitud;

  ◦ procesar el resumen utilizando una clave pública y Token;

  ◦ comprobar la coincidencia entre el resumen procesado y al menos parte del fragmento cifrado;

  ◦ solo en caso de coincidencia: descifrar el fragmento cifrado y devolver el fragmento descifrado al cliente;

en donde al menos un paso de recepción, procesamiento, descifrado informático es realizado por un procesador.

2. El método de la reivindicación 1 en donde:

- la solicitud obtener-token comprende un identificador IDCliente del cliente;

- la función usa el IDCliente como entrada;

- el registro de la tabla hash incluye además el IDCliente asociado con la clave IDSolicitud;

- la solicitud de descifrado comprende además un identificador ID2Cliente del cliente;

- la recuperación del Token se realiza conjuntamente con la recuperación del IDCliente, y el procesamiento posterior del resumen y el descifrado de los fragmentos cifrados solo se realiza en caso de coincidencia entre el IDCliente y el ID2Cliente.

3. El método de la reivindicación 1, en donde la comprobación de la coincidencia entre el resumen procesado y al menos parte del fragmento cifrado incluye realizar una operación XOR entre el Token y la al menos parte del fragmento cifrado.

4. El método de la reivindicación 1, en el que, en caso de no coincidencia, la aplicación del cliente finaliza.

5. El método de la reivindicación 1 que comprende además el paso de eliminar el registro que comprende el Token de valor de token asociado a la clave IDSolicitud de la tabla hash después de que se maneje la solicitud de descifrado.

6. El método de la reivindicación 1, en el que el proceso de gestión de la tabla hash y el proceso de comunicación con el cliente están protegidos en términos de exclusión mutua dentro del agente DRM, para evitar que el cliente obtenga acceso a la tabla hash.

7. El método de la reivindicación 1 además utiliza múltiples claves públicas como una lista blanca de clientes autorizados para admitir múltiples fuentes de clientes.

8. Un método para asegurar el acceso del módulo informático de un cliente a los servicios de un agente DRM, dicho método comprende los pasos de:

- recibir la solicitud de obtención de token del cliente;

- aplicar una función para generar un identificador de solicitud de descifrado IDSolicitud y un Token de valor token, y devolver el IDSolicitud y el Token al cliente;

- insertar, en una tabla hash de valores de token con identificadores de solicitudes obtener-token como claves, registradas en una memoria del agente DRM, un registro que comprende el Token de valor token asociado al ID de Solicitud de clave;

- recibir, la solicitud de descifrado de un fragmento cifrado de contenido multimedia, que comprende el IDSolicitud, el fragmento cifrado y un resumen del fragmento cifrado;

- recuperar el Token, de la tabla hash, en base al IDSolicitud;

- procesar el resumen utilizando una clave pública y el Token;

- comprobar la coincidencia entre el resumen procesado y al menos parte del fragmento cifrado;

- solo en caso de coincidencia: descifrar el fragmento cifrado y devolver el fragmento descifrado al cliente.

en donde al menos un paso de recepción, procesamiento, descifrado informático es realizado por un procesador.

9. Un sistema para asegurar el acceso de un cliente a los servicios de un agente DRM, estando dicho sistema compuesto por:

- un módulo de algoritmo de cliente para recibir el IDSolicitud y el Token del agente DRM, calcular un resumen de un fragmento cifrado de contenido multimedia usando el Token y una clave privada, calcular una solicitud de descifrado del fragmento cifrado de contenido multimedia, que comprende el IDSolicitud, el fragmento cifrado y el resumen del fragmento cifrado y el envío al agente DRM, la solicitud de descifrado del fragmento cifrado;

- un módulo de manejo de solicitudes obtener-token para recibir una solicitud obtener-token, aplicando una función para generar un identificador de solicitud de descifrado IDSolicitud y un Token de valor token, devolviendo el IDSolicitud y el Token al cliente e insertándolo en una tabla hash de valores de token con identificadores de solicitudes obtener-token como claves, un registro que comprende el token de valor de token asociado a la clave IDSolicitud;

- un módulo de manejo de solicitudes de descifrado para recibir una solicitud de descifrado de un fragmento cifrado de contenido multimedia que comprende el IDSolicitud, el fragmento cifrado y un resumen del fragmento cifrado, recuperar el Token, de la tabla hash en base al IDSolicitud, procesar el resumen utilizando una clave pública y el Token, comprobar la coincidencia entre el resumen procesado y al menos parte del fragmento cifrado y, solo en caso de coincidencia: descifrar el fragmento cifrado y devolver el fragmento descifrado al cliente.

