(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 370 764**

(51) Int. CI.:
H04W 8/22 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09153633 .4**
(96) Fecha de presentación: **19.12.2002**
(97) Número de publicación de la solicitud: **2063675**
(97) Fecha de publicación de la solicitud: **27.05.2009**

(54) Título: **GESTIÓN DE DERECHOS DIGITALES (DRM) ROBUSTA Y FLEXIBLE CON UN MÓDULO DE IDENTIDAD INVIOLABLE.**

(30) Prioridad:
15.08.2002 SE 0202451

(45) Fecha de publicación de la mención BOPI:
22.12.2011

(45) Fecha de la publicación del folleto de la patente:
22.12.2011

(73) Titular/es:
TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)
164 83, STOCKHOLM, SE

(72) Inventor/es:
Normann, Karl y
Näslund, Mats

(74) Agente: **de Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Gestión de derechos digitales (DRM) robusta y flexible con un módulo de identidad inviolable

CAMPO TÉCNICO DE LA INVENCIÓN

La presente invención se refiere a la gestión de derechos digitales (DRM, digital rights management) para gestionar contenido digital encargado y distribuido sobre redes tales como internet.

ANTECEDENTES DE LA INVENCIÓN

La distribución de datos de medios o contenido digital utilizando tecnologías modernas de comunicación digital está en constante crecimiento, sustituyendo cada vez más a los métodos tradicionales de distribución. En particular, existe una tendencia creciente a descargar o emitir en tiempo real contenido desde un proveedor de contenidos hasta un usuario quien, a continuación, presenta o ejecuta el contenido utilizando un dispositivo de presentación o de ejecución de acuerdo con ciertas normas o derechos de uso especificados en una licencia asociada al contenido digital. Debido a las ventajas de esta forma de distribución de contenidos, incluyendo que es económica, rápida y fácil de poner en práctica, actualmente pueden encontrarse aplicaciones para la distribución de todos los tipos de medios tales como audio, video, imágenes, libros electrónicos y soporte lógico.

Sin embargo, con esta nueva forma de distribución de contenidos de medios digitales surge la necesidad de proteger los valores digitales frente al uso no autorizado y la copia ilegal. Los propietarios de derechos de autor y los creadores de contenido digital tienen lógicamente un gran interés económico en proteger sus derechos, y esto ha conducido a una creciente demanda de gestión de derechos digitales (DRM). DRM es, en general, una tecnología para proteger los valores del proveedor de contenidos en un sistema de distribución de contenidos digitales, que incluye proteger, monitorizar y limitar el uso del contenido digital así como gestionar el pago. Por lo tanto, un sistema DRM incluye normalmente componentes para cifrado, autenticación, organización de claves, administración de normas de uso y cobro.

Las amenazas más básicas para un sistema DRM incluyen interceptación, copias ilegales, modificación de las normas de uso, y el rechazo del encargo, de la distribución o del uso del contenido. La mayor parte de estos problemas básicos de seguridad se solucionan mediante técnicas criptográficas estándar que incluyen cifrado, autenticación y gestión de claves. Sin embargo, lo que distingue básicamente los problemas de seguridad de un sistema DRM respecto de otros problemas de seguridad en general, es que ni siquiera la otra parte final de la comunicación (el usuario final) es del todo fiable. De hecho, el usuario final puede querer intentar fraudulentamente extender sus derechos de uso, por ejemplo presentando el contenido del medio más veces de las que ha pagado, o copiando ilegalmente el contenido digital a otro dispositivo de presentación o de ejecución. Por lo tanto, es necesario algún modo de aplicación de las normas en el dispositivo de presentación o ejecución del usuario. A este respecto, normalmente se utiliza un circuito inviolable y algún lenguaje formal, tal como XrML, que expresa las normas de uso, junto con las técnicas básicas de criptografía mencionadas anteriormente.

Desgraciadamente, de vez en cuando los algoritmos de los circuitos DRM inviolables son pirateados, y se distribuye abiertamente una pieza de soporte lógico que fuerza alguna parte vital de la seguridad DRM de un tipo concreto de dispositivo de presentación. Desde el punto de vista del proveedor de contenidos, para propósitos de DRM esto hace inseguros todos los dispositivos de presentación de este tipo, y el proveedor de contenidos puede tener que dejar de proporcionar el contenido digital previsto para estos dispositivos de presentación, y utilizar en su lugar un algoritmo que no haya sido pirateado aún. Evidentemente, retirar y sustituir todos los dispositivos de presentación afectados es muy costoso para el fabricante/proveedor de contenidos.

Un sistema DRM robusto hará que los propietarios de derechos de autor estén más dispuestos a distribuir su material y a ofrecer una selección más amplia de contenidos para usuarios finales sobre canales abiertos, no fiables, tales como la red internet. Asimismo, proporcionará oportunidades de negocio para que los operadores de redes proporcionen la infraestructura para la distribución, el mecanismo de cobro, etcétera.

Otro problema es que a menudo es difícil, en ocasiones incluso imposible, desplazar contenido de medios desde un dispositivo de presentación o ejecución a otro. A menudo, la licencia de uso del medio está asociada a un sólo dispositivo, y si el usuario desea usar el contenido en otro dispositivo, necesita una nueva licencia. Éste es un procedimiento pesado para el usuario final, y reduce la flexibilidad en el sistema de medios del usuario.

El documento EP-1237323-A1, correspondiente al documento WO-01/43339-A1, da a conocer un teléfono celular que comprende una unidad de reproducción de música y una tarjeta de memoria extraíble para almacenar contenido, que podría ser utilizada para reproducir el contenido. Una parte de la tarjeta de memoria puede ser un módulo inviolable que comprende información de la licencia y claves públicas utilizadas para la autenticación y el cifrado/descifrado.

El documento WO-03/088054-A 1 da a conocer un sistema en el que un terminal móvil puede descargar datos cifrados desde un proveedor de contenidos. Para cifrar los datos el terminal móvil obtiene una licencia que incluye una clave de descifrado procedente de un agente DRM. Los datos son cifrados utilizando una clave pública de un par de claves pública-privada, en donde la clave pública se corresponde con una clave privada almacenada en un SIM del terminal móvil. El documento WO-03/088054-A 1 ha sido citado y considerado por la Oficina Europea de Patentes con respecto al Art 54(3) del Convenio sobre la patente europea.

El documento WO-02/084980-A1 da a conocer un cliente, tal como un teléfono celular, que interacciona con un servidor de encargos y un servidor de emisión en tiempo real y tiene medios para presentar datos de emisión en tiempo real en una pantalla y/o mediante un altavoz. Opcionalmente, el cliente tiene incorporados módulos de equipamiento físico o de soporte lógico inviolables DRM de propósito especial, asociados con un proveedor de contenidos o un operador de red. Asimismo, el cliente puede contener un módulo de identidad inviolable. El documento WO-02/084980-A1 ha sido citado y considerado por la Oficina Europea de Patentes con respecto al Art 54(3) del Convenio sobre la patente europea

El documento EP-1176757-A2 da a conocer un aparato de procesamiento de datos para la reproducción de datos desde un dispositivo de memoria o para grabar datos en el dispositivo de memoria. Se describe un método de autenticación entre el aparato de procesamiento de datos y el dispositivo de memoria. El documento WO-02/059724-A2 da a conocer un sistema para transferir y validar información a través de una red entre pares. La gestión de derechos digitales puede mejorarse mediante la identificación de contenido como relacionado con el contenido de un editor.

COMPENDIO DE LA INVENCIÓN

La presente invención supera estos y otros inconvenientes de las disposiciones de la técnica anterior.

Es un objetivo general de la presente invención dar a conocer un sistema DRM robusto y flexible.

Otro importante objetivo de la invención es dar a conocer herramientas para una solución de cliente muy flexible y relativamente segura para la gestión de derechos digitales (DRM).

Otro objetivo de la invención es dar a conocer un mecanismo DRM que permita a un operador de red o parte correspondiente ser más activo en el establecimiento y mantenimiento de la funcionalidad DRM adecuada.

Asimismo, es un objetivo de la invención poder reutilizar infraestructura existente en el diseño de un sistema DRM.

Estos y otros objetivos se satisfacen mediante un módulo de identidad inviolable, un módulo DRM de gestión de derechos digitales y un sistema cliente acordes con la invención, tal como se define mediante las respectivas reivindicaciones de patente adjuntas 1, 4 y 15. En las reivindicaciones dependientes se especifican detalles adicionales.

Una idea básica acorde con la invención es implementar un agente DRM en un módulo de identidad inviolable que está adaptado para la conexión, preferentemente conexión física, con un sistema cliente que es capaz de recibir y utilizar contenido digital. El sistema cliente tiene medios para recibir contenido digital sobre una red, y un dispositivo de uso del contenido digital tal como un dispositivo de presentación. Normalmente, el contenido digital está protegido por el proveedor de contenidos, y se transmite en forma codificada al sistema cliente, que necesita descodificar el contenido digital protegido antes de que sea posible usar el contenido digital. Asimismo, puede ser el caso que el contenido digital protegido no se transmita en absoluto al sistema cliente hasta que el cobro haya sido realizado o pueda garantizarse satisfactoriamente. El agente DRM implementado en el módulo de identidad inviolable incluye funcionalidad para habilitar el uso de contenido digital encargado, y sin dicho agente DRM, el sistema cliente simplemente no podrá utilizar el contenido digital.

De ese modo, el agente DRM implementado en el módulo de identidad inviolable puede, por ejemplo, estar dotado de funcionalidad para llevar a cabo un proceso DRM con objeto de extraer una clave apropiada de protección del contenido y/o de permitir el cobro por el uso del contenido digital.

El módulo de identidad inviolable comprende medios, quizás incluso internos al DRM, para llevar a cabo, por lo menos, una parte de un procedimiento de autenticación y gestión de claves (AKA, authentication and key agreement), y el agente DRM en el módulo de identidad inviolable lleva a cabo un proceso DRM en base a información de seguridad procedente del procedimiento AKA. Por ejemplo, la información de autenticación puede utilizarse con propósitos de cobro, y la información de gestión de claves puede utilizarse para extraer una clave de protección del contenido transferida de forma segura al sistema cliente. El procedimiento AKA se lleva a cabo en base a una clave simétrica almacenada en el módulo de identidad inviolable. La clave simétrica puede ser

compartida entre el módulo de identidad inviolable y un operador de red, una clave privada asociada con el módulo de identidad inviolable, y/o incluso una clave específica DRM.

