(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 292 635**

(51) Int. Cl.:
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01990507 .4**
(86) Fecha de presentación : **29.11.2001**
(87) Número de publicación de la solicitud: **1405148**
(87) Fecha de publicación de la solicitud: **07.04.2004**

(54) Título: **Superdistribución segura de datos de usuario.**

(30) Prioridad: **18.12.2000 EP 00204637**

(45) Fecha de publicación de la mención BOPI:
16.03.2008

(45) Fecha de la publicación del folleto de la patente:
16.03.2008

(73) Titular/es: **Koninklijke Philips Electronics N.V.**
Groenewoudseweg 1
5621 BA Eindhoven, NL

(72) Inventor/es: **Staring, Antonius, A., M. y**
Kamperman, Franciscus, L., A., J.

(74) Agente: **Zuazo Araluze, Alexander**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Superdistribución segura de datos de usuario.

La invención se refiere a un método para la superdistribución segura de datos de usuario almacenados en un primer soporte de datos. La invención se refiere además a un sistema para la superdistribución segura de datos de usuario, a un aparato para la reproducción y/o la grabación de datos de usuario y a un soporte de datos para almacenar datos de usuario.

La superdistribución es un planteamiento para la distribución de software en el que el software se pone a disposición de manera libre y sin restricción pero está protegido frente a modificaciones y modos de utilización no autorizados por su distribuidor. La arquitectura de superdistribución, que se conoce por ejemplo por R. Mori y M. Kawahara, "Super distribution - The Concept and the Architecture", The Transaction Of The IEICE, Vol. E 73, nº 7, páginas 1133-1146, julio de 1990 (se encuentra en http://www.virtualschool.edu/mon/electronicproperty/morisuperdist.html), proporciona tres funciones principales: acuerdos administrativos para recopilar información contable sobre la utilización de software y tarifas por la utilización de software; un proceso de contabilidad que registra y acumula cargos por la utilización, pagos y asignación de cargos por la utilización entre diferentes distribuidores de software; y un mecanismo de defensa, que utiliza módulos protegidos digitalmente, que protege el sistema frente a interferencias con su funcionamiento adecuado.

El software de superdistribución se distribuye a través de canales públicos de forma cifrada. Presenta la siguiente combinación de propiedades deseables:

- Los productos de software se distribuyen libremente sin restricción. El usuario de un producto de software paga por la utilización de ese producto, no por su posesión.

- El distribuidor de un producto de software puede establecer los términos y condiciones de su utilización en la lista de tarifas, si la hay, para su utilización.

- Los productos de software pueden ejecutarse por cualquier usuario que tenga el equipo adecuado, siempre que el usuario se adhiera a las condiciones de utilización establecidas por el distribuidor y pague las tarifas aplicadas por el distribuidor

- el funcionamiento adecuado del sistema de superdistribución, incluyendo la aplicación de las condiciones establecidas por los distribuidores, se garantiza mediante dispositivos electrónicos a prueba de manipulación indebida, por ejemplo tarjetas inteligentes.

La superdistribución no sólo puede usarse para la distribución de software, sino también en general para la distribución de datos de usuario como datos de audio y vídeo. La superdistribución de contenido de audio y vídeo puede ser un modelo de negocio atractivo para compañías discográficas y cinematográficas. La razón es que en un modelo de este tipo, los consumidores asumen parte del papel del distribuidor al copiar los datos, por ejemplo sus álbumes favoritos para sus amigos. Por consiguiente, y por ejemplo en función del éxito del álbum, el coste de fabricación y distribución de medios físicos puede reducirse enormemente. Evidentemente, un modelo de negocio que se base en la superdistribución sólo es viable si el uso de copias se paga de manera adecuada, lo que requiere la aplicación mediante un sistema de protección de contenidos fiable. Un sistema de este tipo estará basado en un mecanismo de control de reproducción que emplee tecnologías de cifrado y, lo más probable, de marcas de agua.

El documento EP 0 704 785 A2 da a conocer un sistema de gestión de derechos de autor de datos que comprende una base de datos para almacenar datos originales, un centro de control de claves para gestionar claves de cifrado, un centro de gestión de derechos de autor para gestionar derechos de autor de datos y una red de comunicación para conectar estas secciones entre sí. Los datos suministrados desde la base de datos a los usuarios se cifran y distribuyen, y los usuarios descifran los datos cifrados mediante claves de cifrado obtenidas del centro de control de claves o del centro de gestión de derechos de autor para el uso de los datos. Se prevén dos métodos para suministrar datos a los usuarios, en particular un suministro unidireccional de datos cifrados a los usuarios mediante radiodifusión o similar, y un suministro bidireccional de datos a los usuarios en correspondencia con las peticiones de los usuarios.

El documento US 5.646.992 da a conocer métodos para la recopilación, distribución y utilización de información digital. Se visualizan representaciones gráficas organizadas jerárquicamente de elementos y grupos de elementos de información digital que están disponibles para pedidos de usuarios. El usuario explora de manera interactiva las representaciones y selecciona elementos o grupos para el pedido, utilizando un puntero. Mientras están visualizándose las representaciones gráficas, también se visualiza una lista de elementos o grupos que se han seleccionado para su inclusión en un pedido. Se ejecuta un software que automáticamente determina la configuración del ordenador, y compara la configuración con la información de configuración almacenada antes de que el usuario haga el pedido. Un usuario puede obtener automáticamente acceso a los elementos en una revisión posterior del medio si el usuario tenía acceso a los elementos en una revisión anterior.

Un objeto de la presente invención es proporcionar un método para la superdistribución segura de datos de usuario que también permita la realización de diferentes modelos de negocio.

Este objetivo se consigue mediante un método según la reivindicación 1, que comprende las etapas de

a) copiar dichos datos de usuario desde dicho primer soporte de datos a un segundo soporte de datos;

b) almacenar en dicho segundo soporte de datos información requerida por un centro de servicios para conceder derechos de acceso a dicha copia de dichos datos de usuario; y

c) obtener derechos de acceso a dicha copia de dichos datos de usuario transmitiendo al menos dicha información almacenada a dicho centro de servicios, completar una transacción y recibir información de acceso adicional, en el que dicho centro de servicios utiliza dicha información almacenada para conceder derechos de acceso a dicha copia de dichos datos de usuario para dicho segundo soporte de datos;

en el que dichos soportes de datos primero y segundo comprenden cada uno un identificador de soporte único, y dicha información almacenada consiste en al menos un valor de código determinado a partir de al menos dichos identificadores de soporte únicos de dicho primer y segundo soporte de datos.

La presente invención se basa en la idea de:

a) control de copia: copiar el contenido superdistribuido (que todavía no es accesible ya que todavía no se ha completado una transacción con un centro de servicios) a otra ubicación distinta del segundo soporte de datos es inútil porque no se concederá el acceso por un centro de servicios para la otra ubicación; y

b) control de acceso: una vez completada una transacción con un centro de servicios, sólo puede accederse a la copia de superdistribuida en el segundo soporte de datos con sujeción a un sistema de Gestión de Derechos Digital (DRM).

Otra razón para introducir un concepto como la denominada superdistribución *unicast* es que proporciona medios para hacer los originales más atractivos que las copias, incluso aunque no haya diferencia aparente, y por tanto favorece el mercado al por menor. Por ejemplo, en el caso de superdistribución *unicast* hay un enlace directo entre el propietario del soporte de datos original y el propietario del segundo soporte de datos, a quien va dirigida la copia superdistribuida. Por tanto, la superdistribución *unicast* explota (in)directamente las relaciones sociales existentes entre personas, e incluso puede fortalecer tales relaciones favoreciendo la formación de comunidades. Además, la superdistribución *unicast* puede proporcionar seguridad adicional, porque no es muy útil publicar datos de usuario (cifrados) en Internet para la descarga general, ya que un centro de servicios no concederá acceso a una copia de los datos de usuario que se haya obtenido de este modo.

La decisión de conceder o denegar el acceso a tal copia depende totalmente del centro de servicios; técnicamente no hay motivo para que el centro de servicios no pueda conceder el acceso, por ejemplo debido a información insuficiente. Finalmente, al hacer que sólo puedan seleccionarse originales para la superdistribución, que es una manera de hacer los originales más atractivos que las copias superdistribuidas, por ejemplo porque hay un sistema de premios asociado a la superdistribución, por ejemplo mediante ganancias de “puntos” de audio, se espera que la tasa de crecimiento del número de copias superdistribuidas sea igual a la tasa de crecimiento del número de originales vendidos (suponiendo que para cada original vendido se realizará aproximadamente una copia superdistribuida). De nuevo, esta es una característica que favorece el mercado al por menor.

