(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 569 407**

(51) Int. CI.:

G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.05.2005 E 05735197 (5)**

(97) Fecha y número de publicación de la concesión europea: **09.03.2016 EP 1751646**

(54) Título: **Procesamiento de derechos en sistemas DRM**

(30) Prioridad:

17.05.2004 EP 04102157

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.05.2016

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
HIGH TECH CAMPUS 5
5656 AE EINDHOVEN, NL

(72) Inventor/es:

KAMPERMAN, FRANCISCUS L. A. J.;
PETKOVIC, MILAN;
KOSTER, ROBERT P. y
VRIELINK, KOEN H. J.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procesamiento de derechos en sistemas DRM

Esta invención se refiere a un procedimiento de procesamiento de derechos en un sistema de gestión de derechos digitales (DRM), en el que se han creado derechos DRM para controlar el acceso a contenido, comprendiendo el procedimiento la etapa de recibir los derechos DRM en el sistema DRM. La invención se refiere además a un sistema de gestión de derechos digitales (DRM) dispuesto para recibir derechos DRM para controlar el acceso a contenido. Finalmente, la invención se refiere a un medio legible por ordenador que tiene instrucciones almacenadas en el mismo para hacer que una unidad de procesamiento ejecute el procedimiento anterior, así como a un medio legible por ordenador que tiene una plantilla de programa de derechos (RPT) almacenada en el mismo que comprende datos asociados.

Recientes desarrollos en las tecnologías de distribución de contenido (es decir, Internet y medios extraíbles) han facilitado más que nunca el intercambio de contenido. Su rápida aceptación por los consumidores muestra que tales tecnologías satisfacen realmente sus necesidades. Una tecnología que gestiona el acceso a contenido digital es la gestión de derechos digitales (DRM), que es la gestión digital de derechos y proporciona una descripción, identificación, comercialización, protección, supervisión y seguimiento de todas las formas en que pueden usarse tales derechos. DRM permite, por ejemplo, que los proveedores de contenido, los proveedores de servicios y los distribuidores protejan su contenido y mantengan el control de su distribución. El contenido puede protegerse y/o gestionarse creando licencias para cada contenido (digital). Sin embargo, los usuarios finales no pueden influir en el procesamiento de derechos DRM vigente en la actualidad y, por tanto, el procesamiento de derechos DRM puede parecer inflexible a los usuarios finales y puede no satisfacer sus necesidades.

La solicitud de patente europea EP-A-1 509 024, presentada antes pero publicada después de la fecha de presentación de la solicitud de patente del solicitante, describe un sistema en el que se recibe contenido multimedia en un dispositivo que redistribuye el contenido multimedia a uno o más dispositivos adicionales.

El documento "*Secure Content Management in Authorised Domains*", de Heuvel van den, S.A.F.A. et al., International Broadcasting Convention, 15 de septiembre de 2002 (15/09/2002), páginas 467 a 474, divulga un sistema de gestión segura de contenido en dominios autorizados. El sistema permite acceder a contenido a través de una pluralidad de dispositivos en un dominio autorizado.

Un objeto de la presente invención es proporcionar un procedimiento de procesamiento de derechos DRM que proporcione a un usuario final cierta influencia.

Este objeto, entre otros, se consigue con el procedimiento y el sistema especificados en las reivindicaciones independientes. De este modo, un usuario de un sistema DRM puede añadir restricciones/derechos adicionales en relación con los derechos DRM, que se usan para controlar el uso de y el acceso a contenido. Los derechos DRM recibidos pueden ser, por ejemplo, derechos DRM de distribución creados por un distribuidor o un titular de los derechos, por ejemplo un proveedor de servicios y/o un proveedor de contenido. El término "derechos DRM" incluye "derechos DRM recibidos" y "derechos atribuidos al usuario". En lo expuesto anteriormente y a lo largo de esta memoria descriptiva, el término "usuario" incluye el usuario final, por ejemplo una persona que esté usando contenido que tiene derechos DRM.

El usuario puede introducir los derechos atribuidos al usuario a través de un dispositivo para acceder a contenido que tiene derechos DRM o a través de cualquier otro dispositivo, por ejemplo cualquier ordenador conectado en red. Además, puede concebirse que los derechos atribuidos al usuario puedan descargarse, por ejemplo, desde un sitio web; tales derechos atribuidos al usuario que pueden descargarse pueden ser totales, de modo que el usuario no tiene que ajustar ningún parámetro, o parciales, de modo que los derechos atribuidos al usuario contienen parámetros que pueden ajustarse, añadirse y/o modificarse por el usuario.

Evidentemente, las restricciones adicionales de los derechos DRM recibidos solo pueden limitar el acceso al contenido y no ampliar el acceso a/el uso de contenido más allá de los derechos DRM recibidos definidos por el proveedor de contenido/proveedor de servicios/distribuidor. La introducción, por parte del usuario, de derechos atribuidos al usuario para imponer restricciones adicionales en los derechos DRM recibidos en el sistema DRM puede llevarse a cabo antes, durante, con o después de la recepción de los derechos DRM en el sistema DRM.

Debe observarse que el sistema DRM puede imponer el cumplimiento de los derechos creados por/procedentes del proveedor de servicios/proveedor de contenido/distribuidor, es decir, los derechos DRM recibidos, y los derechos atribuidos al usuario. Es preferente que los derechos DRM recibidos y los derechos atribuidos al usuario usen el mismo mecanismo (por ejemplo, el mismo lenguaje de derechos, los mismos bits de expresión de derechos, el mismo tipo de programas de derechos, etc.) ya que tal mecanismo combinado mejora la eficiencia y reduce la complejidad de la arquitectura del sistema. Sin embargo, también puede concebirse la utilización de mecanismos diferentes bajo el control del sistema DRM.

Un caso especial de un sistema DRM es el sistema de gestión de derechos digitales de dominio autorizado (AD-DRM), que es un sistema que gestiona derechos en un dominio autorizado. El dominio autorizado puede considerarse como un entorno de dispositivos, medios, derechos y usuarios, donde los usuarios y los dispositivos gestionan contenido según los derechos, pero con una libertad relativa si se realiza dentro de los límites del dominio autorizado.

Normalmente, un dominio autorizado define un entorno doméstico con una red doméstica y una pluralidad de usuarios pertenecientes a la red doméstica. Evidentemente, otros escenarios son posibles, tales como una red empresarial. Además, un usuario puede llevar consigo cuando viaja un dispositivo portátil para reproducir audio y/o vídeo con una cantidad limitada de contenido y usarlo en su habitación de hotel para acceder a o descargarse contenido adicional almacenado en su sistema de audio y/o vídeo personal instalado en su hogar. Aunque el dispositivo portátil esté fuera de la red doméstica, forma parte del dominio autorizado del usuario.

Para satisfacer las necesidades del proveedor de contenido y del proveedor de servicios, el intercambio entre diferentes entornos domésticos y el uso de contenido deben controlarse por un sistema DRM de distribución. Las restricciones típicas aplicadas al contenido importado antes de su importación en un sistema AD pueden ser restricciones en el número de veces que el contenido puede reproducirse, si el contenido puede exportarse o no, una fecha tras la cual el contenido no puede reproducirse más, etc.

Sin embargo, los sistemas AD-DRM actuales tienen la desventaja de que la gestión de los derechos recibidos en el dominio autorizado solo está determinada por el proveedor de contenido, el proveedor de servicios y/o el distribuidor a través del sistema DRM de distribución. Por lo tanto, un objeto adicional de la invención es proporcionar un procedimiento mejorado de procesamiento de derechos en un sistema AD-DRM, donde a uno o más usuarios de un dominio autorizado se les proporciona cierta influencia.