El módulo de identidad puede ser cualquier módulo de identidad inviolable conocido en la técnica, incluyendo tarjetas SIM estándar utilizadas en teléfonos móviles GSM (Global System for Mobile Communications, sistema global para comunicaciones móviles), SIM de UMTS (Universal Mobile Telecommunications System, sistema universal de telecomunicaciones móviles) (USIM, UMTS SIM), SIM WAP (Wireless Application Protocol, protocolo de aplicación inalámbrica), conocido asimismo como WIM (WAP SIM), ISIM (IP Multimedia Subsystem Identity Module, módulo de identidad del sistema multimedia IP) y, de manera más general, módulos UICC (Universal Integrated Circuit Card, tarjeta de circuito integrado universal). Se destaca especialmente que la invención encaja en la versión actual del estándar OMA (Open Mobile Alliance, alianza móvil abierta) emergente.

Si bien la invención es particularmente adecuada para unidades móviles y DRM móvil, la invención no se limita a los módulos de identidad de abonado de red utilizados con comunicadores y teléfonos móviles. Por ejemplo, el módulo de identidad inviolable puede ser una tarjeta inteligente asociada con un descodificador para TV por satélite o un módulo de identidad inviolable para un centro de entretenimiento doméstico digital general. De hecho, la invención puede ser utilizada con cualquier cliente, incluyendo sistemas de PC (Personal Computer, ordenador personal) convencionales.

Cuando se utilizan módulos SIM, USIM, WIM, ISIM y UICC estandarizados, el agente DRM puede tener una interfaz lógica o física para algoritmos preexistentes de autenticación y generación de claves. Habitualmente, la relación abonado-operador se utiliza asimismo con propósitos de cobro en el sistema DRM global.

Se ha admitido que es particularmente ventajoso implementar el agente DRM como una aplicación en un entorno de aplicaciones proporcionado en el módulo de identidad inviolable, preferentemente en el entorno del conjunto de herramientas de aplicación del módulo de identidad. La aplicación de agente DRM puede estar preprogramada en el entorno de aplicación del conjunto de herramientas, o ser descargada de manera segura (preferentemente autenticada y cifrada) sobre una red desde una parte externa fiable asociada con el módulo de identidad. El entorno del conjunto de herramientas de la aplicación no es igual que un auténtico circuito encapsulado inviolable, pero es mucho más seguro que llevar a cabo el proceso DRM en un entorno de PC abierto, y quizás incluso hostil, y más flexible que utilizar circuitos cableados inviolables. Por ejemplo, si se encuentra un defecto de seguridad o si es pirateado todo el agente DRM, la funcionalidad es fácilmente sustituida o actualizada (incluso sobre la interfaz aérea) mediante un nuevo agente DRM. Debe entenderse que aunque un agente en soporte lógico es particularmente beneficioso, es posible asimismo tener el agente DRM prefabricado como equipamiento físico en el módulo de identidad.

La solución propuesta proporciona flexibilidad incrementada para el usuario final así como para el proveedor de contenidos y/o el operador de red. El módulo de identidad es fácilmente sustituible (incluso actualizable remotamente), "portátil" entre diferentes dispositivos de presentación o ejecución así como relativamente seguro.

En modelos corporativos en los que está limitado el uso del contenido digital, el agente DRM del módulo de identidad inviolable puede configurarse para permitir solamente el uso controlado del contenido digital encargado. Por ejemplo, el agente DRM del módulo de identidad puede incluir funcionalidad para la aplicación de las normas de uso asociadas con el contenido digital.

Especialmente cuando el dispositivo de uso del contenido digital es un dispositivo autónomo en el sistema cliente, el dispositivo de uso del contenido digital está dotado asimismo de un agente DRM. En este caso, es recomendable configurar el agente DRM en el módulo de identidad inviolable, de manera que permita el uso del contenido digital solamente por un dispositivo de uso del contenido digital que tenga un agente DRM que aplique apropiadamente las normas de uso asociadas al contenido digital. En este escenario, la funcionalidad DRM global del sistema cliente se distribuye, de hecho, con un primer agente DRM en el módulo de identidad y un segundo agente DRM en el dispositivo de uso del contenido digital. La comunicación entre los dos agentes DRM puede basarse en información de claves específicas del dispositivo de uso. De este modo, la comunicación entre los dos agentes DRM puede ser autenticada y/o protegida. En el caso de comunicación autenticada, el objetivo principal es autenticar el dispositivo de uso con objeto de verificar que el dispositivo de uso tiene una funcionalidad DRM válida. En el caso de comunicación protegida, puede asegurarse la transferencia segura de metadatos DRM tales como la clave de protección de contenidos, entre el primer agente DRM y el segundo agente DRM.

El primer agente DRM en el módulo de identidad inviolable puede, por lo tanto, estar dotado de funcionalidad para permitir el registro de dispositivos de uso del contenido digital, almacenando para cada dispositivo de uso información de la clave específica del dispositivo de uso. El registro de dispositivos de uso es particularmente importante cuando el módulo de identidad inviolable es desplazado entre diferentes dispositivos de uso, o cuando se utiliza un equipo autónomo de uso del contenido digital.

La invención proporciona a un operador de red o parte correspondiente la posibilidad de ser más activo estableciendo y manteniendo la funcionalidad DRM apropiada en el lado del cliente, utilizando el módulo de identidad inviolable como un punto común de confianza. Por lo tanto, el módulo de identidad inviolable actúa como un mediador central de funciones y/o datos asociados con DRM. El operador, el proveedor de contenidos y/o la parte correspondiente recibe la posibilidad de controlar totalmente la funcionalidad DRM, tanto en el módulo de identidad inviolable como en el dispositivo de uso interrelacionado. A este respecto, es asimismo beneficioso que el operador de red (procesando un encargo de un medio) y/o un proveedor de contenidos (procesando una solicitud de contenido) autentique que el módulo de identidad utilizado con el sistema cliente incluye un agente DRM compatible/válido. En particular, el proveedor de contenidos puede estar interesado en verificar que el dispositivo de uso está asociado con funcionalidad DRM compatible/válida. Esto puede conseguirse basándose en la autenticación del operador/módulo de identidad, autenticando implícitamente el dispositivo de uso.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La invención, junto con ventajas y objetivos adicionales de la misma, se comprenderá mejor haciendo referencia a la siguiente descripción tomada junto con los dibujos anexos, en los cuales:

la figura 1 es una visión general de un sistema de gestión de derechos digitales para encargar contenido digital sobre una red, que ilustra las partes relevantes y sus relaciones mutuas;

la figura 2A muestra esquemáticamente un sistema cliente acorde con una realización preferida de la presente invención;

la figura 2B muestra esquemáticamente un módulo de identidad inviolable acorde con una realización preferida de la presente invención;

la figura 3 es un diagrama de flujo que ilustra un método de gestión de derechos digitales acorde con una realización preferida de la invención;

la figura 4 es un diagrama esquemático que ilustra un ejemplo de autenticación y gestión de claves cliente-operador, gestión de derechos digitales en el lado del cliente, así como la comunicación asociada cliente-operador;

la figura 5 ilustra una realización de la invención con funcionalidad DRM distribuida entre un módulo de identidad inviolable y un dispositivo de presentación asociado, de acuerdo con una realización de la invención;

la figura 6 ilustra un ejemplo de un módulo DRM distribuido con comunicación entre los agentes DRM distribuidos, en base a una clave específica del dispositivo de uso, de acuerdo con una realización preferida de la invención;

la figura 7A muestra un procedimiento de autenticación pregunta-respuesta entre los agentes DRM en el módulo DRM de la figura 6;

la figura 7B ilustra la comunicación cifrada entre los agentes DRM distribuidos en el módulo DRM de la figura 6;

la figura 8 ilustra una implementación preferida de un módulo DRM distribuido, con comunicación basada en claves de dispositivo entre un agente DRM en un módulo de identidad inviolable y un agente DRM en un dispositivo de presentación;

la figura 9 es un diagrama de flujo esquemático de un método de gestión de derechos digitales para establecer comunicación basada en claves de dispositivo entre agentes DRM distribuidos;

la figura 10 muestra un módulo de identidad inviolable y un dispositivo de presentación asociado de acuerdo con otra realización de la invención;

la figura 11 es un diagrama esquemático de un ejemplo de un protocolo DRM que involucra un operador, un módulo de identidad de abonado inviolable, un proveedor de contenidos y un dispositivo de presentación; y

la figura 12 es un diagrama de bloques esquemático de partes relevantes de un sistema DRM que funciona en base al protocolo de la figura 11.

DESCRIPCIÓN DETALLADA DE REALIZACIONES DE LA INVENCIÓN

A través de los dibujos, se utilizarán los mismos caracteres de referencia para elementos correspondientes o similares.

La presente invención es aplicable, en general, a la gestión de derechos digitales (DRM) utilizada en un sistema de encargo y distribución de contenidos digitales. En dicho sistema de encargo y distribución, se proporcionan medios o contenidos digitales desde un proveedor de contenidos a un cliente sobre una red, por ejemplo internet y/o una red inalámbrica para comunicación móvil, gestionada por un operador de red. Para facilitar la comprensión de la invención, sigue una breve discusión de algunas funciones DRM generales. Tal como se ha mencionado en la sección de antecedentes, la DRM se utiliza para proteger los valores de los propietarios de derechos digitales en un sistema de encargo y distribución de contenidos digitales. En dicho sistema, la DRM contempla habitualmente la autenticación y gestión de claves, la gestión de los derechos de utilización de uso incluyendo la aplicación, y el cobro. Estas funciones DRM están implementadas en módulos DRM dispuestos en las partes pertinentes, es decir por ejemplo en un sistema cliente, en un servidor del operador de red y en un servidor de medios o contenidos del proveedor de contenidos. Comenzando con la autenticación y gestión de claves, se utiliza autenticación para identificar a las partes en el proceso de encargo y distribución de contenidos digitales. Para la autenticación pueden utilizarse técnicas bien conocidas en la técnica, tales como mensajes, autenticación de usuario y/o de dispositivo y firmas digitales que utilizan claves criptográficas [1]. Además, pueden utilizarse técnicas para marcar o estampar contenido digital, de manera que éste puede ser rastreado durante el proceso de distribución y uso posterior. Las marcas de agua y las huellas dactilares son dos técnicas que se utilizan usualmente para marcar contenidos. Asimismo, los módulos DRM en el sistema transportan, almacenan y generan, de manera segura, claves criptográficas para utilizar en el proceso de encargo y distribución de contenido digital. Las claves son utilizadas para proteger criptográficamente mensajes, incluyendo el propio contenido digital, durante la distribución sobre la red.