La información requerida por el centro de servicios para conceder derechos de acceso a la copia de los datos de usuario puede ser cualquier información que pueda usarse por el centro de servicios para identificar los datos de usuario. Por ejemplo, la información puede consistir en cualquiera de las siguientes o en una combinación de las mismas:

- un identificador único de los datos de usuario, por ejemplo el número ISRC de una pista de música;
- un identificador único de un conjunto de datos de usuario; por ejemplo un título de álbum;
- una clave de descifrado de los datos de usuario, cifrada en la clave pública del centro de servicios;
- un identificador único del soporte de datos original;
- un identificador único del soporte de datos de destino;
- un identificador del propietario original de los datos de usuario;
- valores de código derivados de cualquiera de los identificadores anteriores.

Para favorecer la realización de un modelo de negocio que se base en la superdistribución segura, una realización preferida de la presente invención se basa en la idea de emplear un identificador de soporte único en un primer soporte de datos, es decir, un ID de disco único en un disco (ROM) pregrabado. A partir de este identificador de soporte único se determina un valor de código, preferible mediante un reproductor del primer soporte de datos, que se almacena por

un grabador en el segundo soporte de datos junto con el identificador de soporte único del primer soporte de datos. Para habilitar el segundo soporte de datos, es decir, la copia del primer soporte de datos, el valor de código y el identificador de soporte único deben transmitirse a un centro de servicios, por ejemplo al propietario del contenido de los datos de usuario almacenados en el primer soporte de datos, en el que se descodifican y/o verifican estos datos y, en caso de un resultado positivo, los derechos y la información requerida se transmiten de vuelta al grabador o reproductor del segundo soporte de datos para habilitarlo.

En realizaciones preferidas de la invención se utilizan identificadores adicionales para aumentar la funcionalidad del método propuesto de superdistribución, por ejemplo de quién a quién se hace la copia. En particular puede utilizarse un identificador de superdistribución que puede estar almacenado en el primer soporte de datos y puede utilizarse para determinar el valor de código y verificar el valor de código en el centro de servicios.

En una realización adicional de la invención se utilizan una o más claves, que pueden ser parte de una jerarquía de claves, para cifrar los datos de usuario que están almacenados de forma cifrada en el primer soporte de datos. Estas claves tienen que proporcionarse desde el centro de servicios para habilitar el segundo soporte de datos. Tales claves pueden derivarse por ejemplo de una marca de disco física, por ejemplo una desviación en un soporte de grabación óptica.

En un aspecto adicional de la invención se utiliza una clave de reproductor de superdistribución y una clave de grabador de superdistribución para cifrar el valor de código antes de almacenarlo en el segundo soporte de datos. El centro de servicios realiza entonces el descifrado una vez transmitido el valor de código cifrado al centro de servicios para habilitar el segundo soporte de datos.

Adicionalmente, en otro aspecto más de la invención, se utiliza un identificador de reproductor y un identificador de grabador que también se almacenan en el segundo soporte de datos y se transmiten al centro de servicios para descifrar la clave del reproductor de superdistribución y la clave del grabador para habilitar el segundo soporte de datos.

Alternativamente, el descifrado del valor de código cifrado dos veces también puede realizarse por un fabricante del reproductor y/o grabador utilizando identificadores de reproductor y/o grabador. Por tanto los fabricantes de dispositivos están implicados en el proceso de habilitar el segundo soporte de datos, y puede garantizarse que sólo se utilizan dispositivos compatibles lo que también aumenta la seguridad del método de superdistribución propuesto.

En una realización preferida de la invención se propone que el propietario del primer soporte de datos obtenga beneficios del centro de servicios en respuesta a una superdistribución segura de los datos de usuario almacenados en el primer soporte de datos. Tal obtención de beneficios es parte de un modelo de negocio en el que se estimulará la copia y la distribución segura de los datos de usuario. Los beneficios pueden ser premiar a la fuente original del contenido superdistribuido con “puntos de música” si alguien compra el acceso a este contenido. Otros ejemplos son el acceso libre a un “código de acceso personal” tal como se describe en la solicitud de patente europea 00 201 663.2 para desbloquear una pista adicional en el soporte de datos original o puntos de bonificación para una rebaja en una compra futura. También es posible controlar que tales beneficios sólo se obtienen si se ha hecho una copia directa de un soporte de datos original. Este mecanismo garantiza que siga siendo atractiva la compra de soportes de datos originales, lo que proporciona un mecanismo de protección frente al copiado de contenido con acceso controlado.

En una realización preferida adicional, un valor de código de adjudicación generado a partir de al menos el identificador de soporte único del primer soporte de datos se transmite al centro de servicios para recoger los beneficios adjudicados. El centro de servicios puede por tanto determinar si hay beneficios y cuántos deberán adjudicarse al propietario del primer soporte de datos.

Según la invención como soportes de datos se utilizan preferiblemente soportes de grabación óptica, en particular CD o DVD regrabables y/o reescribibles. Sin embargo, también es posible utilizar cualquier otra clase de medios de almacenamiento como soportes de datos en el sentido de la invención. Preferiblemente el método según la invención se usa para la superdistribución de datos de software, vídeo y/o audio almacenados en dichos soportes de datos.

En una realización de la invención, el segundo soporte de datos también comprende un identificador de soporte único que se utiliza para determinar el valor de código y que también se transmite al centro de servicios para habilitar el segundo soporte de datos. Dicho identificador de soporte único del segundo soporte de datos se utiliza preferiblemente si el destino de los datos de usuario es importante.

La invención se refiere además a un sistema para la superdistribución segura de datos de usuario que comprende un reproductor y un grabador, medios de transmisión y un centro de servicios según se reivindica en la reivindicación 12. Además, la invención se refiere a un aparato para la reproducción y/o la grabación de datos de usuario para su uso en un sistema de este tipo y a un soporte de datos para almacenar datos de usuario y datos de superdistribución para su uso en un método de superdistribución segura según la invención. Debe entenderse que tal sistema, aparato y soporte de datos según la invención pueden desarrollarse adicionalmente y pueden tener realizaciones adicionales que son idénticas o similares a las realizaciones descritas anteriormente y que se exponen en las reivindicaciones dependientes de la reivindicación 1.

Desde un punto de vista de alto nivel, el método y el sistema según la invención funcionan como sigue. Un disco pregrabado contiene contenido que está cifrado con una clave de producto que puede estar almacenada en un depósito de clave, tal como se describe en la solicitud de patente europea 00 202 888.4. Sin embargo, también puede usarse una clave que se derive a partir de una marca de disco física, por ejemplo una desviación de un soporte de grabación óptica. Esta clave puede formar parte de un jerarquía de claves y como tal no se utiliza para cifrar directamente el propio contenido, sino más bien un conjunto intermedio de claves. Para un funcionamiento adecuado del método y el sistema, preferiblemente es necesario que la carga útil de esta marca de disco sea secreta, es decir, que sea accesible sólo por reproductores compatibles. La carga útil es única por cada título del disco, pero no tiene que ser única para cada disco, es decir, las claves y el contenido cifrado en todos los discos pregrabados son idénticas. Esto no debería ser un problema para el propietario del contenido, ya que los discos pregrabados son todos originales de fabricación conocida.

Además de la primera marca de disco física hay una segunda marca de disco, preferiblemente secreta, en el disco (ROM) pregrabado, que es única para cada disco. La carga útil de esta segunda marca puede utilizarse durante todas las fases del proceso de superdistribución para evitar la superdistribución no controlada. La clave para la reproducción, es decir, la clave de producto, se entregará (de manera segura) por el centro de servicios. En la copia se realizan previsiones para asegurar que el contenido sólo pueda reproducirse en ese disco particular, para evitar la distribución no controlada a través de Internet. Con este fin, el disco regrabable o reescribible contiene una marca de disco única que se utiliza para derivar la(s) clave(s) requerida(s) para descifrar el contenido. En cuanto a un disco regrabable o reescribible, esta marca de disco único puede incrustarse previamente en el disco o escribirse por el grabador.

Un aspecto de la invención es asegurar que sólo es posible hacer una copia de la fuente en un receptor. La copia desde una fuente a múltiples receptores, es decir, a través de Internet, también podría permitirse. La ausencia de un identificador de disco único para el receptor haría esto posible. Sin embargo, el sistema de bonificaciones podría funcionar en este caso de manera injusta. Si una persona consigue abrir un sitio web popular desde el que todo el mundo se copiara archivos, conseguiría todos los beneficios de la bonificación. Si por el contrario siempre se necesitara un disco original para hacer una copia, sólo los compradores de discos originales recibirían los premios.