Este objeto se consigue con el procedimiento según la invención, caracterizado porque el sistema DRM que recibe los derechos DRM es un sistema AD-DRM, comprendiendo además el procedimiento la etapa de, en el sistema AD-DRM, obtener derechos específicos de dominio autorizado (AD) a partir de los derechos DRM recibidos. Por tanto, un usuario en un dominio autorizado puede añadir restricciones/derechos adicionales en relación con los derechos de un sistema de gestión de derechos digitales de domino autorizado (AD-DRM) introduciendo las restricciones adicionales; por lo tanto, el usuario del dominio autorizado puede impedir, por ejemplo, que los niños de la casa accedan a un contenido particular al que podrían acceder de otro modo, ya que son miembros del dominio autorizado al que pertenece el contenido. Evidentemente, las restricciones adicionales en los derechos específicos de dominio autorizado (AD) solo pueden limitar el acceso al contenido y no ampliar el acceso a/el uso de contenido más allá de los derechos específicos de domino autorizado (AD) definidos por el proveedor de contenido/proveedor de servicios/distribuidor.

Ejemplos de tales restricciones adicionales pueden ser: permisos de qué dispositivo(s) puede(n) usarse para acceder a un contenido, permisos de qué personas pueden acceder y cómo pueden usar un contenido, permisos acerca del momento de uso (por ejemplo, no después de una hora determinada, posiblemente en relación con una persona), valores de clasificación parental, una especificación de las personas que pueden exportar el contenido a otros dominios autorizados, una especificación de los dispositivos que pueden exportar el contenido a otros dominios autorizados, etc.

Preferentemente, el usuario puede introducir los derechos atribuidos al usuario en los derechos DRM con o tras la recepción de los derechos DRM. Por tanto, el usuario puede introducir después los derechos atribuidos al usuario para acceder y/o evaluar contenido que tiene derechos DRM, de modo que puede introducir las restricciones/derechos atribuidos al usuario adicionales si desea, por ejemplo, impedir que uno o más de sus hijos accedan al contenido. Debe observarse que lo anterior no excluye la posibilidad de que un usuario pueda introducir los derechos atribuidos al usuario antes de la recepción de los derechos DRM; esto podría realizarse, por ejemplo, a través de un sitio web (del proveedor de servicios) al que se accede a través de Internet y esto podría ser una manera de garantizar que se proteja la integridad de los derechos atribuidos al usuario como una parte integrante de la protección de derechos DRM.

En una realización preferente del procedimiento según la invención, los derechos específicos de dominio autorizado (AD) son derechos de dominio autorizado cruzado (X-AD), que se establecen para controlar: (1) la transferencia de derechos entre dominios autorizados (AD) y (2) el acceso al contenido en otro dominio autorizado, es decir, tras la exportación a otro dominio autorizado. Por tanto, un usuario del sistema AD-DRM puede restringir además cualquier distribución de contenido que tiene derechos X-AD además de las restricciones en los derechos DRM recibidos en el dominio autorizado. Ejemplos de tales restricciones pueden ser una especificación de las personas que pueden exportar el contenido a otros dominios autorizados, o de los dispositivos que pueden exportar el contenido a otros dominios autorizados. Antes o durante el proceso de exportación, un usuario también puede introducir limitaciones en un derecho de dominio autorizado cruzado (X-AD) con respecto al uso del contenido. Estas limitaciones tendrán efecto en el domino autorizado al que se exportan los derechos.

En otra realización preferente del procedimiento según la invención, los derechos específicos de dominio autorizado (AD) son derechos de dominio autorizado (AD) que se han obtenido a partir de los derechos de dominio autorizado cruzado (X-AD), donde los derechos de dominio autorizado (AD) se establecen para controlar el acceso al contenido en un dominio autorizado (AD). De este modo, un usuario puede introducir restricciones adicionales en el uso de contenido importado en el dominio autorizado y, por tanto, tener un mayor control del uso del contenido en los dispositivos del dominio autorizado. Ejemplos de tales restricciones pueden ser: permisos de qué dispositivo(s) puede(n) usar un contenido, permisos de qué personas pueden usar un contenido y cómo pueden usarlo, por ejemplo copia o reproducción, permisos acerca del momento de uso (por ejemplo, no después de una hora determinada, posiblemente en relación con una persona), valores de clasificación parental.

Antes se ha descrito que un usuario puede introducir derechos atribuidos al usuario en forma de restricciones adicionales en derechos DRM recibidos antes, durante, con o tras la recepción de los derechos DRM en el sistema AD-DRM. Por tanto, esto implica que un usuario, por ejemplo un usuario autorizado que especifica los derechos atribuidos al usuario, puede cambiar o actualizar posteriormente los derechos atribuidos al usuario.

En otra realización preferente del procedimiento según la invención, los derechos específicos de dominio autorizado (AD) son derechos de dominio autorizado (AD) que se han obtenido a partir de los derechos de dominio autorizado cruzado (X-AD), donde los derechos de dominio autorizado (AD) se establecen para controlar el acceso al contenido en un dominio autorizado (AD) y donde un usuario ya ha introducido restricciones adicionales en los derechos de dominio autorizado cruzado (X-AD). Por tanto, un usuario puede introducir en otros dominios autorizados restricciones relacionadas con cualquier distribución de contenido que tiene derechos X-AD , así como restricciones relacionadas con el uso de contenido importado en el dominio autorizado y, por tanto, con el uso del contenido en los dispositivos del dominio autorizado.

Aunque anteriormente se ha hecho una distinción entre derechos X-AD y derechos AD, debe observarse que, por lo general, el tratamiento de los dos tipos de derechos es el mismo. Un ejemplo es cuando un derecho DRM, por ejemplo un derecho DRM de distribución, se recibe en el dominio autorizado y un derecho X-AD se obtiene a partir del derecho DRM recibido. Cuando un usuario especifica derechos atribuidos al usuario para este derecho X-AD, el derecho resultante se usa preferentemente para obtener derechos AD sin que el usuario tenga que especificar más restricciones; en cambio, el derecho AD se crea en función de los derechos X-AD más los derechos atribuidos al usuario en forma de restricciones adicionales añadidas a dichos derechos X-AD.

Según la invención, los derechos atribuidos al usuario y los derechos DRM recibidos constituyen dos conjuntos de derechos que están relacionados entre sí. Por lo tanto, los dos conjuntos de derechos se aplican conjuntamente. Tal relación puede proporcionarse mediante una asociación lógica que usa identificadores o una asociación criptográfica (por ejemplo, cifrando un derecho del primer conjunto con una clave que está almacenada en un derecho del segundo conjunto de derechos). Como alternativa, los derechos atribuidos al usuario se introducen modificando los derechos DRM recibidos. Esto proporciona dos maneras diferentes en las que un usuario puede establecer las restricciones adicionales, impuestas en los derechos recibidos. Por ejemplo, los derechos pueden cambiarse en el proceso de recepción; por ejemplo, los derechos DRM de distribución se convierten en derechos DRM AD. Otra posibilidad está en el proceso de obtener derechos AD a partir de derechos X-AD. En ambos casos, el sistema AD-DRM se asegurará de que los derechos incluyan restricciones adicionales especificadas por el usuario, donde dichos derechos se obtienen transformando derechos en el proceso de recepción (por ejemplo, de derechos DRM de distribución o derechos X-AD a derechos DRM AD). En caso de que el sistema DRM de distribución sea también un sistema AD-DRM, el usuario podrá añadir restricciones como derechos adicionales, los cuales se asociarán a los derechos originales de diversas formas, como se describe posteriormente.