Asimismo, los módulos DRM realizan la gestión de las normas de uso, incluyendo la aplicación de normas. El contenido digital encargado está asociado con una licencia o permiso digital que especifica las normas de uso del cliente y los derechos del medio digital obtenido. Esta forma de gestión está relacionada con el propio contenido digital y trata cuestiones tales como quién lo obtiene, cómo se distribuye, cómo puede ser utilizado, cuántas veces puede ser utilizado (presentado, ejecutado, grabado, reenviado, copiado y/o modificado), qué duración tienen los derechos, quién recibe el pago, cuánto cobra y cómo. Parte o la totalidad de estos aspectos se especifican en la licencia, que puede distribuirse junto con el contenido digital. Para describir las normas de uso, han sido desarrollados lenguajes especiales denominados lenguajes de derechos. Dos de los lenguajes de derechos más extendidos utilizados actualmente son el lenguaje de marcas para derechos (XrML, Rights Markup Language) y el lenguaje abierto de derechos digitales (ODRL, Open Digital Rights Language). En el dispositivo de presentación o ejecución del cliente, el módulo DRM está implementado para asegurar que el uso, en el caso más frecuente la presentación, sigue lo descrito en las normas de uso, y para impedir el rechazo del contenido digital y de las normas de uso.

Finalmente, la gestión del cobro se refiere en general a un procedimiento del propio pago por el uso del contenido digital. Pueden utilizarse varias técnicas diferentes, tales como técnicas de tarjeta de crédito para el pago sobre internet, pago a través de una suscripción o de una cuenta de prepago, o incluso utilizando "dinero electrónico". Asimismo, un sistema DRM puede incluir la gestión de tickets que representan un valor que puede ser recuperado y que autorizan al propietario del ticket a acceder al contenido digital especificado. Por lo tanto, los derechos de uso asociados al contenido digital encargado no están, en general, limitados al propio "uso" tal como la presentación, la copia, el reenvío y similares, sino que puede incluir asimismo la recuperación del valor del ticket o de partes del mismo.

En la figura 1 se muestra esquemáticamente un ejemplo de un sistema de encargo y distribución de contenido digital que incorpora funciones DRM, que ilustra las partes relevantes y sus relaciones mutuas. El sistema ejemplar de la figura 1 incluye un cliente con acceso a una red a través de un acuerdo, por ejemplo una suscripción, con un operador de red. Esta relación de confianza cliente-operador se manifiesta usualmente en una relación criptográfica, es decir compartiendo claves simétricas o teniendo cada uno acceso a la clave pública del otro (certificada por una parte de confianza común) si se utiliza criptografía asimétrica. Se presenta asimismo una relación de confianza entre el operador de red y el proveedor de contenidos, pero en forma de acuerdo comercial. Este acuerdo podría manifestarse mediante una compartición de claves y/o un acceso a claves, similares a lo descrito anteriormente para el cliente y el operador de red. Sin embargo, entre el cliente y el proveedor de contenidos se establece una relación de confianza inducida cada vez que el cliente obtiene contenido digital desde el proveedor de contenidos. Esta confianza inducida se manifiesta en una clave de sesión utilizada para proteger de manera criptográfica el contenido digital cuando éste es transmitido al cliente sobre la red.

En un típico proceso de encargo y distribución de contenidos, el cliente conecta en primer lugar al operador de red. A continuación el operador autentica el cliente y posiblemente verifica que el cliente tenga un agente DRM válido para gestionar metadatos DRM, tales como normas de uso, datos cifrados y claves, asociados con el contenido digital. El cliente selecciona el contenido del medio digital, y acepta/selecciona las normas de uso válidas para el

medio, por ejemplo permitiendo la presentación del medio un número seleccionado de veces o durante un período de tiempo dado. Generalmente, las normas de uso básicas están determinadas por el proveedor de contenidos, pero algunos aspectos de las normas de uso pueden estar abiertos para su selección por el usuario. En la presente invención, contenido digital se refiere a datos digitales que pueden ser descargados o emitidos en tiempo real sobre una red para su uso en un sistema cliente, y por lo tanto incluyen por ejemplo audio, video, imágenes, libros electrónicos y otro material de texto electrónico, así como soporte lógico (programas de aplicación, juegos de ordenador, etcétera). Otros tipos de uso del contenido digital aparte de la presentación y la ejecución incluyen reenviar, grabar, copiar, imprimir, y posiblemente modificar el contenido digital. En lo que sigue, la invención se describirá principalmente haciendo referencia a la presentación de contenido digital. Aunque debe entenderse que la invención no se limita a la presentación de audio, video y texto, sino que cubre cualquier uso o consumo de contenido de medios, incluyendo la ejecución de programas de aplicación y juegos de ordenador.

Se realiza entonces un encargo al operador, que escribe y asegura/protege un ticket que especifica el contenido encargado y las normas de uso. El ticket es enviado al cliente, en donde el agente DRM autentica y descifra ticket y extrae una clave de sesión a partir del ticket recibido. El ticket puede ser descifrado por medios criptográficos convencionales, por ejemplo utilizando una clave simétrica asociada con el cliente y el operador de red, o una clave privada del cliente. Preferentemente, esta clave de descifrado es la clave de suscripción cliente-operador, una clave DRM especial asociada con el agente DRM, o una clave derivada de una o ambas de estas claves. La clave de sesión extraída será utilizada finalmente para descifrar el medio digital procedente del proveedor de contenidos. El cliente recibe asimismo una copia del ticket cifrado con la clave del acuerdo operador-proveedor de contenidos (o una clave derivada de la misma). Esta copia del ticket es reenviada al proveedor de contenidos, en donde es extraída la clave de sesión después de que haya sido verificada la validez del ticket. A continuación, el proveedor de contenidos distribuye al cliente el contenido digital encargado protegido de manera criptográfica, ya sea como datos descargados o como datos emitidos en tiempo real. Finalmente, el contenido digital es descifrado en el cliente mediante la clave de sesión extraída previamente. A continuación el contenido digital puede ser utilizado, por ejemplo presentado o ejecutado, mediante el cliente o un dispositivo asociado de acuerdo con las normas de uso. Puede encontrarse más información sobre sistemas DRM y sobre encargo y distribución de contenido digital en [2], así como en [3].

El proceso global de encargo y distribución de contenidos discutido anteriormente se proporciona simplemente como un ejemplo simplificado para trasladar una imagen general de dichos procesos. Para incrementar la seguridad, pueden introducirse más etapas de autenticación y criptográficas. Además, el cliente deberá pagar por el contenido encargado, de manera que en el proceso de encargo están presentes casi siempre las etapas de facturación y cobro. Dicho cobro puede llevarse a cabo mediante una suscripción al operador de red, enviando el número de la tarjeta de crédito del cliente al operador de red o a un centro dedicado a facturación que gestione el cobro de contenido digital, o mediante algunos otros medios. Además, el operador de red puede proporcionar tanto servicios de red como contenido digital y, por lo tanto, puede actuar al mismo tiempo como operador y como proveedor de contenidos. Sin embargo, el operador tiene habitualmente un servidor de contenidos dedicado y uno o varios servidores de autenticación/cobro dedicados, de manera que las partes ilustradas en la figura 1 están presentes aunque el operador de red gestione asimismo los servicios de provisión de contenidos. En algunas aplicaciones, por ejemplo en aplicaciones WAP (Wireless Application Protocol, protocolo de aplicación inalámbrica), es posible asimismo que otro cliente pueda actuar como proveedor de contenidos. A continuación las normas de uso se pasan desde el operador de red o el proveedor de contenidos al cliente receptor del contenido.

Ha sido admitido que una solución parcial a los problemas objetivos tratados en la sección de antecedentes puede ser utilizar un dispositivo inviolable portátil que pueda ser desplazado entre dispositivos de presentación o ejecución. Sin embargo, si un usuario compra un nuevo dispositivo, habitualmente existe algún molesto procedimiento de configuración antes de que puede utilizarse el nuevo dispositivo.

La idea básica acorde con la invención es implementar un agente DRM en un módulo de identidad inviolable que está previsto para cooperar con un sistema cliente, tal como un teléfono móvil o un sistema informático. Preferentemente, el módulo de identidad inviolable se proporciona como una tarjeta inteligente o equivalente, que está adaptada para la conexión física con partes apropiadas, tales como una ranura para tarjetas del sistema cliente. En general, el agente DRM está implementado con funcionalidad para permitir el uso, tal como la presentación o la ejecución, de contenido digital protegido proporcionado al cliente desde un proveedor de contenidos. Preferentemente, el uso está controlado por normas de uso asociadas al contenido digital. Habitualmente, el agente DRM incluye funcionalidad para el procesamiento criptográfico de metadatos DRM asociados con el contenido digital a presentar. Estos metadatos puede ser, por ejemplo, una o varias claves y datos de usuarios tales como el propio contenido digital cifrado. Por ejemplo, el agente DRM puede incluir alguna funcionalidad básica para, más o menos directamente, generar o extraer una clave de descifrado a utilizar para descifrar el contenido digital cifrado. Asimismo, es posible integrar en el agente DRM el propio descifrado del contenido digital, así como funcionalidad para la aplicación de las normas y para facilitar el cobro.

El módulo de identidad puede ser un módulo de identidad inviolable conocido en la técnica, incluyendo tarjetas SIM estándar utilizadas en teléfonos móviles GSM, SIM de UMTS, módulos WIM y ISIM, así como módulos UICC en general.

En lo que sigue, la invención se describirá principalmente haciendo referencia a un módulo de identidad de abonado de red, tal como un módulo SIM, USIM, WIM, ISIM ó UICC. Si bien la invención es particularmente útil para DRM móvil basado en un módulo de identidad de abonado de red, debe entenderse que la invención no se limita a esto. Alternativamente, el módulo de identidad podría ser emitido por un actor no de telecomunicaciones y proporcionado, por ejemplo, como una tarjeta inteligente emitida por un banco a sus clientes, o como un módulo de identidad asociado a un descodificador para TV por satélite o, más en general, para un centro de entretenimiento doméstico digital.