Una vez completada la transacción, el propietario del contenido, es decir, el centro de servicios, proporciona la(s) clave(s) que se utiliza(n) por el grabador para hacer que la copia (y sólo esa copia particular) sea reproducible. En algún momento de la transacción, un propietario de contenido ha podido determinar el identificador de soporte único del disco original. Para proporcionar un incentivo al consumidor para que haga copias superdistribuidas a los amigos, el propietario del contenido puede decidir proporcionar algún tipo de beneficio al propietario del disco original. Por ejemplo, puede facilitarse el acceso libre a un “código de acceso personal” que puede usarse para desbloquear una pista adicional en el disco original; todos los puntos de bonificación pueden acumularse para una rebaja en una compra futura. Si el propietario del contenido así lo desea, la propia copia superdistribuida puede utilizarse para hacer otra copia superdistribuida, ya sea ilimitadamente o hasta un límite predeterminado. En ese caso, un propietario de contenido puede decidir proporcionar los beneficios asociados con el contenido superdistribuido a cualquier participante en la cadena empezando por el disco original (como un sistema piramidal). Evidentemente, la superdistribución segura de contenido habilita una multitud de modelos de comercialización, que pueden escogerse por álbumes, y pueden proporcionar una rica fuente de información de comercialización.

A continuación se explicará más detalladamente la invención con referencia a los siguientes dibujos, en los que:

la figura 1 muestra un diagrama de bloques de un sistema de superdistribución según la invención,

la figura 2 muestra un diagrama de bloques de la jerarquía de claves utilizada en una realización de la invención,

las figuras 3A, 3B muestran la disposición de un disco original y de una copia,

la figura 4 muestra las etapas para copiar según una primera realización de la invención,

la figura 5 muestra las etapas de habilitación según la primera realización,

la figura 6 muestra las etapas de recogida de beneficios según la primera realización,

la figura 7 muestra las etapas de copiado según una segunda realización de la invención,

las figuras 8a, 8b muestran las etapas de habilitación según la segunda realización, y

las figuras 9a, 9b muestran las etapas de recogida de beneficios según la segunda realización.

En el diagrama de bloques de la figura 1 que muestra una realización de un sistema de superdistribución según la invención, se muestra un reproductor 1 para la reproducción de un soporte de datos pregrabado, por ejemplo un disco (ROM) pregrabado que contiene datos de usuario, por ejemplo datos de software, de audio o de vídeo. Un grabador 2 se utiliza para grabar los datos almacenados en el primer soporte de datos reproducidos por el reproductor 1 en un segundo soporte de datos, por ejemplo un disco regrabable o reescribible. Una vez transmitidos los datos de usuario y todos los datos de superdistribución necesarios desde el reproductor 1 al grabador 2, en el que estos datos se han almacenado en

el segundo soporte de datos, este segundo soporte de datos se habilita, es decir, se le proporcionan todos los derechos e información necesarios para el uso previsto del segundo soporte de datos, transmitiendo los datos de superdistribución requeridos al centro 3 de servicios donde se verifican estos datos y se devuelven los datos de habilitación al grabador 2 si la verificación ha sido satisfactoria. Para verificar los datos de superdistribución proporcionados por el grabador 2, el centro 3 de servicios puede transmitir parte de los datos de superdistribución al fabricante 4 del reproductor y/o al fabricante 5 del grabador para su descifrado y/o verificación. Los enlaces entre el reproductor y el centro de servicios y entre el centro de servicios y el fabricante del reproductor/grabador no son esenciales, sino opcionales. El enlace entre el reproductor y el centro de servicios es para la posible recogida de beneficios. Los demás enlaces se utilizan incluir a los fabricantes en la operación si se desea. El sistema y el método de superdistribución se explicarán más detalladamente a continuación.

En la figura 2 se muestra un diagrama de bloques que muestra la jerarquía de claves en una realización preferida de la invención. En primer lugar se utiliza un lector 6 de marca de disco para leer marcas de disco físicas proporcionadas en un disco para obtener un primer conjunto de claves. A partir de estas claves se genera una denominada clave de depósito de claves KL_Key en el bloque 7. Paralelamente, se utiliza un lector 8 de depósito de claves para obtener una versión cifrada de las claves de producto, claves de producto que se utilizan para cifrar los datos de usuario. La función del lector 8 de depósito de claves es leer el contenido del depósito de claves del disco. El propio depósito de claves es un área especial del disco en la que están almacenadas las claves de descifrado (claves de producto) y los derechos de uso del contenido. El contenido del depósito de claves se cifra utilizando la clave de depósito de claves que se deriva según la jerarquía de claves mostrada en la figura.

En el bloque 9, las claves de producto se descifran utilizando la clave de depósito de claves, y las claves de producto se utilizan entonces en el bloque 10 para descifrar el contenido cifrado, es decir, los datos de usuario almacenados en un disco. Debe observarse que la jerarquía de claves mostrada en la figura 2 es sólo un posible sistema que puede subyacer al sistema de la invención. Hay otros posibles diseños que funcionarían igual de bien.

La disposición de un soporte de datos original y una copia, es decir los datos de superdistribución almacenados en un soporte de datos original y una copia, que son ambos discos ópticos, se muestra en las figuras 3A y 3B. El disco original mostrado en la figura 3A comprende los siguientes datos de superdistribución:

- ID de título: un identificador de datos que puede ser algún número para identificar el título del contenido, que no es secreto;

- UDI-RO: un identificador de soporte (disco) único, en particular de un disco ROM, que no es secreto; el UDI-RO está almacenado en el disco original (de sólo lectura) en una marca de disco física, e identifica un disco particular (es decir, actúa como una especie de número de serie). No está pensado para copiarse. En la copia, el equivalente del UDI-RO es el UDI-R, que puede estar o bien escrito previamente en la copia (por ejemplo por un fabricante) o bien puede escribirse por el grabador con sujeción a un número de reglas de robustez y de aleatoriedad. Ha de observarse que el UDI-R puede estar ubicado dentro del depósito de calves.

- EKB: un bloque de claves de habilitación (no secreto) que es un bloque de datos que contienen una clave que está cifrada por varias claves de reproductor;

- PDM: marca(s) de disco física(s). Tales marcas de disco físicas sólo pueden leerse mediante dispositivos compatibles y son preferiblemente secretas. Si se utiliza una EKB, la PDM puede no ser secreta también;

- SD-ID: un identificador de superdistribución que puede ser algún número utilizado para apoyar la funcionalidad de distribución de la superdistribución, que sea secreto y que pueda ubicarse en el depósito de claves;

- AK: una clave de producto que se utiliza para cifrar alguna parte del contenido o datos de usuario (un producto).

En lugar del identificador de soporte UDI-RO, un disco de copia mostrado en la figura 3B comprende un identificador de soporte UDI-R, que es un identificador de disco único no secreto de n disco regrabable y reescribible. Además, una clave de producto AK no está almacenada en primera instancia en un disco de copia. Sin embargo, si la pista/producto se habilita por el centro de servicio, la clave AK se almacenará en el disco. Adicionalmente también, se almacena un identificador de superdistribución SD-ID' diferente en el disco de copia. El SD-ID' podría generarse por el grabador o también podría obtenerse mediante alguna comunicación con el centro de servicio. En el primer caso debe transmitirse al centro de servicio a través de un canal seguro autenticado.

La Figura 4 muestra las etapas para copiar los datos de usuario almacenados en un primer soporte de datos reproducidos mediante un reproductor a un segundo soporte de datos, grabación que se realiza en un grabador. En una primera etapa, el contenido del primer soporte de datos se transfiere al grabador en versión cifrada y se graba en un segundo soporte de datos. En una segunda etapa, el grabador devuelve el identificador de soporte único UDI-R del segundo soporte de datos (disco de destino) de modo que pueda habilitarse la copia superdistribuida solamente en ese disco. En la etapa 3, el reproductor devuelve la información requerida para habilitar la copia superdistribuida. Esta

información comprende un valor de código, por ejemplo una función *hash* o una función F, que incluye el identificador de soporte único UDI-RO del primer soporte de datos para identificar este disco fuente específico, el identificador de soporte único UDI-R del segundo soporte de datos para identificar este disco de destino específico y un identificador de superdistribución SD-ID para asegurar que solamente un reproductor compatible podría haber calculado el valor de código o el resultado de la función *hash*. Solamente un reproductor compatible puede calcular el código ya que solamente un reproductor compatible puede extraer el SD-ID. Adicionalmente, el identificador de soporte único UDI-RO que posteriormente requiere el centro de servicios para verificar el valor de código (el resultado de la función *hash*) y el identificador de datos, ID de título, que requiere el centro de servicios para determinar un identificador de superdistribución SD-ID se transmiten al grabador y se almacenan en el segundo soporte de datos. Opcionalmente, el UDI-R también puede proporcionarse de manera no cifrada en la segunda comunicación desde el reproductor al grabador.

Las etapas para habilitar el segundo soporte de datos se muestran en la figura 5. Primero, el grabador envía la información requerida para habilitar la copia al centro de servicios, información que incluye el valor F de código, el identificador de soporte del original UDI-RO y el identificador de datos, ID de título. El identificador de soporte de la copia UDI-R se añade a esta información para permitir que el centro de servicios verifique el valor de código (el resultado de la función *hash*). Para la transferencia de los datos, se establece un canal seguro autenticado SAC para identificar el grabador de origen así como para un uso posterior. Un canal seguro autenticado SAC es una interfaz que puede utilizarse para transferir datos de manera segura.