Si el sistema de gestión de derechos digitales de dominio autorizado (AD-DRM) soporta derechos complejos o avanzados, a un usuario le resultará difícil especificar restricciones adicionales en un derecho específico de dominio autorizado (AD) recibido en el sistema AD-DRM. Maneras típicas de dejar que un usuario especifique restricciones adicionales en un derecho específico AD pueden ser dejar que el usuario escriba un programa de derechos que restringa el derecho específico AD o dejar que el usuario asigne un programa de derechos predefinido, donde un programa de derechos de este tipo se ejecuta en el contexto del sistema AD-DRM a través de una máquina virtual incorporada. Sin embargo, la primera posibilidad es compleja y engorrosa para el usuario, y la segunda posibilidad no es flexible.

La invención comprende además la etapa de acceder a una plantilla de programa de derechos (RPT) que comprende datos asociados, y donde la etapa de introducir derechos atribuidos al usuario en un derecho DRM recibido se lleva a cabo usando la plantilla de programa de derechos (RPT). La plantilla de programa de derechos (RPT) puede ofrecer un equilibrio entre complejidad y flexibilidad para el usuario. Por ejemplo, una RPT puede descargarse a través de Internet, puede transferirse mediante *Bluetooth* o IR o puede residir en un dispositivo del sistema de gestión de derechos digitales (DRM).

La etapa de usar la plantilla de programa de derechos (RPT) para introducir restricciones adicionales en un derecho DRM recibido en el procedimiento según la invención se lleva a cabo preferentemente ajustando los datos asociados

a la plantilla de programa de derechos (RPT). De este modo, puede ofrecerse a un usuario una manera sencilla de introducir restricciones adicionales en los derechos relacionados con el acceso a contenido importado en el sistema de gestión de derechos digitales (DRM). La plantilla de programa de derechos puede presentar al usuario los datos asociados y ofrecerle la posibilidad de ajustarlos.

Además, la plantilla de programa de derechos (RPT) puede comprender datos asociados que contienen datos fijos y datos de plantilla, de los cuales el usuario solo puede ajustar los datos de plantilla. Esto contribuye a que la plantilla de programa de derechos (RPT) resulte sencilla para el usuario. Normalmente, los datos fijos no pueden cambiarse, mientras que los datos de plantilla pueden ajustarse o fijarse por el usuario. Las plantillas pueden crearse por proveedores de contenido, por usuarios del sistema de gestión de derechos digitales (DRM) o por otros medios.

La invención se refiere además a un sistema de gestión de derechos digitales (DRM) con características correspondientes al procedimiento descrito anteriormente y que, por tanto, presenta ventajas similares.

Como se ha indicado anteriormente, el término "dominio autorizado" incluye un entorno de dispositivos, medios, derechos y usuarios, donde los usuarios y dispositivos pueden gestionar contenido según los derechos y, normalmente, el término define un entorno, tal como un hogar o una empresa, dentro del cual el contenido puede usarse con relativa libertad, pero que limita el traspaso de contenido más allá de sus límites. El término "medios" abarca cualquier elemento en el que pueda almacenarse información/contenido digital. Los dispositivos pueden disponer de medios de almacenamiento incorporados, por ejemplo una unidad de disco duro, o pueden utilizar medios extraíbles, tales como discos ópticos. El término "derecho" expresa lo que puede hacerse con el contenido, y el término "contenido" abarca un elemento, tal como una composición musical, una película, un programa informático, etc. El término "usuario" abarca una persona que puede hacer funcionar dispositivos, y el término "dispositivo" abarca un equipo o un componente de hardware con capacidades de procesamiento y/o almacenamiento y con capacidad de llevar a cabo operaciones con la información/el contenido digital. Además, un "sistema AD-DRM" es un sistema DRM con un concepto de agrupación añadido al mismo para dispositivos y/o usuarios. La arquitectura puede ser más o menos la misma que un sistema DRM, pero con soporte para el concepto AD añadido.

Como se ha mencionado, el término "derechos DRM" abarca "derechos DRM recibidos", "derechos DRM de distribución" y "derechos atribuidos al usuario", donde los "derechos DRM de distribución" denotan derechos DRM creados por o distribuidos por un proveedor de contenido o de servicios o un distribuidor. Puesto que un dominio autorizado es un caso especial de un sistema DRM, el término "derechos DRM" también abarca derechos AD y derechos X-AD, y los derechos X-AD ofrecidos por un proveedor de servicios o de contenido o un distribuidor son un caso especial de derechos DRM recibidos. Finalmente, debe observarse que aunque los términos "derechos DRM", "derechos AD" y "derechos DRM" están en plural, esto se debe solamente a razones gramaticales; por tanto, estos términos no están limitados necesariamente a una pluralidad de derechos.

Además, los términos relacionados con una etapa llevada a cabo "en un sistema AD-DRM" y "en un sistema DRM", respectivamente, indican que la etapa se lleva a cabo en un dispositivo que implementa o soporta un sistema AD-DRM y un sistema DRM, respectivamente, o que la etapa es parte de un proceso o procedimiento que forma parte de un sistema AD-DRM y un sistema DRM, respectivamente. Finalmente, la expresión "recibir derechos DRM" abarca cualquier manera en que los derechos DRM pueden recibirse, importarse u obtenerse a partir de un sistema de derechos DRM.

A continuación se explicará la invención en mayor detalle en relación con una realización preferente y con referencia a los dibujos, en los que:

la Fig. 1 es un diagrama de flujo del procedimiento de la invención;

la Fig. 2 es una representación esquemática de un sistema híbrido de gestión de derechos digitales de dominio autorizado (AD-DRM) basado en personas y dispositivos;

la Fig. 3 es una representación esquemática de un ejemplo de transcodificación de derechos; y

las Fig. 4a y 4b muestran representaciones esquemáticas de plantillas de programas de derechos (RPT).

La Fig. 1 es un diagrama de flujo del procedimiento de la invención. El procedimiento se lleva a cabo en un sistema DRM. El diagrama comienza en 10 y avanza hasta la etapa 20, donde se reciben derechos DRM en el sistema DRM. Los derechos DRM pueden haberse creado, por ejemplo, por un proveedor de contenido, proveedores de servicio o un distribuidor para proteger su contenido y mantener el control de su distribución. Antes, durante, con o tras la recepción de los derechos DRM, un usuario puede introducir derechos atribuidos al usuario en forma de restricciones adicionales en los derechos DRM del sistema DRM, etapa 30. Un ejemplo de introducción de los derechos atribuidos al usuario antes de la recepción de los derechos DRM puede realizarse por medio de un servicio de Internet que introduce los derechos atribuidos al usuario antes de descargar el contenido digital a un dispositivo

que soporta o implementa el sistema DRM a través de Internet. Un ejemplo de introducción de los derechos atribuidos al usuario con o tras la recepción de los derechos DRM puede realizarse cuando el usuario introduce los derechos atribuidos al usuario a través de un dispositivo, que implementa o soporta el sistema DRM, tras la importación de contenido al dispositivo o a una red doméstica de la que el dispositivo forma parte. Por tanto, un usuario puede importar contenido asociado a derechos DRM y, tras acceder y evaluar el contenido, introducir restricciones en el acceso al mismo. El flujo termina en la etapa 40.