Implementando el agente DRM en un módulo de identidad de abonado de red tal como un módulo SIM, USIM, WIM, ISIM ó UICC, el agente DRM es potencialmente más seguro que en un entorno de PC abierto, y quizás incluso hostil. Esto se debe a que las plataformas de sistema operativo de los PCs, por ejemplo Windows y Linux, son mejor conocidas por el público que las correspondientes plataformas de los módulos SIM, USIM, WIM ó ISIM las cuales, por lo tanto, resultan más difíciles de atacar y modificar. Debido al carácter inviolable inherente de dichos módulos de identidad de abonado de la red, una configuración de seguridad apropiada será difícil de neutralizar.

El hecho de que el módulo de identidad de abonado está, normalmente, dispuesto de modo extraíble desde el sistema cliente facilita mover el módulo de identidad, con su agente DRM, entre diferentes dispositivos, y facilita asimismo la sustitución del agente DRM si éste fuera pirateado.

Si bien el agente DRM puede implementarse como equipamiento físico especial en el módulo de identidad de abonado de red, la implementación más preferida actualmente consiste en un agente DRM basado en soporte lógico. Se ha admitido que es particularmente ventajoso implementar el agente DRM como una aplicación en un entorno de aplicaciones del módulo de identidad, preferentemente el entorno del conjunto de herramientas de aplicación del módulo de identidad de abonado de red, tal como el conjunto de herramientas de aplicaciones SIM (SAT, SIM Application Toolkit) GSM, o el entorno SAT de UMTS (USAT). La aplicación de agente DRM puede estar preprogramada en el entorno del conjunto de herramientas de aplicación, o ser descargada de modo seguro (preferentemente autenticada y cifrada), o más en general cargada, desde un operador de red asociado con el módulo de identidad de abonado. El SAT, USAT o conjunto de herramientas de aplicación equivalente proporciona un entorno que puede ser actualizado fácilmente con soporte lógico nuevo de manera segura, lo cual se describirá en más detalle a continuación.

Además, puede utilizarse la infraestructura del operador móvil para solucionar los problemas de configuración asociados a la utilización del agente DRM con nuevos dispositivos de presentación, tal como se explicará posteriormente.

La figura 2A muestra esquemáticamente un sistema cliente acorde con una realización preferida de la presente invención. El cliente puede ser cualquier clase de aplicación o sistema, que pueda encargar y obtener contenido digital sobre una red, por ejemplo un teléfono móvil con un módulo de identidad dispuesto de manera extraíble en una ranura para tarjetas, o un ordenador personal equipado con un lector de tarjetas en el cual se inserta un módulo de identidad semejante. En el ejemplo de realización, el sistema cliente 100 comprende una unidad 110 de comunicación de red, un módulo 120 de identidad inviolable y un dispositivo de uso de contenidos digitales, ilustrado en este caso como un dispositivo 130 de presentación. La unidad 110 de comunicación de red implementa una pista de protocolos de comunicación de red, y permite de ese modo la descarga o la emisión en tiempo real de contenido digital desde un proveedor de contenidos al cliente, utilizando comunicación de red inalámbrica o no inalámbrica.

Tal como se ha mencionado anteriormente, el módulo 120 de identidad inviolable comprende un agente DRM 125 implementado en equipamiento físico, en soporte lógico o en una combinación de los mismos. El dispositivo 130 de presentación podría implementarse asimismo en soporte lógico, en equipamiento físico o en una combinación de los mismos. Preferentemente, el dispositivo 130 de presentación incluye un procesador 131 de medios, que puede estar implementado en soporte lógico, para presentar el contenido digital utilizando una pantalla o un altavoz, dependiendo del tipo de contenido digital. El dispositivo 130 de presentación comprende usualmente alguna clase de funcionalidad DRM 135, por ejemplo aplicación de normas y habitualmente también descifrado del contenido de medios protegido, en base a una clave generada por el agente DRM 125 implementado en el módulo 120 de identidad.

El dispositivo de presentación puede estar integrado en una unidad móvil o en un PC, pero puede asimismo estar dispuesto como un dispositivo autónomo conectado a estos directa (a través de puertos de comunicación adecuados) o indirectamente. En el caso autónomo, el cliente puede tener una unidad para descarga o emisión en tiempo real de contenido digital y otra unidad separada físicamente para utilizar o presentar de hecho el contenido digital es decir, el dispositivo de presentación. La unidad de descarga o emisión en tiempo real puede ser, por ejemplo, un ordenador personal o una unidad móvil con equipamiento físico/soporte lógico adecuados para recibir el

contenido digital. A continuación, el contenido es preferentemente transmitido al dispositivo de presentación a través de canales ordinarios o mediante comunicación inalámbrica con o sin implicación de una red. Los dispositivos de presentación autónomos típicos incluyen reproductores Mp3, reproductores de MD, reproductores de CD, reproductores de DVD, otras unidades móviles o PCs. Alternativamente, el dispositivo de presentación tiene su propia interfaz de comunicación de red para recibir contenido digital protegido y, posiblemente, también normas de uso del mismo.

Tal como se ha mencionado anteriormente, el agente DRM puede implementarse como una aplicación de soporte lógico en un módulo de identidad inviolable, tal como se ilustra esquemáticamente en la figura 2B. El módulo 120 de identidad comprende preferentemente una unidad 121 de entrada/salida, un módulo AKA (autenticación y gestión de claves) 122, una clave k 123 de suscripción o de abonado así como un entorno 124 de aplicaciones.

La unidad 121 de E/S analiza sintácticamente los comandos enviados al módulo de identidad y maneja la comunicación con las funciones internas. El módulo 122 AKA comprende algoritmos para la autenticación mutua entre el cliente y la red, y para obtener claves. Habitualmente, la función AKA utiliza una clave específica del módulo de identidad, por ejemplo la clave de suscripción k asociada con la suscripción cliente-operador, una clave derivada de la misma o una clave x asociada con el agente DRM 125 implementado en el módulo de identidad. En GSM, por ejemplo, la función AKA está soportada generalmente por los algoritmos A3/A8 AKA. Asimismo, es posible utilizar criptografía asimétrica con propósitos de autenticación.

En general, los procedimientos de autenticación y gestión de claves (AKA) pueden ser más o menos sofisticados, variando desde AKA muy simple, con un procedimiento de gestión de claves en el que se utiliza directamente la información de clave secreta como una clave de sesión, a algoritmos AKA más complejos y seguros.

El entorno 124 de aplicaciones está previsto ventajosamente por el conjunto de herramientas de aplicación del módulo de identidad. Para un SIM GSM, el entorno de aplicaciones puede estar previsto por el conjunto de herramientas de aplicación SIM (SAT) [4], mientras que el entorno de aplicación analógico de SIM UMTS (USIM) está previsto por SAT UMTS (USAT) [5].

Para un SIM GSM, la interfaz SIM-ME (SIM-Mobile Equipment, SIM-equipo móvil) que se define en [6] especifica los "comandos" y datos que pueden ser enviados hacia/recibidos desde el SIM/ME. Por ejemplo, para ejecutar los algoritmos AKA A3/A8 GSM, existe un comando "RUN_GSM_ALGORITHMS" ("ejecutar algoritmos GSM") que encamina los parámetros de entrada/resultados de salida hacia/desde los algoritmos AKA residentes. Los algoritmos AKA calculan una respuesta y/o una o varias claves a partir de una pregunta aleatoria RAND y la clave de abonado memorizada, k, o una clave de seguridad correspondiente. En la lista de posibles comandos sobre la interfaz SIM-ME, destacamos en especial el comando "ENVELOPE" ("sobre"), que está previsto para enviar datos más o menos arbitrarios al SIM para utilizar con el conjunto de herramientas de aplicación SIM (SAT). El formato de entrada/salida para el SIM se especifica explícitamente, pero existe un elevado grado de libertad sobre exactamente qué pueden, o no, hacer las aplicaciones. Por ejemplo, la aplicación podría ser una miniaplicación Java muy general, véase [7]. La miniaplicación puede recibir diversos grados de autorización para acceder a los archivos residentes relacionados con GSM, siendo posiblemente uno de estos proporcionarle "pleno acceso GSM".

En una realización preferida de la invención, el agente DRM se implementa en el entorno de aplicaciones previsto por el conjunto de herramientas de aplicación SIM (SAT) o en un conjunto correspondiente de herramientas para otro tipo de módulo de identidad, utilizando el comando "ENVELOPE" o un comando análogo. A continuación, los datos introducidos a la aplicación son asimismo transferidos al SAT mediante el comando ENVELOPE. Por lo tanto, el conjunto de herramientas de aplicación SIM (SAT) permite al operador "codificar en datos en el programa fuente" ("hardcode"), o descargar, sobre la interfaz aérea en el caso de un móvil, la aplicación de agente DRM al SIM. En el caso de la descarga, es asimismo posible (y muy recomendable) autenticar la aplicación de descarga DRM como procedente del operador correcto. Esto es importante puesto que proporciona protección frente a la descarga de "virus" procedentes de servidores maliciosos. La aplicación DRM descargada puede, asimismo, estar cifrada de manera que el contenido de la aplicación no esté disponible fuera del SIM. Para aspectos de seguridad relacionados con SAT GSM, se hace referencia a [8]. Para la comunicación entre el agente DRM y el módulo AKA existe preferente, pero no necesariamente, una interfaz directa entre el módulo AKA 122 y el entorno 124 de aplicación SAT. La ejecución de la aplicación DRM en el entorno SAT está soportada de forma natural por los recursos de procesamiento del SIM. Para más información sobre los detalles básicos de la especificación SIM GSM, se hace referencia a [9].

Debe entenderse que el entorno 124 de aplicaciones puede, opcionalmente, disponerse con su propio módulo AKA específico, que funciona en base a x y/o a k. Preferentemente, este módulo AKA está integrado en la aplicación de agente DRM, tal como se indica esquemáticamente en la figura 2B.