En la siguiente etapa, el centro de servicios determina el identificador de superdistribución SD-ID y la clave de producto AK a partir del identificador de datos, ID de título, preferiblemente utilizando una base de datos, y verifica el valor de código (el resultado de la función *hash*). En esta etapa, también se almacena un identificador de soporte del original UDI-RO en el centro de servicios junto con los beneficios adjudicados, si los hubiera.

Finalmente, en la última etapa, el centro de servicios devuelve la clave de producto AK, los derechos comprados por el grabador y otro identificador de superdistribución SD-ID'. Adicionalmente, la transacción también puede contener algún tipo de transferencia de dinero. El canal seguro autenticado SAC garantiza así que solamente un grabador compatible puede recibir esta información.

Las etapas para recoger beneficios en la primera realización se explican adicionalmente con referencia a la figura 6. En una primera etapa el reproductor que reproduce el original envía la información requerida para recoger los beneficios al centro de servicios. Esta información incluye otro valor de código o función *hash* que es distinto del valor de código que se muestra en las figuras 4 y 5. La función *hash* que se utiliza para la recogida de beneficios incluye el identificador de soporte del original UDI-RO para identificar al disco para el que se recogen los beneficios y el identificador de superdistribución del original SD-ID para asegurar que solamente un reproductor compatible podría haber calculado el resultado de la función *hash*. Además, esta información transmitida el centro de servicios incluye el UDI-RO que posteriormente requiere el centro de servicios para verificar el resultado de la función *hash* y el identificador de datos, ID de título, que requiere el centro de servicios para determinar el identificador de superdistribución SD-ID. Se establece otra vez un canal seguro autenticado SAC para identificar al reproductor original así como para su uso en la etapa 3 posterior.

En una segunda etapa, el centro de servicios determina el identificador de superdistribución SD-ID a partir del identificador de datos, ID de título, preferiblemente mediante el uso de una base de datos, y verifica el resultado de la función *hash*. Entonces, se determinan los beneficios a partir del identificador de soporte UDI-RO, preferiblemente de nuevo mediante el uso de una base de datos. En una tercera etapa, los beneficios o un resumen del estado de los beneficios se devuelven al reproductor mediante el uso del canal seguro autenticado SAC que asegura que el reproductor compatible correcto recibe esta información. Los beneficios pueden ir acoplados al disco fuente o al reproductor dependiendo de los requisitos de negocio, no solo al disco.

La realización mostrada en las figuras 4 a 6 y descrita anteriormente utiliza criptografía de claves asimétricas para establecer un canal seguro autenticado (SAC) y solamente permite copiar desde un disco original. Además, los fabricantes del dispositivo no están incluidos en la transacción. Sin embargo, la invención no está limitada a un sistema y a un método que tengan tales características. La invención también puede usarse empleando solamente criptografía de claves simétricas y en el que también se permita copiar desde discos ya copiados. Además, los fabricantes del dispositivo pueden estar implicados en la transacción tal como se mostrará en las figuras 7 a 9 y se describirá en la siguiente realización.

La figura 7 muestra las etapas para un procedimiento de copiado según una segunda realización de la invención. En la etapa 1, el contenido del primer soporte de datos se transfiere al grabador en forma cifrada. En la etapa 2, el grabador devuelve otra vez el identificador de soporte UDI-R del disco de destino de modo que pueda habilitarse la copia superdistribuida solamente en ese disco. En la etapa 3, el reproductor devuelve la información requerida para habilitar la copia superdistribuida, información que incluye la función *hash* (función F) del identificador de soporte UDI-RO para identificar el disco fuente específico, el identificador de soporte UDI-R para identificar el disco de destino específico y el identificador de superdistribución SD-ID para asegurar que solamente un reproductor compatible podría haber calculado el resultado de la función *hash* y que solamente un titular de derechos puede invertir una función *hash* (preferiblemente usando una base de datos). Antes de transmitir la información al grabador, el resultado de la función *hash* se cifra opcionalmente usando una clave de reproductor de superdistribución SDPK, que es única para cada

reproductor, para asegurar que los fabricantes del reproductor y del grabador tienen un papel simétrico en la fase de habilitación del procedimiento. Adicionalmente, el identificador de soporte UDI-RO que posteriormente requiere el centro de servicios para verificar el resultado de la función *hash*, y el identificador de datos, ID de título, que requiere el centro de servicios para determinar el identificador de superdistribución SD-ID, así como un identificador de reproductor, ID de reproductor, que identifica al reproductor de origen, se transmiten al grabador. Opcionalmente, el UDI-R también puede proporcionarse de manera no cifrada en la segunda comunicación desde el reproductor al grabador.

Las etapas de habilitación en esta realización se muestran el la figura 8a. En una primera etapa, el grabador envía la información requerida para habilitar la copia. El identificador de soporte UDI-R se añade a esta información para permitir que el centro de servicios verifique el resultado de la función *hash*. Antes de transmitir el resultado de la función *hash*, se cifra utilizando una clave de grabador de superdistribución SDRK para garantizar que un grabador particular ha enviado la información. Además, se añade un identificador de grabador, ID de grabador, para identificar al grabador de origen. En una segunda etapa, el centro de servicios se pone en contacto con los fabricantes del reproductor y del grabador para el descifrado del resultado de la función *hash* y posteriormente determina un identificador de superdistribución SD-ID y la clave de producto AK a partir del identificador de datos, ID de título, preferiblemente usando una base de datos, y verifica los resultados de la función *hash*. Se almacena el identificador de soporte UDI-RO proporcionado desde el grabador junto con los beneficios adjudicados en el centro de servicios.

En una tercera etapa, el centro de servicios devuelve la clave de producto AK y los derechos comprados por el grabador. Esta información se cifra primero utilizando una clave derivada del identificador de soporte UDI-R para asegurar que el fabricante del grabador no pueda hacer un mal uso de esta información. Entonces, la información cifrada se cifra adicionalmente por el fabricante del grabador para garantizar que solamente el grabador correcto pueda recibir la información. El cifrado asegura que la información devuelta por el centro de servicios solamente pueda usarse para habilitar una copia específica, concretamente la identificada por el UDI-R.

La comunicación entre el centro de servicios y el fabricante del grabador o el fabricante del reproductor para el cifrado se muestra en la figura 8b.

Las etapas para una recogida de beneficios en la segunda realización se muestran en la figura 9a. En la misma, el reproductor envía la información requerida para recoger los beneficios al centro de servicios en la etapa 1. Esta información comprende la función *hash* que incluye el identificador de soporte UDI-RO para identificar el disco para el que se recogen los beneficios y el identificador de superdistribución SD-ID para asegurar que solamente un reproductor compatible podría haber calculado el resultado de la función *hash* y que solamente el titular de los derechos puede invertir la función *hash*. Además, la información transmitida al centro de servicios comprende el identificador de soporte UDI-RO que posteriormente requiere el centro de servicios para verificar el resultado de la función *hash* y el identificador de datos, ID de título, que requiere el centro de servicios para determinar el identificador de superdistribución SD-ID. Antes de la transmisión, el resultado de la función *hash* se cifra con una clave de reproductor de superdistribución para garantizar que un reproductor compatible envía esta información.

En la segunda etapa, el centro de servicios se pone en contacto con el fabricante del reproductor para el descifrado del resultado de la función *hash* y posteriormente determina el identificador de superdistribución SD-ID a partir del identificador de datos, ID de título, preferiblemente mediante el uso de una base de datos, y verifica el resultado de la función *hash*. Adicionalmente, los beneficios se determinan a partir del identificador de soporte UDI-RO, preferiblemente mediante el uso de una base de datos.

En la tercera etapa, los beneficios o un resumen del estado de los beneficios se devuelven al reproductor. Antes de la transmisión, se cifra primero la información usando una clave derivada del identificador de soporte UDI-RO para asegurar que el fabricante del grabador no pueda hacer un mal uso de esta información. El fabricante del grabador realiza un segundo cifrado de esta información para garantizar que solamente el grabador correcto pueda recibir la información.

E{SDRK} y E{SDPK} indican un cifrado simétrico. Por supuesto, también es posible utilizar un cifrado asimétrico o un SAC ya presente. Puesto que la clave de producto AK debería ser secreta, puede protegerse cifrándola mediante UDI-R(O) en la comunicación con el fabricante del grabador. El UDI en un disco no necesita ser secreto. Sin embargo, el cifrado mediante un UDI-R(O) proporciona un nivel de seguridad aumentado ya que el fabricante del grabador no conoce el UDI utilizado durante la superdistribución.

La comunicación entre el centro de servicios y el fabricantes del grabador o el fabricante del reproductor para el cifrado se muestra en la figura 9b.