10. El sistema de la reivindicación 9 en el que:

- la solicitud obtener-token comprende un identificador IDCliente del cliente;

- la función usa el IDCliente como entrada;

- el registro de la tabla hash incluye además el IDCliente asociado con la clave IDSolicitud;

- la solicitud de descifrado comprende además un identificador ID2Cliente del cliente.

11. El sistema de la reivindicación 9, en el que la comprobación de la coincidencia entre el resumen procesado y al menos parte del fragmento cifrado incluye realizar una operación XOR entre el Token y la al menos parte del fragmento cifrado.

12. El sistema de la reivindicación 9, en el que, en caso de no coincidencia, la aplicación del cliente finaliza.

13. El sistema de la reivindicación 9, que comprende además medios para proteger, en términos de exclusión mutua dentro del agente DRM, el proceso de gestión de la tabla hash y el proceso de comunicación con el cliente para evitar que el cliente obtenga acceso a la tabla hash.

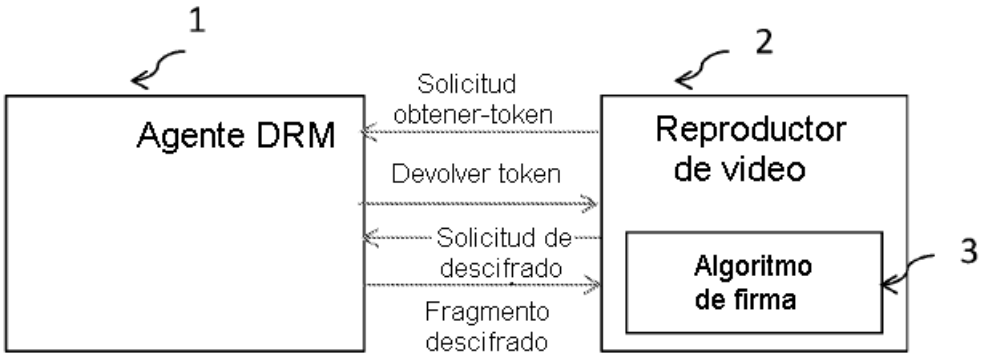
1
2
Agente DRM
Solicitud obtener-token
Devolver token
Solicitud de descifrado
Fragmento descifrado
Reproductor de video
Algoritmo de firma
3