La Fig. 2 es una representación esquemática de un sistema híbrido de gestión de derechos digitales de dominio autorizado (AD-DRM) 100 basado en personas y dispositivos, que es un ejemplo de una realización preferente de un sistema AD-DRM que se usa en la invención. La Fig. 2 muestra contenido, dispositivos y personas relacionadas con el mismo sistema AD-DRM. En este sistema AD-DRM híbrido 100 hay contenido (contenido p_1, contenido p_2, contenido p_3, contenido p_z (donde z es igual o mayor que 1)) asociado a una persona específica (persona 1 en la Fig. 2) y las personas (persona 1, persona 2, persona 3, persona y (donde y es igual o mayor que 1)) están asociadas a un identificador de dominio (Id_dominio). Además, puede haber contenido (contenido d_1, contenido d_2, contenido d_3, contenido d_w (donde w es igual o mayor que 1)) asociado a uno o más dispositivos (dispositivo 1 en la Fig. 2) y los dispositivos (dispositivo 1, dispositivo 2, dispositivo 3, dispositivo x (donde x es igual o mayor que 1)) están asociados al mismo identificador de dominio (Id_dominio), de modo que los diferentes dispositivos, personas y contenido están asociados entre sí. En el sistema AD-DRM 100 mostrado en la Fig. 2, el contenido puede estar asociado a personas o directamente a dispositivos. El sistema AD-DRM híbrido mostrado en la Fig. 2 refleja la pertenencia de contenido, de modo que puede determinarse fácilmente la identificación de una persona a la que pertenece el contenido y, por tanto, quién puede manipular el contenido. Como alternativa, el contenido puede asociarse directamente al identificador de dominio.

La agrupación y la asociación de dispositivos, personas y contenido se llevan a cabo mediante certificados, donde los certificados de dispositivos de domino (DDC) asocian dispositivos al dominio, los certificados de usuarios de dominio (DUC) asocian personas al dominio, los certificados de derechos de usuario (URC) asocian contenido a personas/usuarios y los certificados de derechos de dispositivo (DRC) asocian contenido a dispositivos. El DDC enumera los dispositivos que forman parte del dominio y el DUC enumera los usuarios que forman parte del dominio. El DDC y el DUC están asociados entre sí por medio del identificador de dominio (Id_dominio), que está incluido en ambos certificados.

Cuando se solicita acceso al contenido en el sistema AD-DRM mostrado en la Fig. 2, tiene que aprobarse por medio de los certificados que se autoriza el acceso. Esto puede ser el caso, por ejemplo, si el contenido está asociado a una persona que es un miembro del mismo dominio que el dispositivo, si el contenido está asociado a un dispositivo que es un miembro del mismo dominio, o si un usuario que pertenece al dominio está autenticado en el dispositivo, incluso cuando el contenido está asociado a otro usuario del mismo dominio, independientemente del dominio al que pertenece el dispositivo.
Cuestiones relacionadas con dispositivos que entran o salen del sistema AD-DRM y con usuarios que se unen y/o abandonan el dominio autorizado están más allá del alcance de esta descripción, así como cuestiones sobre cómo se identifican personas y/o dispositivos (tal como identificar personas en función de, por ejemplo, datos biométricos, tarjetas inteligentes o dispositivos de identificación).

La opción anterior de un sistema AD-DRM híbrido es meramente ilustrativa. Existen diferentes conceptos y propuestas para implementar dominios autorizados. En los denominados AD basados en dispositivos, el dominio se forma mediante un conjunto específico de dispositivos y contenido. Un gestor de dominio, que puede ser uno o más de los dispositivos, una tarjeta inteligente u otro dispositivo, controla qué dispositivos pueden unirse al dominio. Solamente el conjunto específico de dispositivos del domino puede usar el contenido de ese dominio, por ejemplo abrirlo, copiarlo, reproducirlo o exportarlo. Ejemplos de tales AD basados en dispositivos se describen en la solicitud de patente internacional WO 03/098931 (n.º de expediente PHNL020455) y en la solicitud de patente internacional WO 04/027588 (n.º de expediente PHNL030283) del mismo solicitante.

Otro tipo de AD es el denominado dominio autorizado basado en personas, donde el dominio está basado en personas en lugar de en dispositivos. Un ejemplo de un sistema de este tipo se describe en la solicitud de patente internacional WO 04/038568 (n.º de expediente PHNL021063) del mismo solicitante, donde el contenido está asociado a personas, las cuales se agrupan después en un dominio.

Un sistema DRM basado en dominio autorizado híbrido asocia contenido a un grupo que puede contener dispositivos y personas. En tal sistema híbrido, el contenido puede visualizarse en cualquier dispositivo que pertenezca al grupo. Además, el contenido puede visualizarse en cualquier dispositivo por cualquier persona que pertenezca al grupo después de que se haya autenticado en ese dispositivo. Tal autenticación implica normalmente un dispositivo de autenticación de usuario, tal como una tarjeta inteligente. Ejemplos de sistemas AD híbridos pueden encontrarse en la solicitud de patente internacional con n.º de serie PCT/IB2004/051226 (n.º de expediente PHNL030926) y en la solicitud de patente europea con n.º de serie 04101256.8 (n.º de expediente PHNL040315).

La Fig. 3 es una representación esquemática de un ejemplo de transcodificación de derechos. La parte situada a la izquierda de la línea discontinua vertical representa un sistema de gestión de derechos digitales (DRM) de distribución que puede proporcionar derechos DRM de distribución a un sistema de gestión de derechos digitales de dominio autorizado (AD-DRM). Los derechos DRM de distribución están relacionados con contenido y representan los permisos del proveedor de servicios, por ejemplo, el número de veces que puede reproducirse el contenido, si el contenido puede copiarse, etc. Tras la recepción de los derechos DRM de distribución en el sistema AD-DRM, los derechos DRM de distribución se convierten en un derecho específico de dominio autorizado (AD) que se refiere al dominio autorizado específico, es decir, las personas y dispositivos del dominio autorizado. En el ejemplo mostrado en la Fig. 3, los derechos específicos de dominio autorizado (AD) abarcan derechos de dominio autorizado cruzado (X-AD) y derechos de dominio autorizado (AD), donde el derecho DRM, tras su recepción en el sistema AD-DRM, se convierte en un derecho X-AD que se usa para controlar el intercambio de contenido y derechos entre diferentes dominios autorizados y el acceso al contenido en otros dominios autorizados (es decir, en dominios diferentes al dominio autorizado al que pertenece el derecho/contenido). Los derechos AD se obtienen a partir de derechos X-AD en un dominio autorizado. Los derechos AD se usarán solamente en el dominio autorizado. Por tanto, un derecho X-AD puede exportarse desde un dominio autorizado (AD1) a otro dominio autorizado (AD2) usando el mismo tipo, o un tipo análogo, de sistema AD-DRM, y a partir del derecho X-AD recibido en el dominio autorizado AD2 pueden obtenerse derechos AD relacionados con el acceso al contenido en el AD2.

La invención ofrece la posibilidad de que un usuario pueda restringir los derechos X-AD, los derechos AD o ambos. Tales restricciones pueden referirse a:

- permisos acerca de qué dispositivo puede acceder al contenido
- permisos acerca de qué personas pueden acceder al contenido
- permisos acerca de cómo una persona puede usar el contenido (por ejemplo, un cierto número de reproducciones)
- permisos acerca del momento de uso, por ejemplo "no después de las 10 horas" (en relación con una persona)
- valores de clasificación parental
- permisos acerca de quién puede exportar contenido a otros dominios autorizados.