Según la invención, se proporciona un método y sistema para la superdistribución segura de datos de usuario. Pueden realizarse en los mismos diversos modelos de negocio en los que se distribuye contenido mediante el copiado privado controlado. Las copias se hacen no reproducibles hasta que se haya completado una transacción correcta. Además, se proporcionan nuevas oportunidades de comercialización debido al contacto directo entre el propietario del contenido y el consumidor. Pueden darse incentivos a los consumidores para que copien los datos de usuario. Por ejemplo, las copias pueden ser más baratas que los originales y pueden proporcionarse beneficios al propietario de los originales, como el acceso libre a códigos de acceso para pistas adicionales o rebajas en compras futuras (“puntos de

audio”). Además, un método de superdistribución de este tipo es más conveniente que bajar un álbum completo desde Internet.

Pueden tomarse medidas para mantener el atractivo de los originales, por ejemplo, permitiendo que solamente estén disponibles los originales para la superdistribución, evitando la superdistribución de “fábrica”.

El método y el sistema según la invención pueden usarse para recopilar información de comercialización, por ejemplo, usando los puntos de música. Los dispositivos utilizados para las transacciones pueden o no permanecer anónimos. Además, puede decidirse si el copiado para la superdistribución solamente podría permitirse en línea o también fuera de línea. En resumen, la invención permite el control del copiado que se realiza sobre contenido de acceso controlado.

REIVINDICACIONES

1. Método para la superdistribución segura de datos de usuario almacenados en un primer soporte de datos que comprende las etapas de

a) copiar dichos datos de usuario desde dicho primer soporte de datos a un segundo soporte de datos;

b) almacenar en dicho segundo soporte de datos información requerida por un centro (3) de servicios para conceder derechos de acceso a dicha copia de dichos datos de usuario; y

c) obtener derechos de acceso a dicha copia de dichos datos de usuario transmitiendo al menos dicha información almacenada a dicho centro (3) de servicios, completar una transacción, y recibir información de acceso adicional, utilizando dicho centro de servicios dicha información almacenada para conceder derechos de acceso a dicha copia de dichos datos de usuario para dicho segundo soporte de datos;

caracterizado porque

dichos primer y segundo soportes de datos comprenden cada uno un identificador de soporte único (UDI), y porque dicha información almacenada consiste en al menos un valor (F) de código determinado a partir de al menos dichos identificadores de soporte únicos (UDI) de dicho primer y segundo soporte de datos.

2. Método según la reivindicación 1, **caracterizado** porque el acceso a dichos datos de usuario almacenados en dicho primer soporte de datos está controlado mediante un sistema de acceso condicional o de gestión de derechos digital.

3. Método según la reivindicación 1, **caracterizado** porque dichos identificadores de soporte únicos (UDI) también se transmiten a dicho centro (3) de servicios.

4. Método según la reivindicación 1 ó 3, **caracterizado** porque dicho primer soporte de datos comprende un identificador de superdistribución (SD-ID) que se utiliza para determinar dicho valor (F) de código.

5. Método según la reivindicación 1, **caracterizado** porque dicho valor (F) de código se cifra mediante una clave de reproductor de superdistribución (SDPK) antes de almacenarlo en dicho segundo soporte de datos, y porque dicho valor (F) de código cifrado se cifra adicionalmente mediante una clave de grabador de superdistribución (SDRK) antes de la transmisión a dicho centro de servicios.

6. Método según la reivindicación 5, **caracterizado** porque dicho identificador de reproductor que corresponde a dicha clave de reproductor de superdistribución (SDPK) está almacenado en dicho segundo soporte de datos, y porque dicho identificador de reproductor y un identificador de grabador que corresponde a dicha clave de grabador de superdistribución (SDRK) se transmiten a dicho centro (3) de servicios.

7. Método según la reivindicación 6, **caracterizado** porque el descifrado de dicho valor (F) de código cifrado se lleva a cabo por los fabricantes (4, 5) del reproductor y/o grabador respectivos.

8. Método según la reivindicación 1 ó 2, **caracterizado** porque un valor de código de adjudicación generado desde al menos dicho identificador único de dicho primer soporte de datos se transmite a dicho centro de servicios para recoger los beneficios adjudicados, que dicho centro (3) de servicios adjudica al propietario de dicho primer soporte de datos en respuesta a un procedimiento completado de superdistribución segura de dichos datos de usuario almacenados en dicho primer soporte de datos.

9. Método según la reivindicación 1 ó 2, **caracterizado** porque se utilizan discos ópticos, en particular CD o DVD regrabables y/o reescribibles como soportes de datos.

10. Método según la reivindicación 1 ó 2, **caracterizado** porque dicho datos de usuario son datos de audio, datos de vídeo o software.

11. Método según la reivindicación 1, **caracterizado** porque dicho centro (3) de servicios utiliza dicha información almacenada para conceder derechos de acceso a dicha copia de dichos datos de usuario solamente para dicho segundo soporte de datos.

12. Sistema para la superdistribución segura de datos de usuario almacenados en un primer soporte de datos, que comprende

a) un reproductor (1) y un grabador (2) para copiar dichos datos de usuario desde dicho primer soporte de datos a un segundo soporte de datos, comprendiendo dichos primer y segundo soportes de datos cada uno un identificador de soporte único (UDI) y almacenar datos de superdistribución en dicho segundo soporte de datos;

b) medios de transmisión para transmitir los datos de superdistribución almacenados a un centro (3) de servicios; y

c) un centro (3) de servicios para conceder derechos de acceso a dicha copia de dichos datos de usuario en dicho segundo soporte de datos,

caracterizado porque:

dicho reproductor (1) se proporciona para determinar un valor (F) de código a partir de al menos dichos identificadores de soporte únicos (UDI) de dichos primer y segundo soportes de datos, y dicho grabador (2) se proporciona para almacenar al menos dicho valor (F) de código y dicho identificador único (UDI-RO) de dicho primer soporte de datos en dicho segundo soporte de datos.

13. Aparato para la reproducción y/o grabación de datos de usuario para el uso en un sistema según la reivindicación 12.

14. Soporte de datos para almacenar datos de usuario y datos de superdistribución para el uso en un método para la superdistribución segura según la reivindicación 1, comprendiendo los datos de superdistribución

a) un identificador de soporte único (UDI-RO) que identifica el soporte de datos,

b) un identificador de datos (ID de título) que identifica los datos de usuario almacenados en el soporte de datos,

c) un identificador de superdistribución (SD-ID) que se utiliza para proporcionar la funcionalidad de superdistribución;

d) una o más claves (AK) para cifrar los datos de usuario y/o los datos de superdistribución,

caracterizado porque dichos datos de superdistribución comprenden además:

un valor (F) de código determinado a partir de al menos dicho identificador de soporte único (UDI-RO) de dicho soporte de datos y un identificador de soporte único (UDI-R) de un segundo soporte de datos.

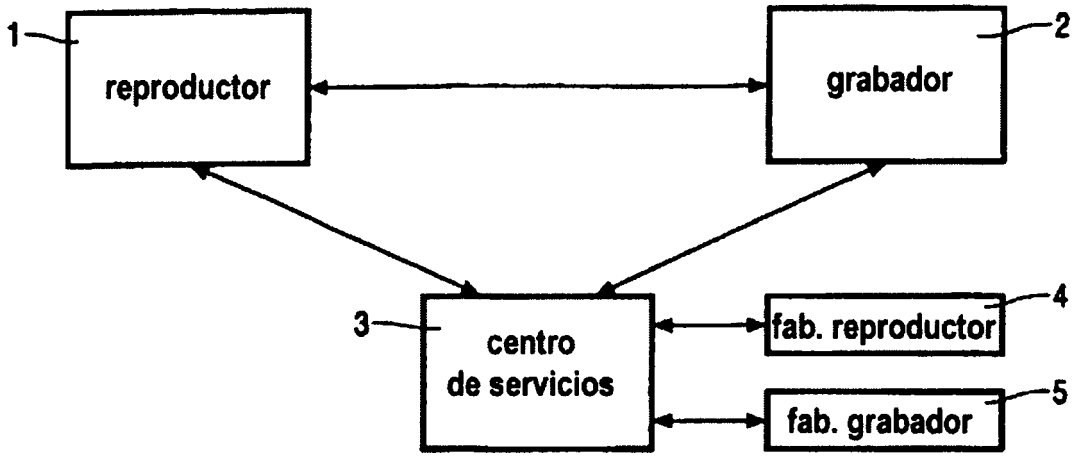
1
reproductor
2
grabador
3
centro
de servicios
4
fab. reproductor
5
fab. grabador