Fig. 1

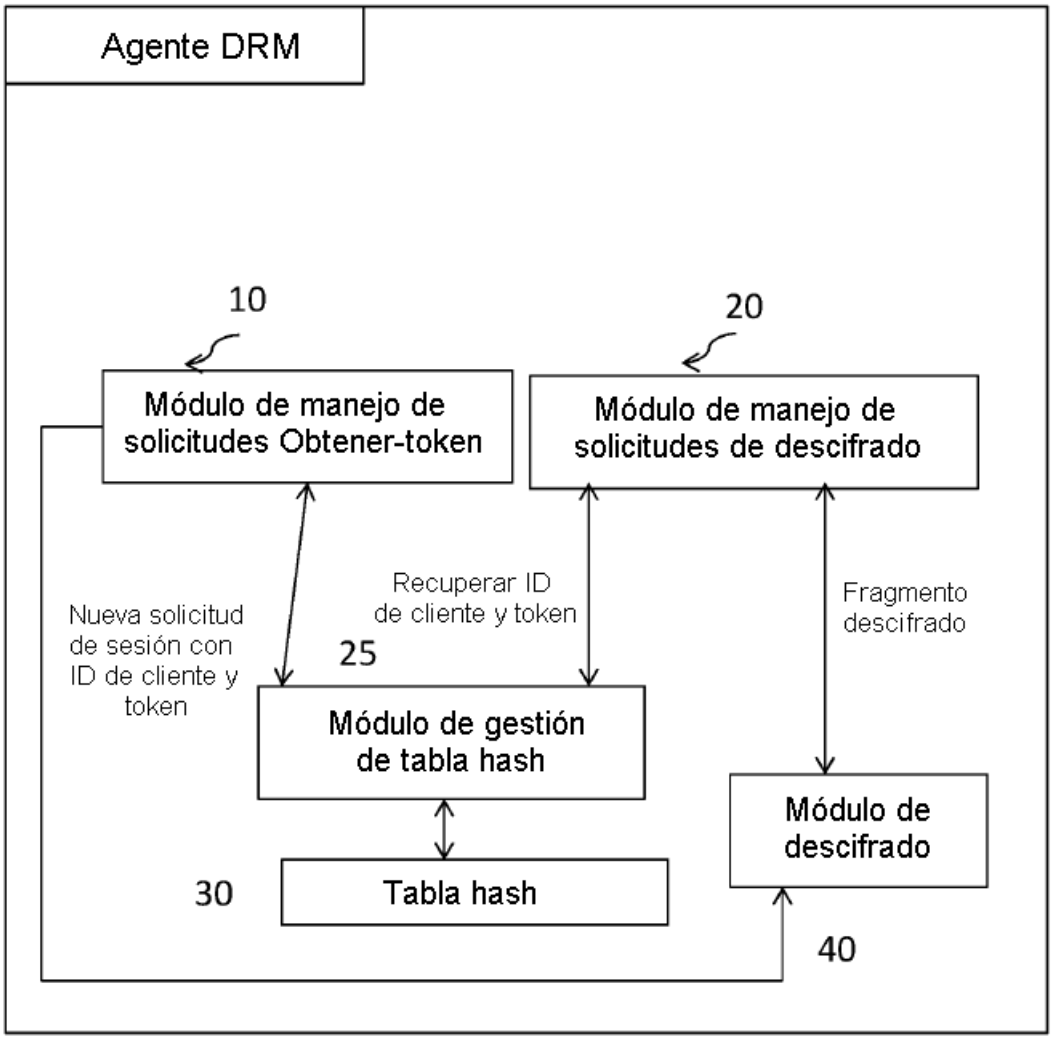
Agente DRM
10
20
Módulo de manejo de solicitudes Obtener-token
Módulo de manejo de solicitudes de descifrado
Nueva solicitud de sesión con ID de cliente y token
Recuperar ID de cliente y token
25
Fragmento descifrado
Módulo de gestión de tabla hash
Módulo de descifrado
30
Tabla hash
40