Cuando los derechos AD se han obtenido a partir de un derecho X-AD que asocia contenido a uno o más dispositivos o personas, los derechos que especifican el uno o más dispositivos o personas, qué/quién puede acceder al contenido, se obtienen a partir del derecho X-AD de manera que su efecto en lo que respecta al uso de/acceso al contenido en el dominio autorizado se mantiene.

Cuando el contenido se exporta desde un dominio autorizado a otro, un derecho X-AD relacionado con el mismo puede restringirse adicionalmente por un usuario por medio de la invención. De esta manera, el usuario añade restricciones adicionales a los derechos DRM de distribución definidos por el proveedor de servicios.

Para más información acerca de los derechos X-AD, se hace referencia a la solicitud de patente internacional WO 03/098931 (n.º de expediente PHNL020455).

Normalmente, el usuario que define los derechos atribuidos al usuario en forma de restricciones adicionales relacionadas con el acceso al contenido en un dominio autorizado es el usuario que compró el contenido o, como alternativa, una persona que pertenece al dominio autorizado y que actúa como el administrador del dominio autorizado.

A continuación se ofrecen dos ejemplos, donde el primer ejemplo muestra la obtención de un derecho X-AD a partir de un derecho DRM de distribución, donde se añaden restricciones adicionales, y el segundo ejemplo muestra una restricción de un derecho AD en relación con las personas y dispositivos que tienen acceso a contenido relacionado con el derecho AD.

Ejemplo 1

Derecho DRM de distribución = {IDContenido, Reproducir = CopiarUnaVez = {Personas = {Todas}, Dispositivos = {D_1, D_2, D_3}}} → Derecho X-AD = {IDContenido, Reproducir = {Personas = {Todas}, Dispositivos = {D_1, D_2, D_3}}, CopiarUnaVez = {Personas = {P_1}, Dispositivos = {D_1, D_2, D_3}}, Mover = {Personas = {P_1}}},

La flecha "→" denota "se convierte en" y D_i y P_j denotan un dispositivo específico y una persona específica, respectivamente.

El ejemplo muestra la obtención de un derecho X-AD a partir de un derecho DRM de distribución (es decir, la conversión de un derecho DRM de distribución en un derecho X-AD), con la introducción simultánea de derechos atribuidos al usuario. El derecho DRM de distribución permite que contenido con identificación de contenido "IDContenido" pueda reproducirse y copiarse una vez por todas las personas y en cualquiera de los dispositivos D_1, D_2 o D_3. Un usuario ha añadido restricciones (antes, después o durante la obtención de un derecho X-AD), por lo que el contenido con identificación de contenido "IDContenido" solo puede copiarse o sacarse del dominio por la persona P_1. El formato de los derechos puede contener campos adicionales; sin embargo, no se muestran en aras de la brevedad.

Ejemplo 2

Derecho X-AD = {IDContenido, Reproducir = {Personas = {Todas}, Dispositivos = {D_1, D_2, D_3}}, CopiarUnaVez = {Personas = {P_1}, Dispositivos = {D_1, D_2, D_3}}, Mover = {Personas = {P_1}}} → DerechoAD = {IDContenido, Reproducir = {Personas = {P_1, P_2}, Dispositivos = {D_1, D_2}}}.

El ejemplo muestra la obtención de un derecho AD a partir de un derecho X-AD, con la introducción simultánea de derechos atribuidos al usuario. En este ejemplo, el usuario restringe el conjunto de personas que pueden reproducir el contenido a solamente las personas P_1 y P_2, así como el conjunto de dispositivos a D_1 y D_2 a través de los cuales puede accederse al contenido. Los derechos "CopiarUnaVez" y "Mover" no son relevantes en un derecho AD ya que no son relevantes para el uso de contenido en el dominio autorizado. Por lo tanto, se omiten en el derecho AD en este ejemplo.

Aunque los ejemplos anteriores y la Fig. 3 se refieren a derechos DRM de distribución, debe entenderse que cualquier ejemplo equivalente recibido puede describirse en relación con cualquier derecho DRM, tal como un derecho AD o un derecho X-AD.

Las Fig. 4a y 4b muestran representaciones esquemáticas de plantillas de programas de derechos (RPT) que pueden usarse para implementar la introducción de restricciones adicionales en derechos según la invención.

Es de suponer que las expresiones de derechos en la parte de gestión de derechos del sistema AD DRM están en forma de aplicaciones de derechos ejecutables, y que tales aplicaciones de derechos ejecutables también se usan en el sistema DRM que proporciona derechos al sistema AD DRM. En este ejemplo de una realización de la invención, los derechos son plantillas de programas de derechos (RPT) que tienen datos asociados y código asociado, véase la Fig. 4a. Tales RPT pueden ejecutarse en el contexto del sistema AD-DRM a través de una máquina virtual integrada. El código contiene un programa que exporta procedimientos, por ejemplo un procedimiento "validarAcceso()" que indica si puede accederse al contenido. Los datos contienen datos usados por el programa, por ejemplo cadenas de caracteres, constantes, etc.

En una plantilla de programa de derechos (RPT) proporcionada por un proveedor de contenido, el segmento de código de la RPT puede verificar en su procedimiento "validarAcceso()" que solo pueda accederse al contenido entre dos fechas específicas. Estas fechas pueden estar incluidas en el segmento de datos de la RPT.

Según la invención, el segmento de datos de la RPT contiene datos fijos así como datos de plantilla, donde un usuario solo puede ajustar los datos de plantilla. El segmento de código de la RPT es fijo.

La siguiente Tabla 1 ilustra cómo puede usarse en la práctica el principio de los datos de plantilla. Los datos fijos no se muestran en la tabla. Un usuario puede fijar los elementos de la columna "datos de plantilla" (las variables) a cualquier valor válido de la variable.

Tabla 1

Nombre de plantilla	Descripción	Seudocódigo	Datos de plantilla
Control parental	Personas que superan un cierto límite de edad <límite_edad> pueden acceder al contenido	Permitir acceso si obtenerEdad(obtenerPersonaAutorizada()) ≥ <límite_edad>	<límite_edad>

Compartición en comunidad	Personas que pertenecen a una comunidad <id_comunidad> pueden acceder al contenido	Permitir el acceso si <id_comunidad> es miembro de obtenerComunidades(obtenerPersonaAutorizada())	<id_comunidad>
ACl	Determinadas acciones se permiten a determinada	Permitir acción si <acción> en <lista_acciones> y <permisos_acción [obtenerPersonaAutorizada()] es verdadero	<acción><lista_acciones><permisos_acción>
Plantillas de combinación	Puede accederse al contenido si se cumplen otros ciertos derechos (por ejemplo, personas por encima de un límite de edad y que pertenecen a una comunidad pueden acceder al contenido)	Permitir si cada invocación de <instancias_perfil[x]> es verdadera	<instancias_perfil[x]>, por ejemplo intancias_perfil[0] = "control_parental_mayorQue16", instancias_perfil[1] = "comunidad_comparte_clubDe*Bridge*"

La Tabla 1 ilustra cómo puede usarse en la práctica el principio de los datos de plantilla en la RPT. La columna "Seudocódigo" de la Tabla 1 ilustra el seudocódigo de una RPT ejecutada para una operación de acceso al contenido. Se concibe que una representación del derecho AD o del derecho X-AD puede estar disponible al usuario para indicar los permisos/restricciones fijados por la RPT, normalmente, pero sin limitarse necesariamente a, los derechos atribuidos al usuario introducidos. Las variables de los datos de plantilla pueden influir en los permisos/restricciones fijados por la RPT y, por lo tanto, se propone una representación textual del derecho AD o del derecho X-AD, donde la representación textual también está basada en las variables de la columna "datos de plantilla". Por ejemplo, para el control parental, tal representación textual podría ser (seudocódigo):

```
ObtenerTextoIndicacionesDerechos(acción)
    { switch(acción)
            case "acceso"
                return "Acceso permitido si el usuario es mayor que" + <límite_edad>
            case "…"
              …
            }.
```

Debe observarse que la plantilla de programa de derechos (RPT) puede descargarse en aquellos dispositivos del sistema AD-DRM, que comprendan una interfaz de usuario, desde proveedores de servicios, proveedores de contenido u otras entidades. Como alternativa, la RPT puede ser una plantilla por defecto en un dispositivo o estar escrita posiblemente por un usuario.