FIG. 1

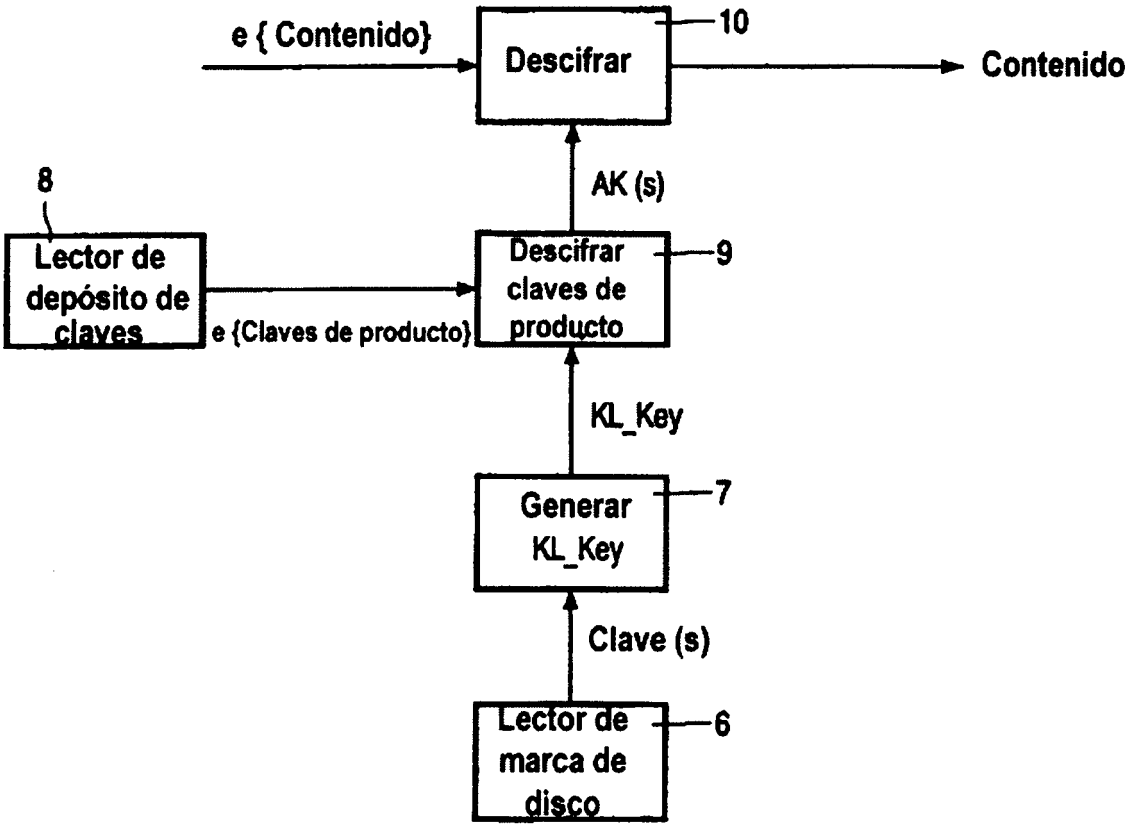
e { Contenido}
Descifrar
10
Contenido
AK (s)
8
Lector de
depósito de
claves
e {Claves de producto}
Descifrar
claves de
producto
9
KL_Key
Generar
KL_Key
7
Clave (s)
Lector de
marca de
disco
6

FIG. 2

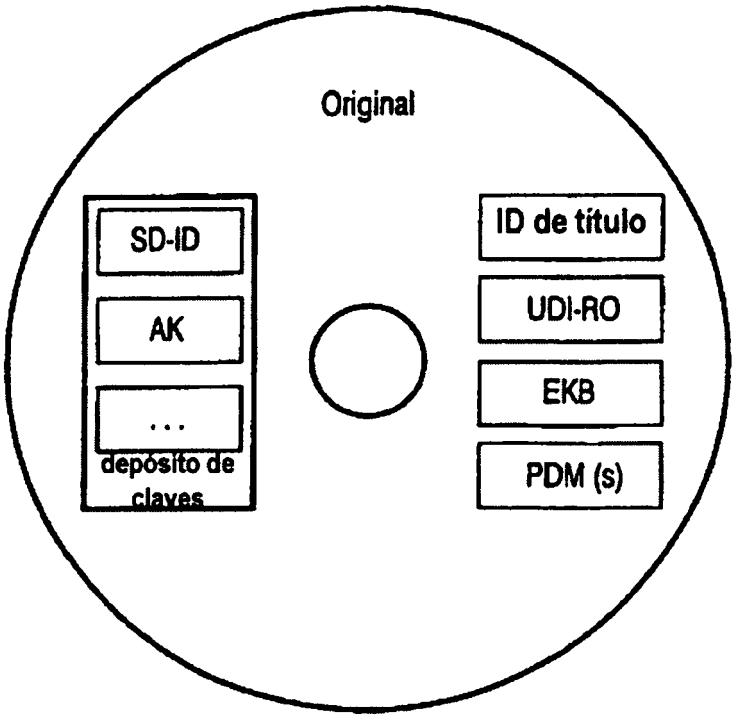
Original
SD-ID
AK
...
depósito de claves
ID de título
UDI-RO
EKB
PDM (s)

FIG. 3A

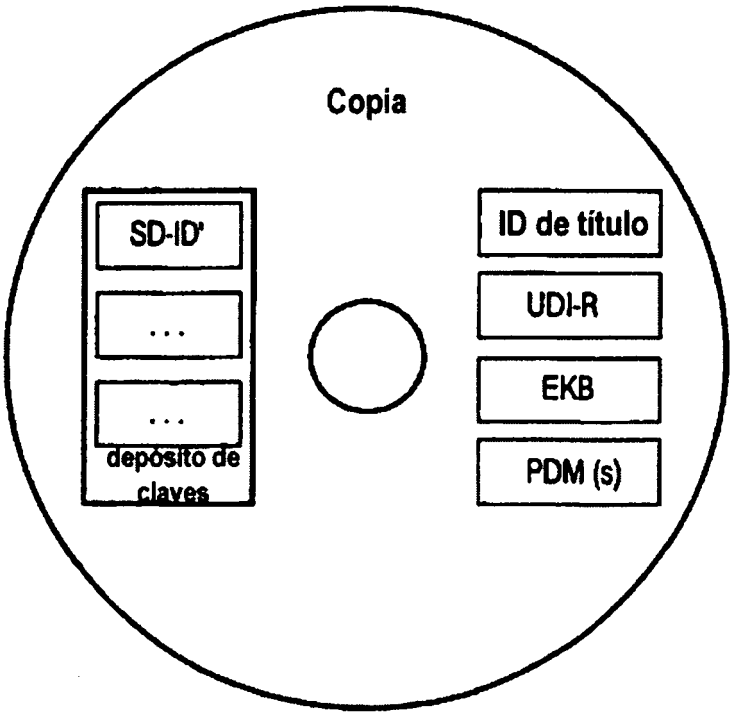
Copia
SD-ID'
...
...
depósito de claves
ID de título
UDI-R
EKB
PDM (s)

FIG. 3B

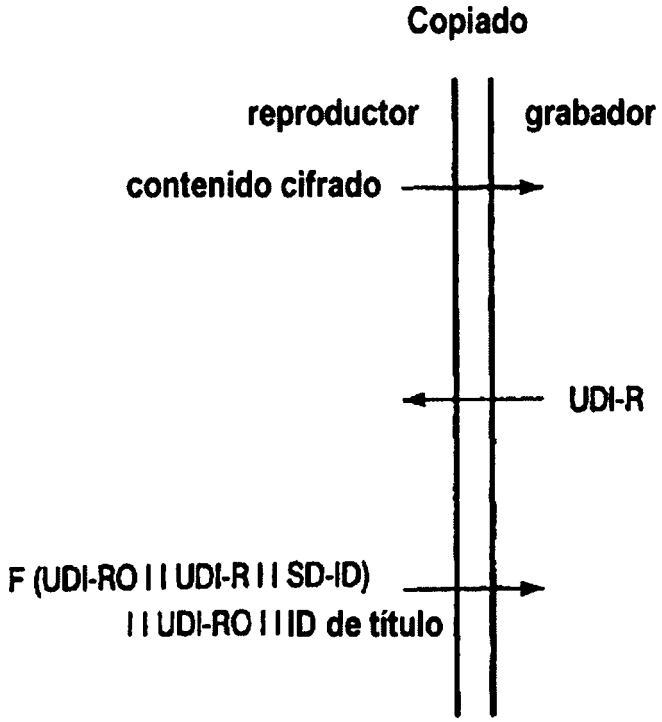
Copiado
reproductor
grabador
contenido cifrado
UDI-R
F (UDI-RO I I UDI-R I I SD-ID)
I I UDI-RO I I ID de título