Fig. 2

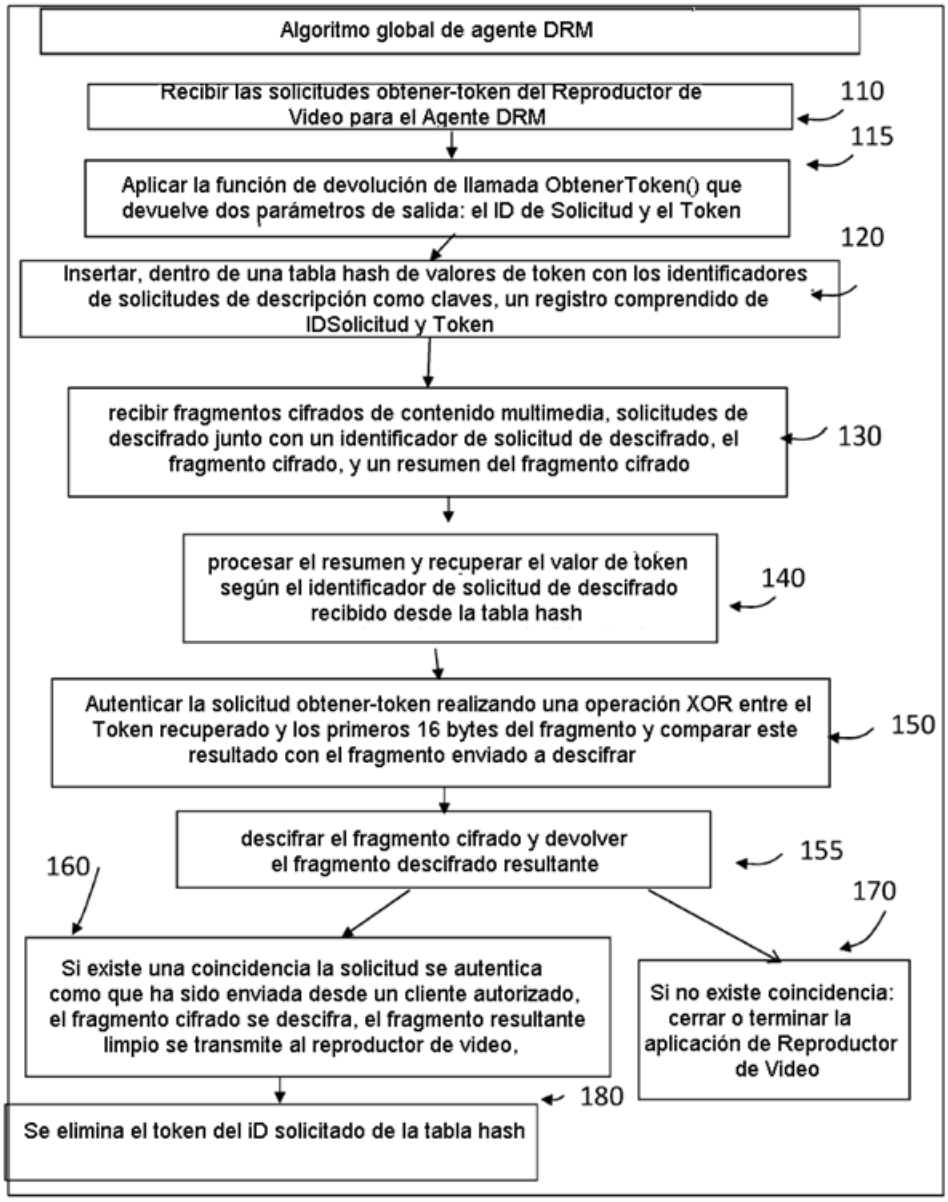
Algoritmo global de agente DRM
Recibir las solicitudes obtener-token del Reproductor de Video para el Agente DRM
110
Aplicar la función de devolución de llamada ObtenerToken() que devuelve dos parámetros de salida: el ID de Solicitud y el Token
115
Insertar, dentro de una tabla hash de valores de token con los identificadores de solicitudes de descripción como claves, un registro comprendido de IDSolicitud y Token
120
recibir fragmentos cifrados de contenido multimedia, solicitudes de descifrado junto con un identificador de solicitud de descifrado, el fragmento cifrado, y un resumen del fragmento cifrado
130
procesar el resumen y recuperar el valor de token según el identificador de solicitud de descifrado recibido desde la tabla hash
140
Autenticar la solicitud obtener-token realizando una operación XOR entre el Token recuperado y los primeros 16 bytes del fragmento y comparar este resultado con el fragmento enviado a descifrar
150
descifrar el fragmento cifrado y devolver el fragmento descifrado resultante
155
160
170
Si existe una coincidencia la solicitud se autentica como que ha sido enviada desde un cliente autorizado, el fragmento cifrado se descifra, el fragmento resultante limpio se transmite al reproductor de video,
Si no existe coincidencia: cerrar o terminar la aplicación de Reproductor de Video
180
Se elimina el token del iD solicitado de la tabla hash