Un usuario puede decidir asignar una RPT disponible a contenido del que tiene ciertos derechos. La RPT puede mostrarse al usuario de manera similar a la columna "Descripción" de la Tabla 1 o mediante "ObtenerTextoIndicacionesDerechos()" de la RPT. Esto puede llevarse a cabo en la interfaz de usuario de un dispositivo en el sistema AD-DRM o en una página web de un proveedor de servicios o de contenido que ofrece la RPT.

El usuario puede ajustar valores de los parámetros fijados en la RPT. Evidentemente, los posibles valores de las variables deben estar predefinidos (por ejemplo, ser un número natural, un usuario, un nombre de usuario, un dispositivo, una acción). La definición previa de los posibles valores puede estar incluida en los datos fijos de la RPT. Los cambios realizados por el usuario al elegir valores en la RPT pueden mostrarse al mismo, de manera que pueda ajustar la RPT hasta que quede satisfecho. Finalmente, el usuario debe asociar al contenido los derechos proporcionados por la RPT.

A continuación se describen diferentes maneras de asociar derechos DRM de distribución y derechos X-AD obtenidos tras la recepción de los derechos DRM de distribución en un dominio autorizado.

Los derechos DRM de distribución proporcionados por un proveedor de servicios/proveedor de contenido/distribuidor están normalmente protegidos de tal manera que la integridad y el origen de los derechos pueda verificarse, por ejemplo los derechos se firman con una firma que impide alteraciones no autorizadas. Una firma de este tipo también impide normalmente que los derechos se modifiquen y, por tanto, impide que los derechos atribuidos al usuario se incorporen en los derechos DRM de distribución. Cuando los derechos DRM de distribución se transforman en derechos X-AD, estos derechos X-AD pueden convertirse al formato apropiado y, de nuevo, la integridad y el origen de los derechos X-AD resultantes debe protegerse. Esto puede realizarse dejando que el dispositivo de recepción firme los derechos X-AD resultantes. Además, en este caso, los derechos no pueden modificarse más adelante para tener en cuenta derechos atribuidos al usuario.

Las siguientes opciones están disponibles cuando un usuario desea introducir derechos atribuidos al usuario en derechos DRM de distribución o derechos X-AD existentes. Los derechos atribuidos al usuario pueden simplemente coexistir con los derechos atribuidos al proveedor de servicios o de contenido, es decir, los derechos DRM de distribución o los derechos X-AD. Los derechos atribuidos al usuario también deben protegerse; esto puede realizarse normalmente haciendo que los derechos atribuidos al usuario sean firmados por el usuario que define los derechos o por el dispositivo que se usa para llevar a cabo esta operación (suponiendo que el dispositivo sea compatible y solo permita que un usuario asociado al contenido especifique un derecho atribuido al usuario).

Sin embargo, la presencia de dos tipos de derechos (es decir, derechos DRM de distribución y derechos atribuidos al usuario) que coexisten tal y como se ha propuesto anteriormente no se considera una buena práctica en lo que concierne a la seguridad. Es necesario que haya una asociación entre los dos tipos de derechos, como se define en las reivindicaciones, de manera que uno de los derechos no pueda eliminarse fácilmente para engañar al sistema. Posibles maneras de llevar a cabo la asociación son:

- Cuando un proveedor de servicios o de contenido o un distribuidor genera un derecho DRM de distribución, también incluye los derechos atribuidos al usuario que el usuario le ha indicado que añada. Sin embargo, no es un escenario muy habitual, ya que el usuario no podría cambiar nada después. Sin embargo, daría como resultado un objeto de derechos DRM con una firma.

- Durante la recepción de un derecho DRM de distribución, los derechos X-AD se crean mediante un dispositivo AD compatible que puede juntar los derechos atribuidos al usuario y los derechos DRM de distribución creados por el proveedor de servicios o de contenido o por el distribuidor y crear un objeto de derechos DRM con una firma.

- Durante la recepción de un derecho DRM de distribución, los derechos X-AD obtenidos a partir de los derechos DRM de distribución pueden modificarse de tal manera que se garantice que los derechos X-AD solo estén más restringidos e implementen de manera eficaz los derechos atribuidos al usuario.

- Los derechos DRM de distribución creados por el proveedor de contenido o de servicios o por el distribuidor o una derivación de los mismos, es decir, los derechos X-AD, pueden incluirse en los derechos atribuidos al usuario como un todo, formando un objeto de derechos que relaciona los dos tipos de derechos entre sí. El usuario o el dispositivo pueden firmar el objeto resultante.

- Los derechos X-AD que contienen una derivación de los derechos DRM de distribución se cifran con una clave que está almacenada en los derechos atribuidos al usuario; por lo tanto, puede crearse una asociación criptográfica entre los derechos X-AD y los derechos atribuidos al usuario, lo que implica que durante un acceso al contenido, relacionado con los derechos, se requiera acceso a los derechos atribuidos al usuario así como a los derechos X-AD obtenidos.

Aunque se ha descrito cómo se usa la RPT en relación con derechos recibidos desde un sistema DRM, también puede concebirse que la RPT pueda usarse en relación con contenido generado o creado por un usuario. Por tanto, ningún derecho DRM está relacionado intrínsecamente con el contenido, pero el usuario puede aplicar la RPT para imponer una gestión de derechos del contenido cada vez que el contenido se exporte o se comunique.

Como se ha descrito anteriormente, en una realización los derechos atribuidos al usuario restringen adicionalmente el ejercicio de los derechos DRM recibidos a determinadas personas. Para ello, puede introducirse en el sistema DRM información que indica que solamente ciertas personas de un dominio autorizado pueden usar el contenido, preferentemente añadiéndolas en un derecho DRM existente. Después, estas personas tienen que autenticarse con una tarjeta inteligente antes de que puedan usar el contenido. Sin embargo, el determinadas situaciones, usar una tarjeta inteligente puede ser algo engorroso. Por otro lado, este tipo de control de acceso es deseable, por ejemplo, para proteger a los niños de películas violentas.

Para ello, en lugar de indicar solamente las personas durante la adición de, por ejemplo, atributos de privacidad, es posible asociar datos que identifican a personas, tales como datos biométricos o un código PIN, con el contenido. El tipo de datos que identifican a personas puede elegirse dependiendo del nivel de seguridad requerido. Esto tiene la ventaja de que los atributos de privacidad pueden asociarse y usarse de manera más sencilla.

Una alternativa es que un objeto diferente contenga datos de identificación de usuario . Puede hacerse referencia a este objeto con los atributos de privacidad.