FIG. 4

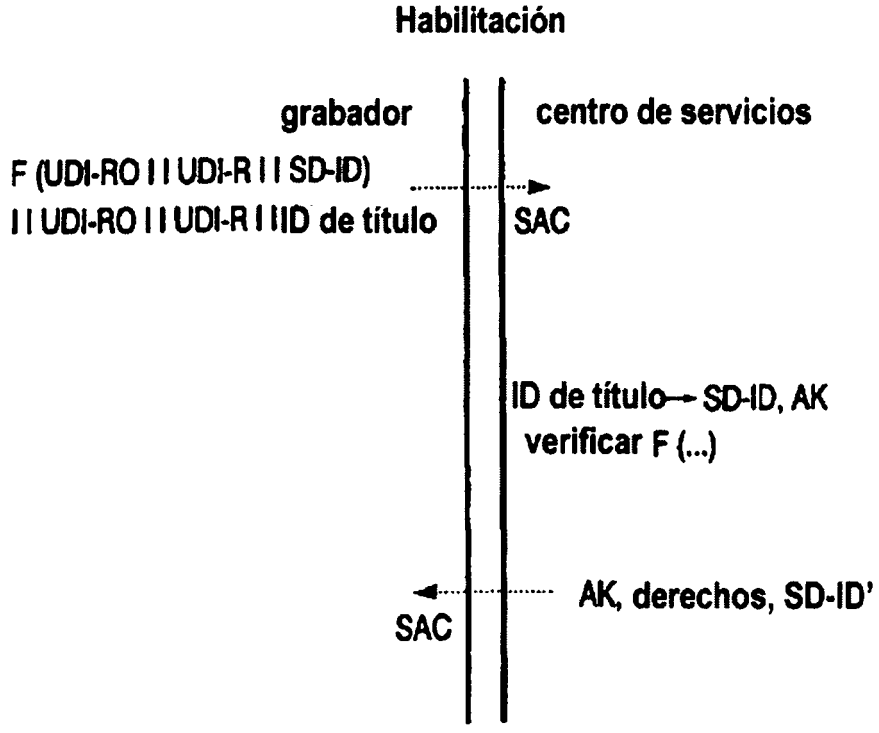
Habilitación
grabador
centro de servicios
F (UDI-RO I I UDI-R I I SD-ID)
I I UDI-RO I I UDI-R I I ID de título
SAC
ID de título→ SD-ID, AK
verificar F (...)
AK, derechos, SD-ID'
SAC

FIG. 5

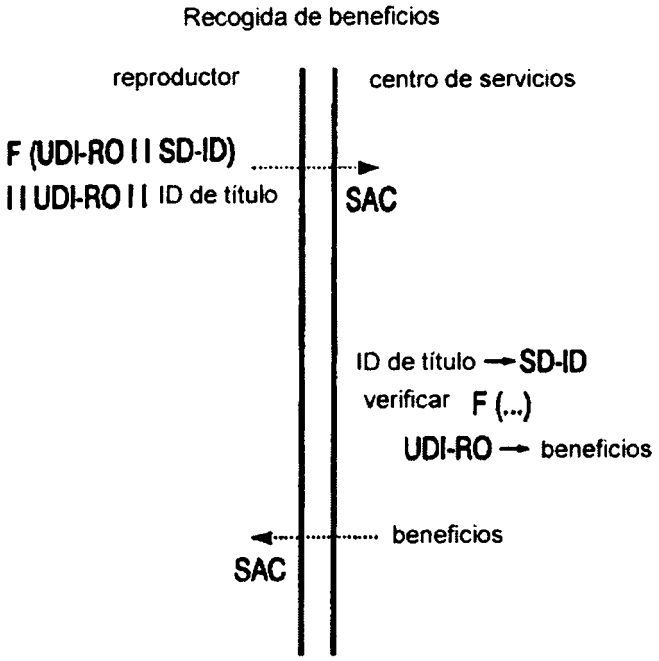
Recogida de beneficios
reproductor
centro de servicios
F (UDI-RO || SD-ID)
|| UDI-RO || ID de título
SAC
ID de título → SD-ID
verificar F (...)
UDI-RO → beneficios
beneficios
SAC

FIG. 6

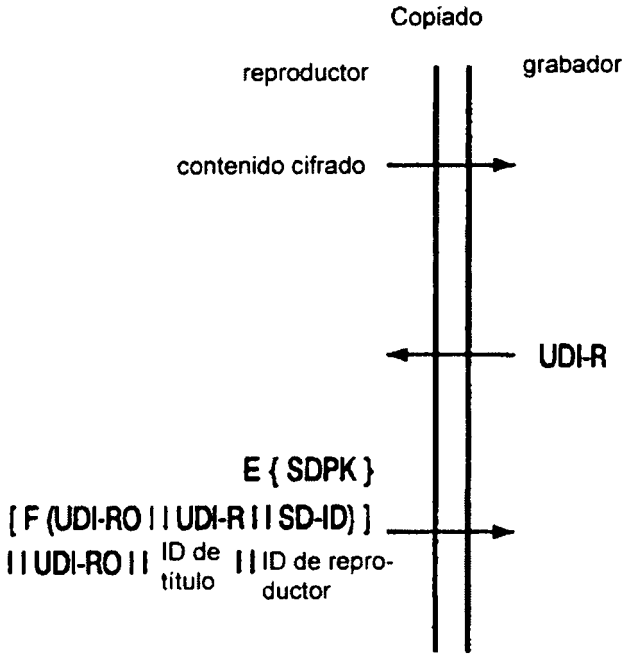
Copiado
reproductor
grabador
contenido cifrado
UDI-R
E { SDPK }
[F (UDI-RO || UDI-R || SD-ID)]
|| UDI-RO || ID de título || ID de reproductor

FIG. 7

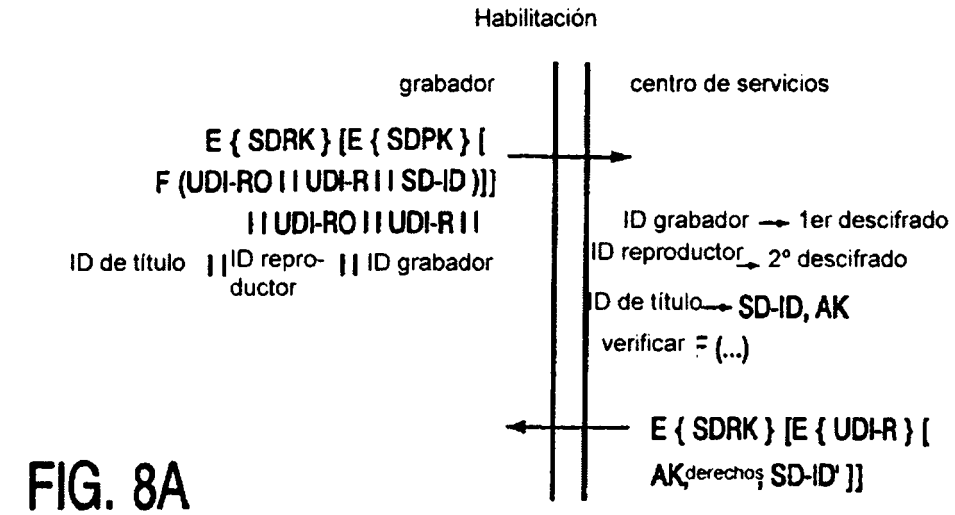
Habilitación
grabador
centro de servicios
E { SDRK } [E { SDPK } [
F (UDI-RO I I UDI-R I I SD-ID)]]
I I UDI-RO I I UDI-R I I
ID de título I I ID repro- ductor I I ID grabador
ID grabador → 1er descifrado
ID reproductor → 2º descifrado
ID de título → SD-ID, AK
verificar F (...)
E { SDRK } [E { UDI-R } [
AK derechos; SD-ID']]