Fig. 3

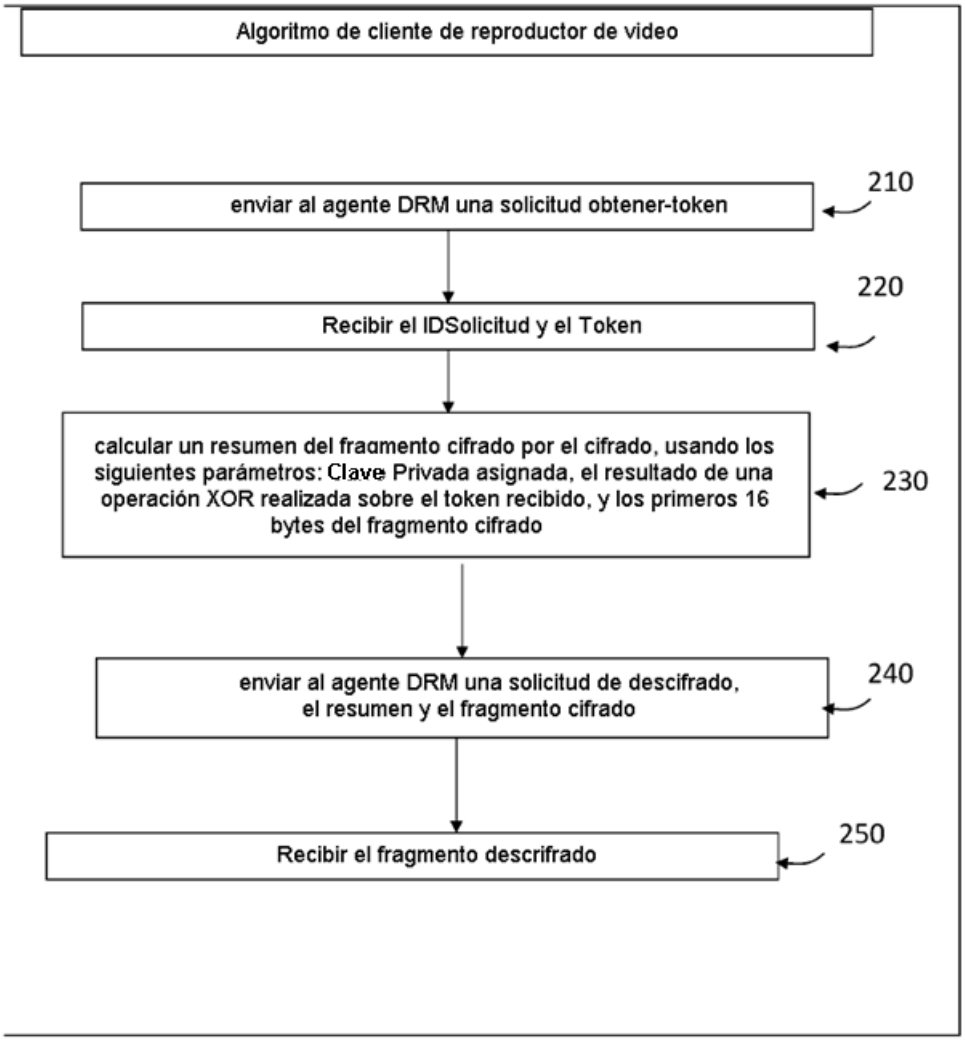
Algoritmo de cliente de reproductor de video
enviar al agente DRM una solicitud obtener-token
210
Recibir el IDSolicitud y el Token
220
calcular un resumen del fragmento cifrado por el cifrado, usando los siguientes parámetros: Clave Privada asignada, el resultado de una operación XOR realizada sobre el token recibido, y los primeros 16 bytes del fragmento cifrado
230
enviar al agente DRM una solicitud de descifrado, el resumen y el fragmento cifrado
240
Recibir el fragmento descrifrado
250