Implementando el agente DRM del módulo de identidad inviolable en el entorno de aplicaciones, es posible asimismo actualizar la funcionalidad del agente DRM. Las actualizaciones son descargadas simplemente utilizando comandos de descarga asociados con el cliente e implementados, por ejemplo utilizando el comando ENVELOPE,

en el entorno de aplicaciones del cliente. Ésta es una solución ventajosa si el agente DRM está estropeado o "pirateado", de manera que su código y/o sus claves secretas se hacen disponibles públicamente, por ejemplo en la red internet. Entonces, en lugar de cambiar todos los dispositivos cliente, el agente DRM asociado es simplemente actualizado descargando e implementando nuevos algoritmos y/o claves.

Para el cifrado y la autenticación en el sistema DRM, pueden utilizarse cualesquiera técnicas criptográficas estándar, incluyendo cifrado y autenticación tanto simétricos como asimétricos. Utilizando cifrado y/o autenticación simétricos, la clave de cifrado es una clave simétrica compartida, de la cual se almacena una copia tanto en el módulo de identidad como en el operador de red o el proveedor de contenidos. Alternativamente, pueden utilizarse un par de claves asimétricas para el cifrado y la autenticación en base a una infraestructura de clave pública (PKI, Public Key Infrastructure). Para el cifrado asimétrico, se utiliza la clave pública para el cifrado y la correspondiente clave privada para el descifrado. Para la autenticación asimétrica, se utiliza la clave privada para la firma y la correspondiente clave pública para la autenticación. Asimismo, en el contexto de la autenticación pueden utilizarse nombres de usuario y claves asociadas con la suscripción. Si el cliente tiene una o varias direcciones de red, por ejemplo direcciones IP, asociadas a ésta, dicha dirección o direcciones pueden utilizarse asimismo para autenticación, al menos en cierta medida.

No obstante, en lo que sigue, el cifrado y la autenticación se describirán principalmente en el contexto de criptografía simétrica, utilizando la clave de abonado k y/o una clave x específica DRM del módulo de identidad. La clave específica DRM x puede estar ubicada en cualquier lugar en el módulo de identidad, preferentemente en el entorno de aplicaciones, e incluso integrada en el agente DRM.

La figura 3 es un diagrama de flujo que ilustra un método de gestión de derechos digitales acorde con una realización preferida de la invención. El método está dirigido al lado del operador de redes del sistema DRM global, y se ocupa de la descarga, o más en general de la carga, de un agente DRM en un módulo de identidad inviolable dispuesto en relación con un sistema cliente. Como una primera etapa (S1) recomendada, pero opcional, se lleva a cabo la autenticación mutua entre cliente y operador o parte correspondiente. El operador puede generar opcionalmente datos de autenticación para su transmisión al módulo de identidad del cliente, con objeto de permitir al cliente autenticar que el agente DRM procede de un operador fiable. El operador realiza una descarga (S2), opcionalmente autenticada, de un agente DRM al módulo de identidad, por ejemplo como una aplicación SAT en un SIM utilizando el comando "ENVELOPE". Si es necesario, por ejemplo debido a un defecto de seguridad, el agente DRM puede ser actualizado remotamente (S3) por el operador de red, que descarga los parches o algoritmos DRM completamente nuevos requeridos. El operador o el proveedor de contenidos pueden, asimismo, autenticar que los clientes solicitantes tienen módulos de identidad con agentes DRM compatibles, utilizando cualquier técnica de autenticación conocida. La autenticación del agente DRM incluye normalmente la verificación de que el agente DRM es de un tipo compatible, pero preferentemente incluye asimismo la verificación de la versión del agente DRM.

La figura 4 es un diagrama esquemático que ilustra un ejemplo de autenticación y gestión de claves cliente-operador, gestión de derechos digitales en el lado del cliente, así como la comunicación asociada cliente-operador. En este ejemplo concreto, el cliente envía al operador una solicitud de autenticación (o activación DRM), junto con una etiqueta de identificación. El operador lleva a cabo la autenticación y gestión de claves (AKA) utilizando una pregunta aleatoria, RAND, otros datos del usuario opcionales, la clave k y/o una clave DRM x especial como entrada a las funciones criptográficas f y m, generando de ese modo una clave de sesión t a utilizar para una comunicación segura entre el cliente y el operador y una respuesta esperada, XRES, respectivamente. El operador envía la pregunta aleatoria, RAND, posiblemente junto con una etiqueta de autenticación, al módulo de identidad del cliente. Los datos son recibidos por el módulo de identidad del cliente y, si está presente una etiqueta de autenticación, el módulo de identidad autentica en primer lugar los datos recibidos utilizando k/x y a continuación ejecuta las mismas funciones AKA f y g con la misma entrada para obtener la clave de sesión t y una respuesta, RES. La respuesta, RES, se devuelve al operador y se compara con la respuesta esperada calculada previamente, XRES, de manera que puede verificarse que el operador está en contacto con la aplicación correcta. En lo que sigue, $E_z(m)$ representa un mensaje m, protegido por una clave z. Se entiende que "E" indica "filtrado" ("encryption"), pero puede (y a menudo debe) abarcar autenticación, integridad y, para ciertos tipos de contenido digital, quizás incluso protección contra repetición. A continuación, el cliente realiza un encargo, protegido por la clave de sesión t, al operador. El operador, que en este ejemplo concreto actúa como un servidor de encargos, genera un ticket y otra clave de sesión s, denominada asimismo una clave de protección del medio o del contenido, y cifra el ticket y la clave s con la clave de sesión t generada previamente. El ticket y la clave s de protección del medio cifrados son enviados al cliente, que invoca al agente DRM para descifrar el ticket y la clave s de protección del medio utilizando la clave t. Asimismo, la clave s de protección del medio y el ticket asociado son enviados de forma segura al proveedor de contenidos, que a continuación cifra el contenido digital encargado utilizando la clave s de protección del medio y envía el medio protegido al cliente. Una vez recibido por el cliente, el contenido del medio protegido es descifrado, por el agente DRM o más probablemente por alguna funcionalidad DRM presente en el dispositivo de presentación, utilizando la clave s de protección del medio.

Preferentemente, el módulo de identidad es la base para un mecanismo de cobro que puede ser utilizado asimismo para el pago de contenido digital en el sistema DRM. En la forma más simple, el cobro por el uso de contenido digital

está basado en suscripción, y el procedimiento AKA en el módulo de identidad asegura que se cobrará y facturará por el contenido al usuario/abonado correcto. Lo mismo aplica a una suscripción de prepago en donde es necesario asegurarse de que se accederá para el cobro a la cuenta de prepago correcta. En una solución más avanzada, pueden utilizarse tarjetas de crédito o alguna forma de micropago, en donde puede utilizarse información, tal como una clave de sesión, procedente del procedimiento AKA para proteger la transferencia de datos de cobro tales como el número de tarjeta de crédito o “marcas” de pago, posiblemente junto con información de integridad protegida relativa al uso del contenido.

Por ejemplo, es posible configurar el agente DRM en el módulo de identidad, especialmente cuando está estrechamente asociado al dispositivo de presentación, de tal modo que compile información relacionada con el propio proceso de uso del contenido digital, tal como información relativa a qué contenido se utilizó, la calidad del contenido utilizado, qué cantidad de datos y durante cuánto tiempo o cuantas veces se ha utilizado el contenido. A continuación, esta información puede servir como base para el cobro por el uso del contenido digital. A continuación, la integridad de la información reunida puede protegerse en base a una clave k/x específica del módulo de identidad y transferirse al operador de red o a un centro de facturación dedicado que gestiona el propio cobro del contenido digital.

Tal como se ha indicado previamente, el agente DRM implementado en el módulo de identidad incluye habitualmente funcionalidad para el procesamiento criptográfico de metadatos DRM asociados con el contenido digital a presentar. Los metadatos pueden ser, por ejemplo, una o varias claves así como información cifrada. Normalmente, el agente DRM incluye alguna funcionalidad básica para generar o extraer más o menos directamente una clave de descifrado a utilizar para descifrar el contenido digital cifrado, tal como se describe a continuación haciendo referencia a la figura 5.

En la figura 5, el módulo de identidad y el dispositivo de presentación se muestran como unidades separadas. Estas unidades pueden estar situadas conjuntamente en el mismo dispositivo cliente, tal como un teléfono móvil, un PC, un receptor de radio o, alternativamente, el dispositivo de presentación puede proporcionarse como un dispositivo cliente externo autónomo, mediante lo cual los dispositivos cliente separados están interconectados directa o indirectamente. El diagrama de bloques de la figura 5 ilustra solamente aquellos componentes que son relevantes para la invención. El módulo 120 de identidad tiene un módulo 122 AKA, y un agente 125 DRM. Entre otras cosas, el módulo 122 AKA genera la clave t de sesión, preferentemente en base a la clave de abonado, k, y/o a una clave DRM especial, x. El agente 125 DRM comprende una unidad criptográfica C1 para extraer la clave s de protección del medio (denominada asimismo una clave de sesión) en base a la clave t de sesión recibida desde el módulo AKA 122 y a la información cifrada $E_t(s)$ recibida desde el operador de red. En esta realización, el dispositivo 130 de presentación incluye un procesador 131 de medios y un agente 135 DRM. El agente 135 DRM del dispositivo 130 de presentación incluye una unidad criptográfica C2 para descifrar el contenido del medio protegido procedente del proveedor de contenidos utilizando la clave de protección del medio extraída por el agente 125 DRM del módulo de identidad. El contenido del medio descifrado es enviado finalmente al procesador 131 del medio en el dispositivo 130 para preparar la propia presentación.

Debe observarse que la protección de la clave s de protección del contenido, por ejemplo mostrada en la figura 5, se aplica preferentemente al nivel de la aplicación, facilitando de ese modo actualizaciones de funcionalidad. En un típico sistema de comunicación (por ejemplo GSM, UMTS), la clave s de protección del contenido se protegerá asimismo en una capa inferior (de enlace) mediante la protección de la interfaz (aérea). Lógicamente, esta última protección está basada asimismo en procedimientos de gestión de claves, utilizando habitualmente solamente la clave k de suscripción de red. En otras palabras, la clave de protección del contenido estará habitualmente protegida "doblemente", en la capa de enlace por una clave t'(k) y en el nivel de aplicación por la clave t(k/x). Si se tiene la confianza suficiente en la protección de la capa de enlace y en la inviolabilidad del sistema del cliente, puede omitirse la protección adicional mediante t en el nivel de la aplicación.

A través de los siguientes ejemplos, debería entenderse que cuando se aplica la protección al nivel de aplicación, puede haber opcional/alternativamente un módulo AKA DRM-interno (indicado por líneas de trazos), que funciona preferentemente en base a una clave x especifica de DRM.