Tomando el segundo ejemplo anterior como punto de partida, la opción sencilla mencionada anteriormente puede implementarse añadiendo a los derechos AD un campo tal como id_Persona_Requerido = <plantillla_biométrica>. El elemento <plantillla_biométrica> representa datos biométricos o información que puede verificarse usando una medición biométrica.

Por ejemplo, en la solicitud de patente internacional WO 04/104899 (n.º de expediente PHNL030552) y las solicitudes de patente europeas con n.º de serie 04102609.7 (n.º de expediente PHNL040676) y 04104386.0 (n.º de expediente PHNL040985) se divulga un proceso de inscripción y autenticación usando datos biométricos. En este proceso, una medición biométrica X de referencia se toma de la persona en cuestión. La medición X se transforma en un secreto S. Se calculan datos de Helper W de manera que una medición biométrica Y posterior pueda transformarse de manera fiable en este secreto S. Aplicar esta técnica a la presente invención significa que los valores W y S pueden almacenarse como la plantilla biométrica. preferentemente se almacena una versión de S, sometida de manera criptográfica a una función *hash*, en lugar del propio S.

Debe observarse que las realizaciones mencionadas anteriormente ilustran, en lugar de limitar, la invención, y que los expertos en la técnica pueden diseñar muchas realizaciones alternativas sin apartarse del alcance de las reivindicaciones adjuntas.

En las reivindicaciones, no debe considerarse que un signo de referencia colocado entre paréntesis limita la reivindicación. La expresión "que comprende" no excluye la presencia de elementos o etapas diferentes a los enumerados en una realización. El artículo "un" o "una" delante de un elemento no excluye la presencia de una pluralidad de tales elementos. La invención puede implementarse mediante hardware que comprende varios elementos diferentes, y mediante un ordenador programado de manera adecuada.

En la reivindicación de sistema que enumera varios medios, varios de estos medios pueden realizase por el mismo elemento de hardware. El mero hecho de que ciertas medidas se enumeren en reivindicaciones dependientes diferentes entre sí no indica que una combinación de estas medidas no pueda usarse de manera ventajosa.

REIVINDICACIONES

1. Un procedimiento de procesamiento de derechos DRM (gestión de derechos digitales) en un sistema de gestión de derechos digitales (DRM), donde se han creado derechos DRM para controlar el acceso a contenido, que comprende la etapa de recibir los derechos DRM en el sistema DRM, caracterizado porque el procedimiento comprende además la etapa de permitir que un usuario del sistema DRM introduzca derechos atribuidos al usuario en forma de restricciones adicionales en los derechos DRM recibidos en el sistema DRM, en el que

- los derechos atribuidos al usuario constituyen un segundo conjunto de derechos y los derechos DRM recibidos constituyen un primer conjunto de derechos, donde los dos conjuntos de derechos se asocian entre sí cifrando un derecho del primer conjunto con una clave que está almacenada en un derecho del segundo conjunto de derechos.

2. Un procedimiento según la reivindicación 1, caracterizado porque el sistema DRM que recibe los derechos DRM es un sistema AD-DRM, y porque comprende además la etapa de

- en el sistema AD-DRM, obtener derechos específicos de dominio autorizado (AD) a partir de los derechos DRM recibidos.

3. Un procedimiento según la reivindicación 2, caracterizado porque el usuario puede introducir los derechos atribuidos al usuario en los derechos DRM con o tras la recepción de los derechos DRM.

4. Un procedimiento según la reivindicación 2 o 3, caracterizado porque los derechos específicos de dominio autorizado (AD) son derechos de dominio autorizado cruzado (X-AD) que están dispuestos para controlar la transferencia de derechos entre dominios autorizados (AD) y el acceso al contenido en otros dominios autorizados.

5. Un procedimiento según la reivindicación 2 o 3, caracterizado porque los derechos específicos de dominio autorizado (AD) son derechos de dominio autorizado (AD) que se han obtenido a partir de los derechos de dominio autorizado cruzado (X-AD), donde los derechos de dominio autorizado (AD) se establecen para controlar el acceso al contenido en un dominio autorizado (AD).

6. Un procedimiento según la reivindicación 2 o 3, caracterizado porque los derechos específicos de dominio autorizado (AD) son derechos de dominio autorizado (AD) que se han obtenido a partir de los derechos de dominio autorizado cruzado (X-AD), donde los derechos de dominio autorizado (AD) se establecen para controlar el acceso al contenido en un dominio autorizado (AD) y donde un usuario ya ha introducido derechos atribuidos al usuario en los derechos de dominio autorizado cruzado (X-AD).

7. Un procedimiento según cualquiera de las reivindicaciones 1 a 6, caracterizado porque el procedimiento comprende además la etapa de acceder a una plantilla de programa de derechos (RPT) que comprende datos asociados, y donde la etapa de introducir los derechos atribuidos al usuario en un derecho DRM recibido se lleva a cabo usando la plantilla de programa de derechos (RPT).

8. Un procedimiento según la reivindicación 7, caracterizado porque la etapa de usar la plantilla de programa de derechos (RPT) para introducir los derechos atribuidos al usuario en un derecho DRM recibido se lleva a cabo ajustando los datos asociados a la plantilla de programa de derechos (RPT).

9. Un procedimiento según la reivindicación 1, caracterizado porque los derechos atribuidos al usuario restringen adicionalmente el ejercicio de los derechos DRM recibidos a determinadas personas.

10. Un procedimiento según la reivindicación 9, caracterizado porque los derechos atribuidos al usuario contienen datos que identifican a personas, tales como datos biométricos, para indicar las determinadas personas.

11. Un sistema de gestión de derechos digitales (DRM) dispuesto para recibir derechos DRM para controlar el acceso a contenido, caracterizado porque comprende medios para permitir que un usuario del sistema DRM introduzca derechos atribuidos al usuario en forma de restricciones adicionales en derechos DRM recibidos en el sistema DRM, en el que

- los derechos atribuidos al usuario constituyen un segundo conjunto de derechos y los derechos DRM recibidos constituyen un primer conjunto de derechos, donde los dos conjuntos de derechos se asocian entre sí cifrando un derecho del primer conjunto con una clave que está almacenada en un derecho del segundo conjunto de derechos.

12. Un sistema DRM según la reivindicación 11, caracterizado porque el sistema DRM dispuesto para recibir derechos DRM es un sistema AD-DRM, y comprende además

- en el sistema AD-DRM, medios para obtener un derecho específico de dominio autorizado (AD) a partir de los derechos DRM recibidos.

13. Un sistema DRM según la reivindicación 12, caracterizado porque los derechos específicos de dominio autorizado (AD) son derechos de dominio autorizado cruzado (X-AD) que están dispuestos para controlar la transferencia de derechos entre dominios autorizados (AD) y el acceso al contenido en otros dominios autorizados.

14. Un sistema DRM según la reivindicación 12, caracterizado porque los derechos específicos de dominio autorizado (AD) son derechos de dominio autorizado (AD) que se han obtenido a partir de los derechos de dominio autorizado cruzado (X-AD), donde los derechos de dominio autorizado (AD) se establecen para controlar el acceso al contenido en un dominio autorizado (AD).

15. Un sistema DRM según la reivindicación 12, caracterizado porque los derechos específicos de dominio autorizado (AD) son derechos de dominio autorizado (AD) que se han obtenido a partir de los derechos de dominio autorizado cruzado (X-AD), donde los derechos de dominio autorizado (AD) se establecen para controlar el acceso al contenido en un dominio autorizado (AD) y donde un usuario ya ha introducido derechos atribuidos al usuario en los derechos de dominio autorizado cruzado (X-AD).