Fig. 4

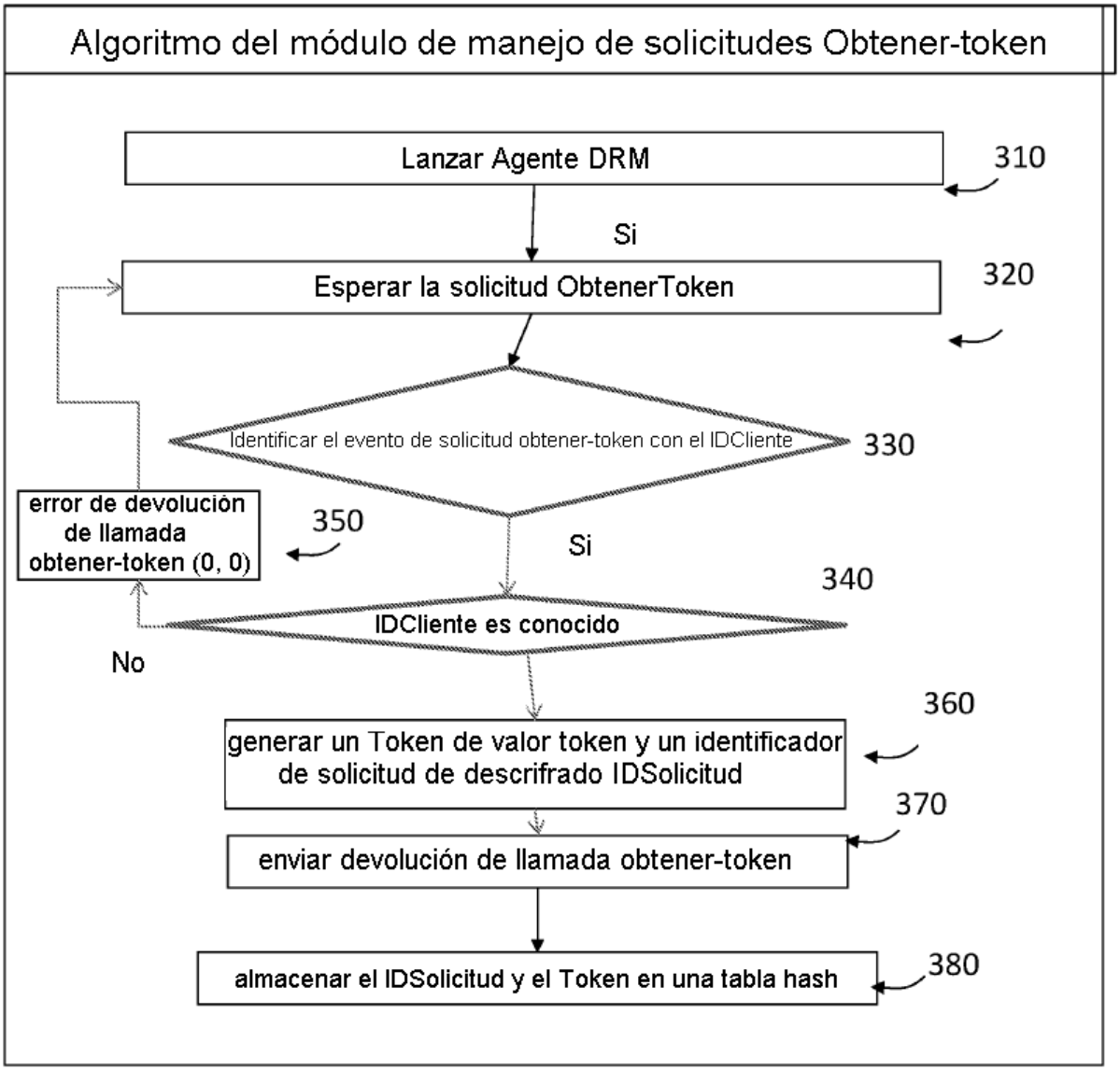
Algoritmo del módulo de manejo de solicitudes Obtener-token
Lanzar Agente DRM
310
Si
Esperar la solicitud ObtenerToken
320
Identificar el evento de solicitud obtener-token con el IDCliente
330
error de devolución de llamada obtener-token (0, 0)
350
Si
340
IDCliente es conocido
No
360
generar un Token de valor token y un identificador de solicitud de descrifrado IDSolicitud
370
enviar devolución de llamada obtener-token
almacenar el IDSolicitud y el Token en una tabla hash
380