Para un módulo DRM distribuido, con un primer agente DRM en el módulo de identidad y un segundo agente DRM en el dispositivo de uso, puede ser conveniente, especialmente cuando el dispositivo de uso está en un dispositivo autónomo, configurar de manera inviolable el módulo de identidad y el dispositivo de uso con información de clave específica del dispositivo de uso, para permitir la comunicación entre los dos agentes DRM en base a esta información de la clave del dispositivo. La información de la clave del dispositivo puede ser una clave secreta compartida, o un par de claves asimétricas, permitiendo la autenticación y/o la protección de información comunicada entre los agentes DRM. Normalmente, la clave del dispositivo está almacenada de manera inviolable en el dispositivo de presentación, y puede utilizarse la infraestructura del operador de red y/o de una parte de certificación fiable con objeto de transferir de manera segura la información de la clave del dispositivo correspondiente para su almacenamiento en el módulo de identidad inviolable, tal como se describirá a continuación haciendo referencia a la figura 9.

La figura 6 ilustra un ejemplo de un módulo DRM distribuido con comunicación entre los agentes DRM distribuidos, en base a una clave específica del dispositivo de uso, de acuerdo con una realización preferida de la invención. De manera similar a la estructura básica de la figura 5, el módulo 120 de identidad comprende un módulo 122 AKA y un primer agente 125 DRM, y el dispositivo de uso, ilustrado en este caso como un dispositivo 130 de presentación, comprende un procesador 131 de medios y un segundo agente 135 DRM. Los agentes 125, 135 DRM pueden estar implementados en equipamiento físico, soporte lógico o una combinación de los mismos.

En el ejemplo concreto de la figura 6, que se refiere a autenticación y/o cifrados simétricos, tanto el módulo 120 de identidad como un dispositivo 130 de presentación están configurados con una clave específica, y, del dispositivo de presentación (o, de forma más general, del dispositivo de uso), secreta, compartida. En el ejemplo de realización, la clave compartida, y, del dispositivo está implementada en los agentes 125, 135 DRM de las entidades involucradas. Esta es una solución perfectamente válida, por ejemplo cuando el agente 135 DRM del dispositivo de presentación está implementado como un circuito de equipamiento físico. Sin embargo, puede ser beneficioso realizar una implementación inviolable de la clave, y, del dispositivo fuera del agente DRM del dispositivo de presentación, especialmente cuando el agente DRM del dispositivo de presentación es una aplicación basada en soporte lógico. En este caso, la clave, y, del dispositivo está preferentemente almacenada en el dispositivo de presentación en el interior de un entorno inviolable especial, tal como un circuito de seguridad dedicado (tal como se indica por la caja de trazos que contiene "y" en la figura 6).

El canal de comunicación entre los dos agentes DRM está preferentemente autenticado y/o protegido en base a la clave del dispositivo, y, o posiblemente a una representación de la clave del dispositivo. En el caso de comunicación autenticada, tal como se ilustra en la figura 7A, el agente DRM en el módulo de identidad puede autenticar que está en contacto con un dispositivo de uso que tiene un agente DRM inviolable válido. Más en concreto, el primer agente 125 DRM autentica el dispositivo de uso para verificar que éste incluye un agente 135 DRM válido, por ejemplo uno que aplique apropiadamente las normas de uso asociadas con el contenido. Preferentemente, se lleva a cabo una autenticación explícita utilizando un procedimiento pregunta-respuesta basado en la clave del dispositivo, y. La comunicación entre los agentes DRM distribuidos puede alternativamente, o como complemento, estar cifrada o protegida de otro modo, tal como se ilustra en la figura 7B. A continuación, el agente 125 DRM en el módulo de identidad 120 podría basarse en autenticación implícita, es decir solamente un dispositivo 130 de presentación que implemente la clave, y, puede descifrar datos DRM cifrados mediante la clave, y, del dispositivo. Aunque la comunicación basada en la clave del dispositivo es especialmente útil cuando el dispositivo de presentación es un dispositivo "autónomo", debe entenderse que la comunicación con la clave del dispositivo es aplicable asimismo a un dispositivo cliente, tal como un teléfono móvil, con su propia aplicación de presentación integrada, emparejando de ese modo el módulo de identidad al propio teléfono móvil.

La comunicación basada en la clave del dispositivo entre el módulo de identidad inviolable y el dispositivo de presentación puede ser utilizada para transferir datos DRM, tales como claves de protección de contenidos, información relativa al proceso de uso de contenidos, e incluso aplicaciones/actualizaciones DRM entre dos nuevas entidades.

Si el dispositivo de presentación es un dispositivo autónomo, se recomienda que tenga su propia aplicación de normas DRM y que las normas de uso sean enviadas en el ticket junto con el medio, o reenviadas desde el agente DRM del módulo de identidad, de manera que el dispositivo de presentación pueda actuar como un agente en nombre del proveedor/propietario del contenido y corroborar que se cumplen las normas de uso.

La figura 8 ilustra una implementación preferida de un módulo DRM distribuido, con comunicación basada en la clave del dispositivo entre un agente DRM en un módulo de identidad inviolable y un agente DRM en un dispositivo de presentación. Más específicamente, la figura 8 ilustra cómo una clave s de protección de un medio o de un contenido puede enviarse cifrada entre el agente DRM del módulo de identidad y el agente DRM del dispositivo de presentación, con un nivel mayor de seguridad para la propia clave del dispositivo. Aunque es posible implementar el módulo de identidad con un caso de la clave, y, del dispositivo, y cifrar la clave s de protección del contenido directamente mediante la propia clave, y, del dispositivo, normalmente es recomendable determinar otra clave y' derivada de la clave, y, original del dispositivo y transferir de manera segura la clave determinada y' al módulo de identidad para su uso en la provisión de comunicación segura/autenticada entre los agentes DRM distribuidos. De este modo, no es necesario almacenar la propia clave, y, del dispositivo en el módulo de identidad.

Haciendo referencia a la figura 8, el agente 125 DRM del módulo de identidad 120 comprende dos unidades criptográficas C1 y C3 separadas lógicamente. La unidad criptográfica C1 es similar a la de la figura 5, y la unidad criptográfica C3 está configurada para cifrar la clave de protección s mediante la clave y', antes de su transmisión al dispositivo 130 de presentación. En este caso se asume que la representación y' de la clave del dispositivo ha sido implementada en el módulo de identidad, y más en concreto en el agente 125 DRM. La clave y' puede obtenerse, por ejemplo, mediante una parte de certificación fiable, utilizando la clave, y, secreta del dispositivo (o una representación de la misma) y una pregunta r como entrada en una función criptográfica C', y transferirse de forma segura para su almacenamiento en el módulo de identidad, tal como se explicará más adelante con mayor detalle.

Para poder realizar comunicaciones basadas en "claves de dispositivo" entre los dos agentes DRM, el dispositivo de presentación debe ser capaz de determinar la información y' de la clave del dispositivo. A este respecto, el dispositivo 130 de presentación está preferentemente equipado con un circuito 133 de seguridad inviolable, que incluye tanto la clave, y, del dispositivo como una función criptográfica C'' (correspondiente a la función C') que determina y' en respuesta a la pregunta r y a la clave interna, y, del dispositivo. De este modo, la clave, y, del dispositivo nunca tiene que salir del entorno controlado del circuito de seguridad inviolable, y se mantiene un nivel de seguridad alto de la clave del dispositivo incluso con un agente DRM basado en soporte lógico en el dispositivo de presentación.

La pregunta, r, es transferida preferentemente desde la parte de certificación fiable al módulo de identidad, quizás en el momento en que y' es transferida al módulo de identidad e implementada en el mismo, o después, por ejemplo cuando el contenido cifrado y/o un ticket correspondiente son transferidos al módulo de identidad. Finalmente, la pregunta r puede ser almacenada en el módulo de identidad. A continuación, la pregunta r es transmitida, posiblemente junto con la clave de protección del contenido cifrado, s, al segundo agente 135 DRM del dispositivo 130 de presentación. El agente 135 DRM del dispositivo 130 de presentación invoca el circuito 133 de seguridad reenviando la pregunta r, y el circuito de seguridad responde reenviando al agente 135 DRM la representación y' de la clave del dispositivo. El agente 135 DRM del dispositivo 130 de presentación incluye asimismo una unidad criptográfica C4 para descifrar la clave cifrada s utilizando la clave generada y', y una unidad criptográfica C2 para descifrar el contenido del medio cifrado utilizando la clave descifrada s. Finalmente, el contenido digital es enviado al procesador 131 de medios para su presentación. La clave y' puede ser considerada una clave de sesión que es única para cada sesión de comunicación entre el agente DRM del módulo de identidad y el agente DRM del dispositivo de presentación. Por supuesto, en el módulo DRM distribuido de la figura 8 puede implementarse asimismo un protocolo de autenticación pregunta-respuesta explícito, basado en la clave, y, del dispositivo o en la representación y' de la clave del dispositivo.

La figura 9 es un diagrama de flujo esquemático de un método de gestión de derechos digitales para establecer comunicación basada en claves de dispositivo entre agentes DRM distribuidos. El dispositivo de presentación está configurado de manera inviolable con una clave, y, especifica del dispositivo de uso (S10).

Puesto que la clave, y, del dispositivo es especifica del dispositivo de presentación, el cliente (el módulo de identidad) puede establecer una relación de confianza con dicho dispositivo, en particular la primera vez, cuando el dispositivo de presentación es nuevo. Obsérvese que no es seguro escribir simplemente "y" en el exterior del dispositivo de presentación, puesto que podría copiarse y podría crearse fácilmente un dispositivo clonado, no seguro. En cambio, puede unirse información de identificación, tal como el resultado de aplicar alguna función criptográfica h a la clave, y, a una "etiqueta" en el dispositivo de presentación cuando éste es vendido, o ser transferida desde el dispositivo de presentación al dispositivo cliente asociado cuando se interconectan, realizando por lo tanto una representación criptográfica de la clave del dispositivo disponible para un usuario/el dispositivo cliente (S11). La representación criptográfica del dispositivo puede, por ejemplo, involucrar un cifrado asimétrico o simétrico de función criptográfica unidireccional. El dispositivo está asociado con una clave, y, del dispositivo secreta, aleatoria, y cuando el comprador desea activar el dispositivo, envía la representación h(y) criptográfica (abierta), o información de identificación similar, al operador (o a otra parte de certificación fiable), quien verifica que h(y) está asignada a un dispositivo válido, recibe la clave del dispositivo (S12) o información de clave adecuada, tal como y', derivada de la clave del dispositivo, y finalmente actualiza (S13) la aplicación DRM del módulo de identidad con la clave, y, del dispositivo o con información de la clave derivada de ésta.