FIG. 8A

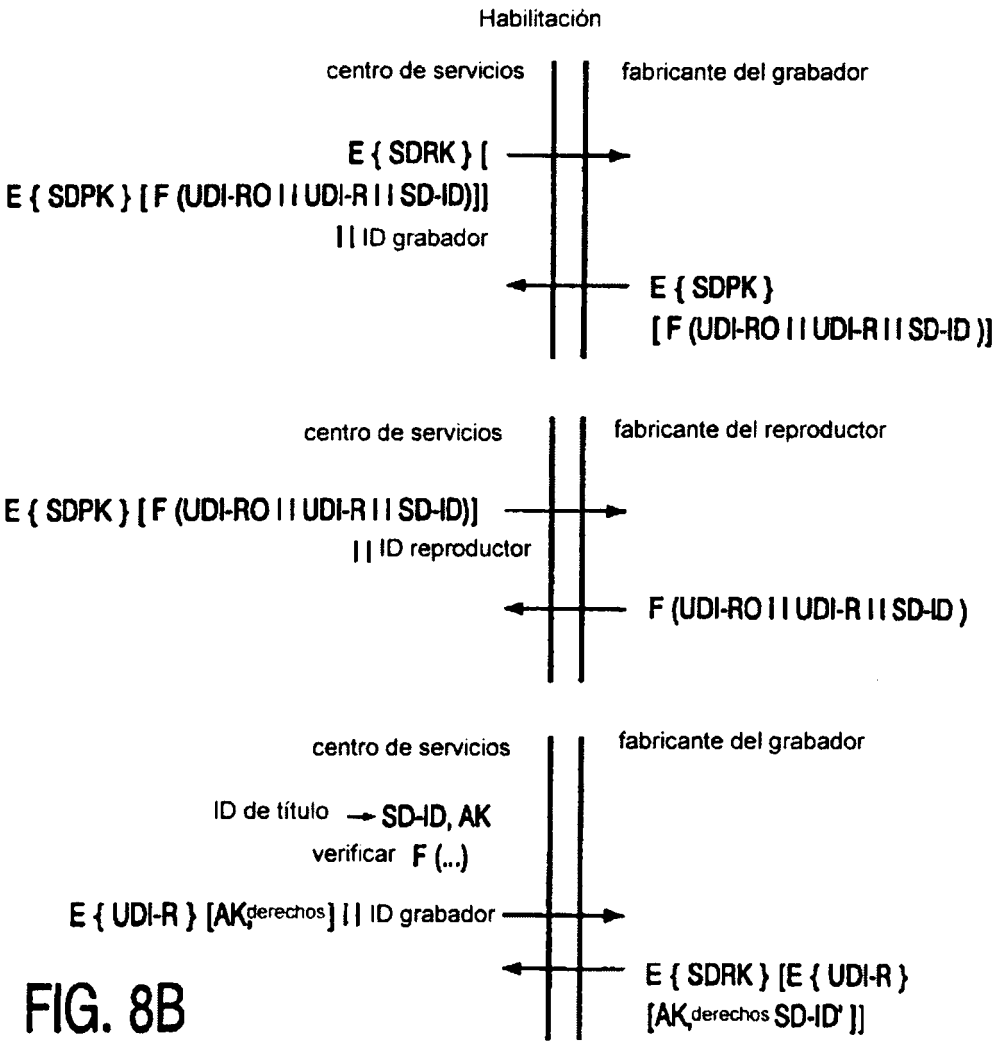
Habilitación
centro de servicios
fabricante del grabador
E { SDRK } [
E { SDPK } [F (UDI-RO I I UDI-R I I SD-ID)]]
I I ID grabador
E { SDPK }
[F (UDI-RO I I UDI-R I I SD-ID)]
centro de servicios
fabricante del reproductor
E { SDPK } [F (UDI-RO I I UDI-R I I SD-ID)]
I I ID reproductor
F (UDI-RO I I UDI-R I I SD-ID)
centro de servicios
fabricante del grabador
ID de título → SD-ID, AK
verificar F (...)
E { UDI-R } [AK derechos] I I ID grabador
E { SDRK } [E { UDI-R }
[AK derechos SD-ID']]

FIG. 8B

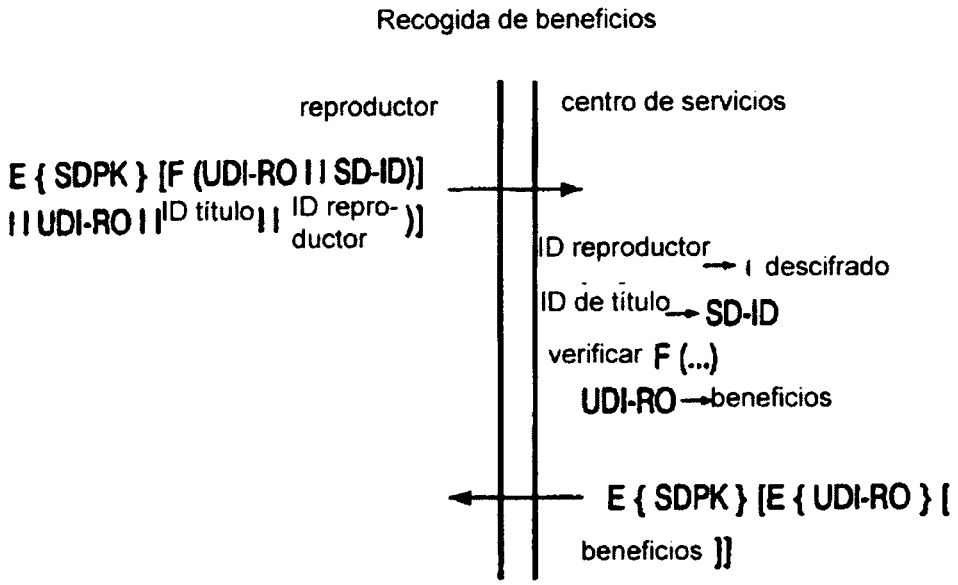
Recogida de beneficios
reproductor
centro de servicios
E { SDPK } [F (UDI-RO || SD-ID)]
|| UDI-RO || ID título || ID repro-
ductor)]
ID reproductor → descifrado
ID de título → SD-ID
verificar F (...)
UDI-RO → beneficios
E { SDPK } [E { UDI-RO } [
beneficios]]

FIG. 9A

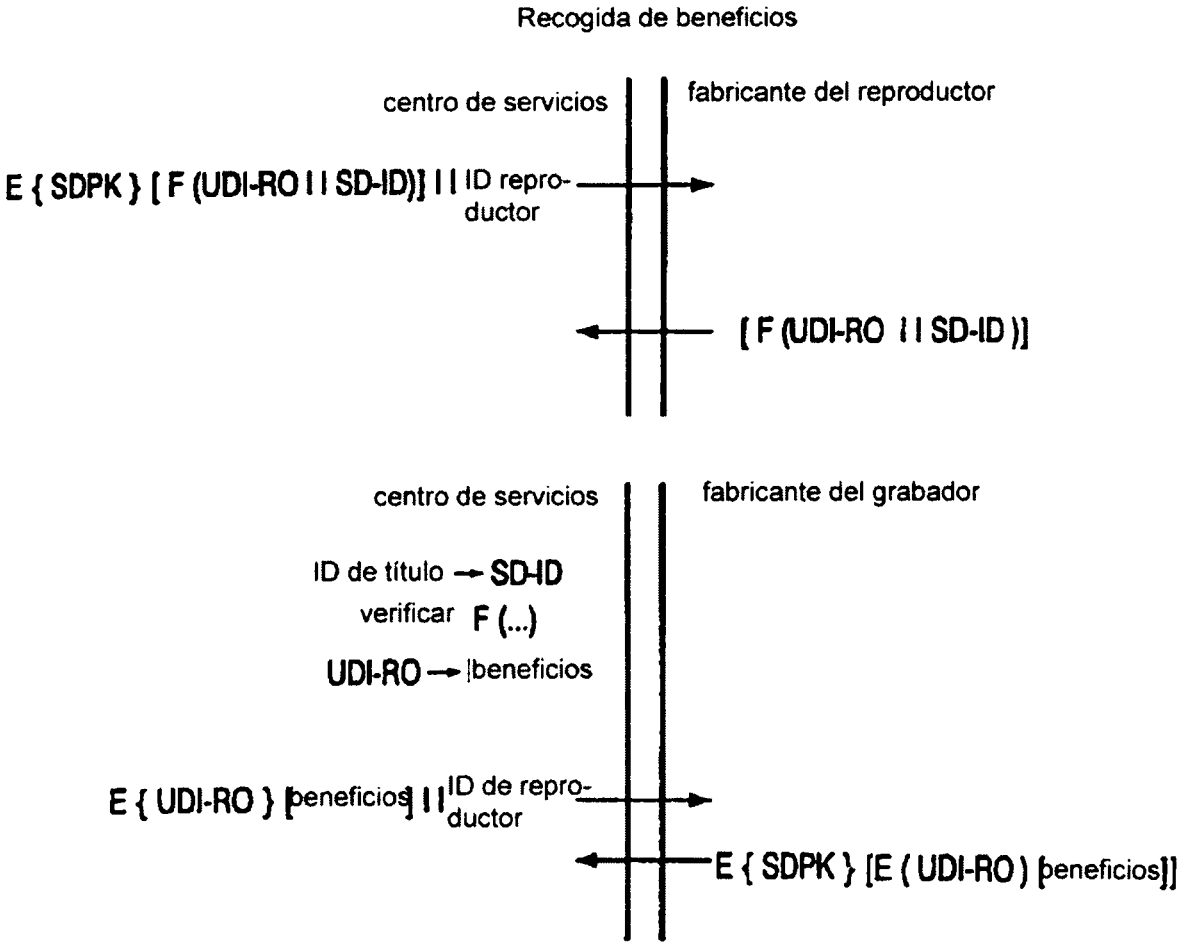
Recogida de beneficios
centro de servicios
fabricante del reproductor
E { SDPK } [F (UDI-RO || SD-ID)] || ID repro-
ductor
[F (UDI-RO || SD-ID)]
centro de servicios
fabricante del grabador
ID de título → SD-ID
verificar F (...)
UDI-RO → beneficios
E { UDI-RO } [beneficios] || ID de repro-
ductor
E { SDPK } [E (UDI-RO) [beneficios]]

FIG. 9B