Fig. 5

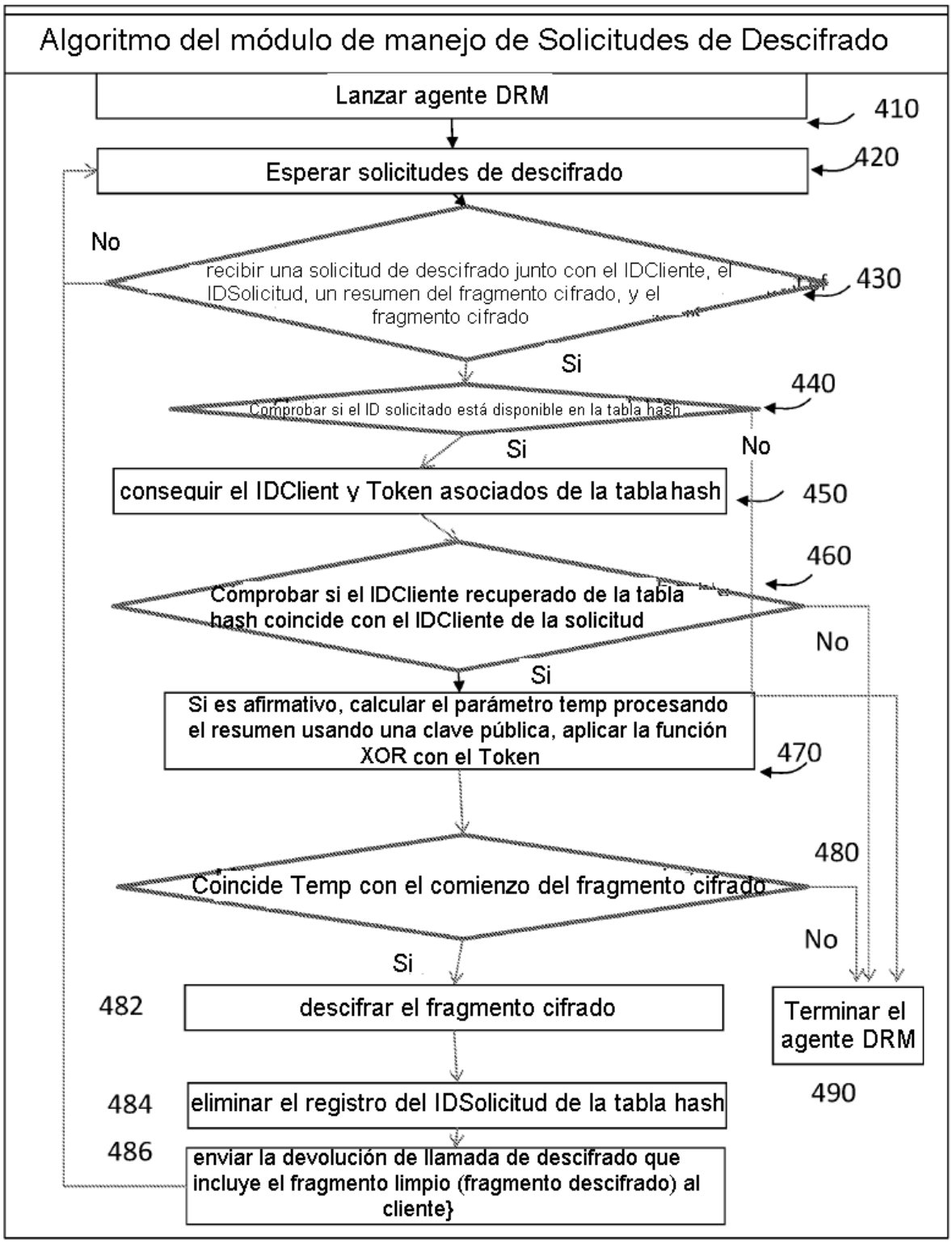
Algoritmo del módulo de manejo de Solicitudes de Descifrado
Lanzar agente DRM
410
Esperar solicitudes de descifrado
420
No
recibir una solicitud de descifrado junto con el IDCliente, el IDSolicitud, un resumen del fragmento cifrado, y el fragmento cifrado
430
Si
Comprobar si el ID solicitado está disponible en la tabla hash
440
Si
No
consequir el IDClient y Token asociados de la tabla hash
450
Comprobar si el IDCliente recuperado de la tabla hash coincide con el IDCliente de la solicitud
460
No
Si
Si es afirmativo, calcular el parámetro temp procesando el resumen usando una clave pública, aplicar la función XOR con el Token
470
Coincide Temp con el comienzo del fragmento cifrado
480
No
Si
482
descifrar el fragmento cifrado
Terminar el agente DRM
490
484
eliminar el registro del IDSolicitud de la tabla hash
486
enviar la devolución de llamada de descifrado que incluye el fragmento limpio (fragmento descifrado) al cliente}

Fig. 6