Se asume que el operador u otra parte de certificación fiable (en algunos modelos comerciales, la parte fiable puede ser el fabricante del dispositivo) tiene alguna clave que le permite invertir la función h, o que de lo contrario es capaz de recibir información adecuada de la clave del dispositivo, por ejemplo utilizando tablas de consulta (S12). Por ejemplo, puede ser el caso que la propia clave del dispositivo no deba nunca estar disponible en el exterior del dispositivo de presentación, ni ser conocida explícitamente por la parte de certificación. En este caso, la parte de certificación es capaz de recibir información de la clave, tal como y', que se basa en la propia clave, y, del dispositivo y quizás datos de entrada adicionales.

Asimismo, se asume que la información de la clave del dispositivo se transfiere de manera segura desde la parte de certificación al módulo de identidad del dispositivo cliente, en base a alguna clave específica del módulo de identidad (S13). Una vez configurado apropiadamente el agente DRM del módulo de identidad, la información de la clave del dispositivo, es decir la clave del dispositivo o alguna otra clave derivada de la clave del dispositivo, puede ser utilizada para establecer la comunicación (segura y/o autenticada) con el agente DRM en el dispositivo de presentación (S14). Aparentemente, si una clave derivada de la propia clave, y, del dispositivo es transferida al módulo de identidad e implementada en el mismo, el dispositivo de presentación tiene que implementar alguna función que, basada en la clave del dispositivo, genere la misma clave derivada que hay en el módulo de identidad.

El valor, y, puede ser verificado por la parte de certificación para verificar que en el sistema se utilizan solamente dispositivos de presentación "auténticos" (es decir, no robados, pirateados o comprometidos de otro modo), con valores, y, "válidos". Si un usuario compra un nuevo dispositivo de presentación, puede añadir soporte (una nueva

clave en su modelo de identidad) para el dispositivo de una manera sencilla. Esto puede utilizarse para el registro, en el módulo de identidad (así como en una tercera parte de registro), de varios dispositivos de presentación con los cuales el cliente (módulo de identidad) desea establecer relaciones fiables.

En DRM, existe frecuentemente una necesidad de "uso leal", es decir, si el usuario compra contenido, debe permitirse a éste utilizarlo en cualquier dispositivo (compatible DRM) registrado satisfactoriamente en su "dominio local" (por ejemplo, un dominio familiar). Sin embargo, existe el riesgo de que diferentes usuarios a lo largo del mundo formen un "dominio virtual global" de manera que el contenido pueda compartirse más o menos globalmente de cualquier modo. La presente invención puede limitar el riesgo de dicha dispersión global del contenido. Puesto que el registro del dispositivo está basado en un módulo de identidad, asociado a un usuario o a una suscripción, es posible que la parte fiable (por ejemplo, el operador) que gestiona los requisitos del registro verifique que se permite un nuevo dispositivo en un cierto dominio. Por ejemplo, si tres miembros de una familia tienen suscripciones con el mismo operador (o con operadores diferentes bajo un acuerdo contractual), el operador puede verificar que si un dispositivo ha sido ya registrado, lo fue mediante un usuario que pertenece al mismo dominio. Tras un registro satisfactorio, el operador autoriza que el dispositivo se registre en el nuevo módulo de identidad, por ejemplo enviando claves específicas del dispositivo u otra información.

Debe entenderse que la respuesta de enviar la clave de identificación "etiquetada" a la parte de certificación puede ser cualquier representación de la clave del dispositivo que permita al agente DRM comunicar con el agente DRM del dispositivo de presentación.

La propia información de la clave utilizada para la comunicación entre los agentes DRM distribuidos puede ser la misma independientemente de qué módulo de identidad sea utilizado. Sin embargo, alternativamente la información de la clave utilizada para la comunicación autenticada y/o segura se hace dependiente de la clave del dispositivo de uso así como del módulo de identidad concreto que está actualmente asociado al dispositivo de presentación. De este modo, diferentes terminales cliente (que tienen cada uno su propio módulo de identidad) asociados con el mismo dispositivo de presentación, pueden tener información de la clave del dispositivo única.

De hecho, esto representa un caso especial de enviar una clave obtenida a partir de la clave, y, del dispositivo en lugar de enviar la propia clave del dispositivo, desde la parte de certificación fiable al módulo de identidad. Igual que antes, la representación criptográfica h(y) de la clave, y, del dispositivo es enviada al operador (o a otra parte de certificación fiable) que verifica que h(y) esté asignada a un dispositivo válido. A continuación el operador genera, por ejemplo, un valor b que depende de una clave específica del módulo de identidad, tal como k y/o x, y finalmente genera una representación y'' de la clave del dispositivo basada en el valor b generado y en la clave, y, del dispositivo:

$$b = \text{función } (k/x),$$

$$y'' = \text{función } (b, y).$$

Preferentemente, los valores b e y'' son transferidos de forma segura desde el operador al módulo de identidad. La representación y'' de la clave del dispositivo (y, posiblemente, asimismo b) es almacenada de forma segura en el módulo de identidad, y el valor b es transferido al dispositivo de presentación (posiblemente, junto con una identificación del módulo de identidad). El dispositivo de presentación, que está configurado con un caso de la misma función que el operador para generar la representación y'' de la clave del dispositivo, calcula y'' basándose en b y en la clave interna, y, del dispositivo. A continuación, la representación y'' de la clave del dispositivo puede ser utilizada para la comunicación entre el módulo de identidad y el dispositivo de presentación, en analogía con la realización de la figura 8.

Si no se desea una dependencia rígida con k/x, el valor b podría simplemente ser un numero aleatorio u otro valor generado o asignado por el operador, o parte correspondiente. Asimismo, debería entenderse que la clave del dispositivo en el dispositivo de presentación podría ser alternativamente una clave privada, conteniendo el módulo de identidad una copia de la clave pública correspondiente.

Tal como se ha descrito previamente, el agente DRM del módulo de identidad puede configurarse para reunir información sobre el proceso de uso del contenido digital, que puede ser utilizada como base para el cobro. Sin embargo, para un módulo DRM distribuido con un primer agente DRM en el módulo de identidad y un segundo agente DRM en el propio dispositivo de presentación, esta información de uso es reunida habitualmente por el agente DRM del dispositivo de presentación. El segundo agente DRM compila información cuando el dispositivo de presentación consume el contenido digital, y envía la información al primer agente DRM, preferentemente utilizando la comunicación autenticada y/o segura basada en la clave del dispositivo. Por ejemplo, es beneficioso utilizar la clave del dispositivo para proteger la integridad de la información compilada. El primer agente DRM autentica y/o descifra la información compilada en base a la información de la clave del dispositivo correspondiente, y almacena la información en un registro y/o envía la información a una parte fiable externa para su registro. Preferentemente, el

primer agente DRM protege la integridad y/o cifra la información de registro antes de transferirla a la parte fiable externa, utilizando criptografía simétrica o asimétrica. A continuación puede ser utilizada la información de registro, por ejemplo con propósitos de no rechazo.

En un protocolo de comunicación más elaborado, el primer agente DRM y el segundo agente DRM intercambian señales de control para controlar el proceso de presentación, o más en general el proceso de uso. Por ejemplo, el segundo agente DRM del dispositivo de presentación genera intermitentemente una señal de acuse de recibo ACK que indica que el proceso de utilización del contenido digital recibido prosigue sin alteraciones. Preferentemente, la señal ACK se acompaña de información de registro, por ejemplo relacionada con la cantidad del tiempo de presentación, la cantidad de datos presentados satisfactoriamente, la calidad de la presentación, retardos temporales, desbordamientos de memoria intermedia, y otros datos relacionados con el proceso de presentación. El primer agente DRM incluye funcionalidad para procesar la información de esta señal y para enviar en respuesta una denominada señal de seguir adelante FPS (forward proceed signal) al segundo agente DRM. La señal FPS se requiere para que el proceso de presentación continúe, mientras que la ausencia de una señal FPS provoca que el proceso de presentación se detenga o prosiga de acuerdo con limitaciones predeterminadas, por ejemplo una calidad de servicio (QoS, Quality of Service) limitada. La señal FPS puede incluir información, tal como un código de acceso del dispositivo (DAC, Device Access Code) extraído del ticket correspondiente por el primer agente DRM, o información obtenida analizando los datos de registro recibidos del segundo agente DRM, que puede ser utilizada para controlar el proceso de presentación. Por lo tanto, el segundo agente DRM está configurado para recibir la señal FPS y para controlar el proceso de presentación dependiendo de los datos asociados con la señal FPS. Este tipo de protocolo de comunicación puede ser particularmente útil en las denominadas aplicaciones de difusión, en las que la información de registro procedente del segundo agente DRM sirve como base para el cobro. Si el primer agente DRM no recibe dicha información de registro, el primer agente DRM es capaz de controlar mediante la señal FPS el proceso de presentación continuado.

El primer agente DRM puede, asimismo, ser capaz de extraer del ticket las normas de uso asociadas con el contenido digital y reenviar estas normas al dispositivo de presentación para su aplicación mediante el segundo agente DRM. Sin embargo, alternativamente estas normas de uso son enviadas directamente, preferentemente junto con el contenido digital cifrado, al dispositivo de presentación y al agente DRM que éste contiene.

Este protocolo de comunicación utiliza preferentemente la comunicación descrita anteriormente basada en la clave del dispositivo, en la que se realiza autenticación y/o cifrado en base a información de la clave específica del dispositivo de uso.

De manera similar al agente DRM implementado como una aplicación en un entorno de aplicaciones dentro del módulo de identidad, el agente DRM del dispositivo de presentación puede implementarse asimismo como una aplicación de soporte lógico, preferentemente en un entorno de aplicación inviolable en el dispositivo de presentación. Esto significa que una aplicación DRM adaptada para ser utilizada en un dispositivo de presentación puede ser descargada al entorno de aplicaciones del dispositivo de presentación a través de un operador de red y del módulo de identidad asociado (con su agente DRM), o bien más o menos directamente desde un proveedor de contenidos o parte correspondiente, en base a información de la clave específica del dispositivo de uso.