16. Un sistema DRM según cualquiera de las reivindicaciones 11 a 15, caracterizado porque comprende además una plantilla de programa de derechos (RPT) que comprende datos asociados, y los derechos atribuidos al usuario pueden introducirse en un derecho DRM recibido usando la plantilla de programa de derechos (RPT).

17. Un sistema DRM según la reivindicación 16, caracterizado porque el sistema DRM comprende medios para ajustar los datos asociados a la plantilla de programa de derechos (RPT) para introducir los derechos atribuidos al usuario en un derecho DRM recibido.

18. Un sistema DRM según la reivindicación 11, caracterizado porque los derechos atribuidos al usuario restringen adicionalmente el ejercicio de los derechos DRM recibidos a determinadas personas.

19. Un sistema DRM según la reivindicación 18, caracterizado porque los derechos atribuidos al usuario contienen datos que identifican a personas, tales como datos biométricos, para indicar las determinadas personas.

20. Un medio legible por ordenador que tiene instrucciones almacenadas en el mismo para hacer que una unidad de procesamiento ejecute el procedimiento según una cualquiera de las reivindicaciones 1 a 10.

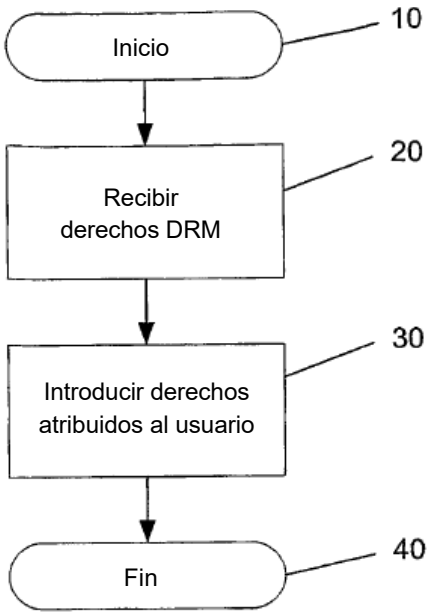
Inicio
10
Recibir
derechos DRM
20
Introducir derechos
atribuidos al usuario
30
Fin
40

Fig. 1

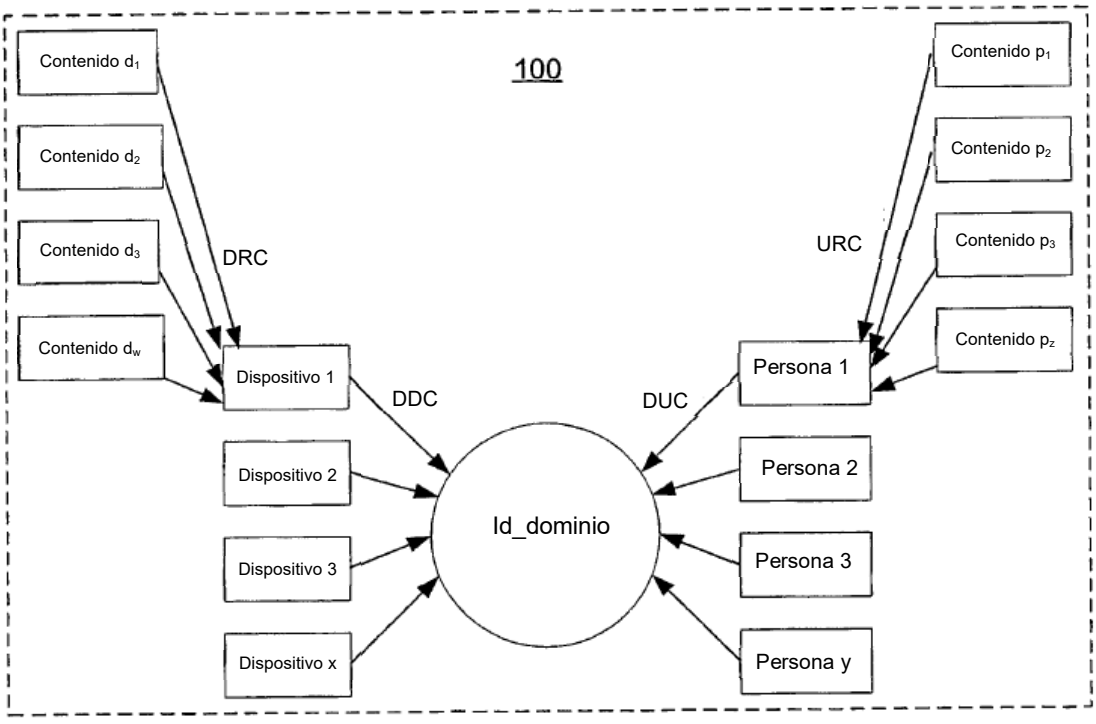
100
Contenido d_1
Contenido d_2
Contenido d_3
Contenido d_w
DRC
Dispositivo 1
Dispositivo 2
Dispositivo 3
Dispositivo x
DDC
Id_dominio
DUC
URC
Contenido p_1
Contenido p_2
Contenido p_3
Contenido p_z
Persona 1
Persona 2
Persona 3
Persona y

Fig. 2

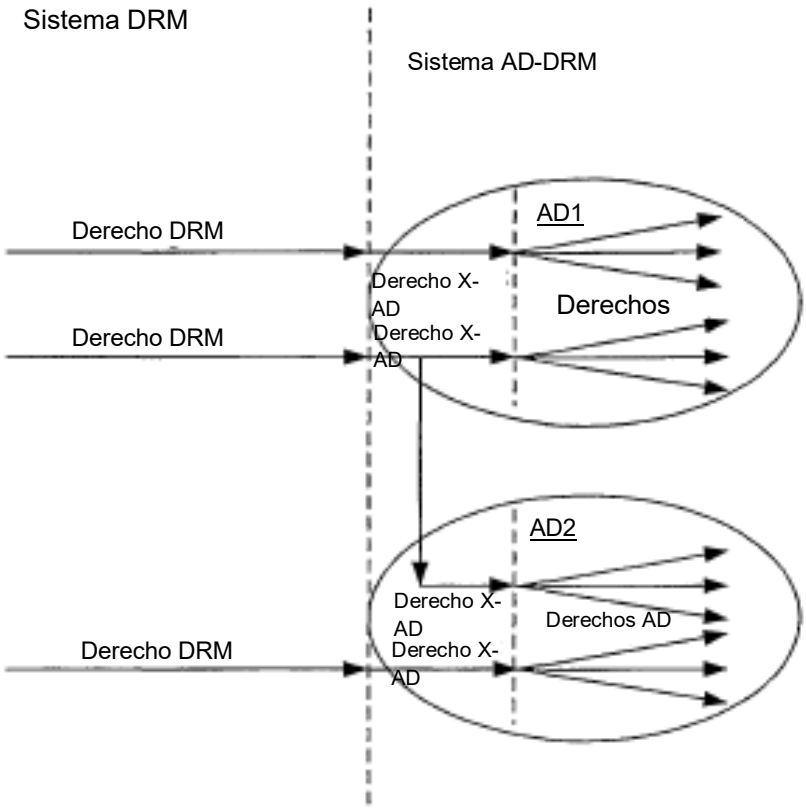

Fig. 3

Fig. 4a

Fig. 4b