Debe observarse que la "descarga" de agentes DRM es posible asimismo cuando un dispositivo no tiene su propio medio de comunicación de salida. Considérese, por ejemplo, un receptor de TV y un descodificador. Para actualizar la TV y/o el descodificador con nueva funcionalidad DRM, se puede proceder como sigue. Utilizando un dispositivo de comunicación separado, por ejemplo un teléfono, el usuario encarga un agente DRM. Si es necesario, se introducen datos específicos del dispositivo que permiten al operador configurar el agente DRM para el dispositivo, por ejemplo cifrándolo con claves específicas del dispositivo. A continuación, el agente DRM es transportado al dispositivo asignando ancho de banda al canal de difusión. Por ejemplo, en el caso de un receptor de TV, el agente DRM podría ser transportado codificándolo en el canal de información de teletexto. Para radio, puede utilizarse el canal de información RDS. Si el agente DRM se cifra con las claves específicas del dispositivo, no importa que el medio de difusión sea interceptado fácilmente.

Para asegurar una autenticación apropiada del agente DRM en el dispositivo de presentación cuando se descarga un agente DRM o una nueva versión actualizada de dicho agente DRM, la información de la clave del dispositivo original (actual) debería preferentemente ser sustituida por nueva información de la clave del dispositivo que esté asociada con el agente DRM descargado. Habitualmente, esto implica que la información de la clave del dispositivo esté almacenada en una memoria regrabable, por ejemplo en un circuito de seguridad inviolable dotado de una memoria regrabable, en un entorno de aplicaciones del dispositivo de presentación inviolable o en una memoria accesible desde dicho entorno de aplicaciones.

Preferentemente, el agente DRM y un valor de reinicialización asociado con el mismo son descargados de manera segura (cifrados y/o autenticados) al entorno de aplicaciones del dispositivo de presentación en base a la clave del dispositivo original (actual). La clave original del dispositivo, aquí denominada y_1, junto con el valor de reinicialización re-init, autenticado preferentemente en base a la clave del dispositivo original, son utilizados como entrada a una

función criptográfica, f', para generar una nueva clave del dispositivo, denominada y_2, que sustituye a continuación la clave y_1 original del dispositivo en la memoria regrabable.

$$y_2 = f' (y_1, \text{re-init}).$$

Por ejemplo, el valor de reinicialización re-init puede ser generado por un operador de red, un proveedor de contenidos o una parte de certificación fiable, parte que utiliza la misma función f' y la misma entrada y_1 y re-init para generar una nueva clave y_2 del dispositivo. Si el agente DRM y el valor de reinicialización re-init son transferidos al dispositivo de presentación a través de un operador de red y el módulo de identidad asociado, y el agente DRM del módulo de identidad está configurado con una copia de la función f' y la clave original y_1 del dispositivo, la nueva clave y_2 del dispositivo puede ser generada directamente en el módulo de identidad, sustituyendo la información de la clave original del dispositivo. Alternativamente, tal como se ha descrito previamente para la clave original del dispositivo, la nueva clave del dispositivo o una representación de la misma pueden ser transferidas de forma segura desde la parte de certificación al módulo de identidad en base a la clave específica del módulo de identidad, tal como una clave k de suscripción.

A continuación, puede ser utilizada la información de la nueva clave del dispositivo, por ejemplo para comunicación entre agentes DRM en el sistema cliente, o cuando posteriormente se descargue un agente DRM aún más nuevo al entorno de aplicaciones del dispositivo de presentación.

En general, puede haber otras circunstancias que requieran la sustitución de la clave del dispositivo, por ejemplo si la clave, y, del dispositivo está en peligro. El fabricante del dispositivo o alguna otra parte fiable pueden tener acceso al código de acceso del dispositivo (DAC), el cual cuando es aplicado al dispositivo permite la sustitución (autenticada) de la clave del dispositivo. Sin embargo debe entenderse que la sustitución de la clave del dispositivo en el dispositivo de presentación no forma parte, en general, de las rutinas cotidianas normales para la gestión de derechos digitales, y que la sustitución de la clave del dispositivo implica asimismo, habitualmente, procedimientos administrativos tales como actualizar bases de datos de clave/identificación del dispositivo.

Si el dispositivo de presentación va a ser transferido a otro usuario que tiene su propio terminal cliente tal como un móvil o un PC, se realiza normalmente el "procedimiento de registro" descrito previamente para transferir la información de la clave del dispositivo correspondiente al módulo de identidad del nuevo terminal del cliente. Tal como se ha mencionado, normalmente es mejor registrar información de la clave derivada de la clave del dispositivo en lugar de la propia clave del dispositivo, de manera que la clave del dispositivo, y, no esté presente en todos y cada uno de los terminales clientes utilizados con el dispositivo de presentación. De cualquier modo, es ventajoso revocar o invalidar de otro modo la información de la clave del dispositivo en terminales de usuario que ya no vayan a ser utilizados con dicho dispositivo de presentación. Existen diferentes maneras de tratar este problema. Por ejemplo, puede ser actualizada la clave, y, de dispositivo en el dispositivo de presentación, de manera que los terminales "antiguos" dejan de poder ser utilizados con el dispositivo. Esto podría ser realizado por un punto de servicio autorizado, o de forma remota sobre una red. Alternativamente, la información de la clave del dispositivo del módulo de identidad puede ser borrada por una parte fiable tal como un operador de red, por ejemplo mediante la utilización de un código de acceso específico del módulo de identidad que permita el borrado de la clave del dispositivo y/o autenticando que el comando ”borrar” procede de la parte fiable.

Por otra parte, tal como se ha mencionado previamente, podría haber casos en los que se desea realmente que el mismo dispositivo pueda ser utilizado por dos (o varios) diferentes módulos de identidad/terminales de usuario.

Asimismo, se admite que la utilización de "claves" en el interior de los dispositivos podría ser utilizada con propósitos antirrobo: sin conocer la clave, el dispositivo es inútil, y si alguien intenta configurar un dispositivo, éste podría ser comprobado contra un registro de dispositivos robados.

En un entorno de aplicaciones más abierto, la inviolabilidad del dispositivo de presentación y su funcionalidad DRM pueden proporcionarse en base al concepto de seguridad por oscuridad, escribiendo el código de soporte lógico y las claves asociadas de manera complicada, oscura, para hacer extremadamente difícil que una parte externa comprenda el código, e incluso aún más difícil distinguir claves de seguridad entre el resto del código.

Además de los aspectos de seguridad discutidos anteriormente, normalmente se requiere realizar el propio descifrado del contenido digital en el agente DRM del dispositivo de presentación, debido a la capacidad limitada de procesamiento de los actuales módulos estándar de identidad. Sin embargo, con la capacidad de procesamiento incrementada en los módulos de identidad, por ejemplo en la futura generación de módulos de identidad tales como futuras tarjetas UICC, puede ser factible integrar el descifrado del contenido en el agente DRM del módulo de identidad, tal como se ilustra en la figura 10. No obstante, esta realización se refiere típicamente al caso de un dispositivo cliente, tal como una unidad móvil, con su propia aplicación de presentación integrada, con requisitos de seguridad algo más relajados en relación con la gestión de derechos digitales. En el ejemplo de la figura 10, el módulo 120 de identidad comprende una unidad criptográfica C1 para generar la clave s de protección del medio, y

una unidad criptográfica C2 para descifrar el contenido del medio cifrado, utilizando la clave s de protección procedente de la unidad criptográfica C1. A continuación, el contenido del medio descifrado es enviado al dispositivo 130 de presentación para su procesamiento y presentación. Si se requiere aplicación de normas, funcionalmente dicha aplicación de normas puede implementarse asimismo en el agente DRM del módulo de identidad. Por lo tanto, es evidente que la invención no siempre requiere una funcionalidad DRM distribuida.

Para una comprensión más completa de la invención, a continuación se describirá una solución DRM a modo de ejemplo haciendo referencia a las figuras 11 y 12, que muestran esquemáticamente el protocolo DRM en general y un correspondiente diagrama de bloques del lado del cliente, respectivamente.

Tal como se ha mencionado, en una solución DRM, parte del proceso DRM debe tener lugar normalmente en un dispositivo inviolable, preferentemente un módulo de identidad inviolable. Para una comprensión más detallada de la invención, el ejemplo de las figuras 11 y 12 se referirá a un módulo de identidad de abonado de red tal como una tarjeta GSM SIM, USIM, WIM, ISIM, en adelante denominado simplemente un SIM. Típicamente, se descarga un contenedor que comprende una o varias claves y/o datos, y estas una o varias claves/datos tienen que ser procesadas en un entorno protegido. En este caso, el comportamiento del proceso podría estar especificado completamente por un SAT/USAT o aplicación correspondiente, posiblemente interactuando con los algoritmos de autenticación/generación de claves preexistentes en la tarjeta, reutilizando la relación operador-abonado. Utilizar SAT en este contexto no es lo mismo que utilizar un "verdadero" módulo inviolable, pero es más seguro que realizar el proceso en un entorno PC abierto y quizás incluso hostil, y más flexible que utilizar módulos inviolables cableados. Si se encuentra un defecto de seguridad, la tarjeta es actualizada fácilmente (incluso de forma inalámbrica) mediante un nuevo conjunto de algoritmos de proceso DRM.

En este ejemplo, se asume que la tarjeta SIM 120 (figura 12) contiene k, la clave de abonado usual. El SIM contiene asimismo un entorno de aplicaciones (por ejemplo, SAT/USAT) que está prefabricado con una aplicación DRM, o alternativamente, la aplicación DRM es descargada de forma segura (cifrada y autenticada). Asimismo, en el SIM y en el operador está presente una segunda clave, x, específica para propósitos DRM. Igual que k, x está asimismo almacenada de manera que no puede ser leída fuera de la tarjeta SIM. Obsérvese no obstante que x puede ser almacenada en soporte lógico, por ejemplo como parte de la aplicación DRM, si puede garantizarse la suficiente protección. Además del operador de red, existe un proveedor de contenidos que, si es distinto al operador, tiene un acuerdo contractual con el operador, manifestado por una clave compartida c.

En primer lugar, y opcionalmente, cada vez que se invoca el agente DRM en el SIM, la aplicación verifica que está funcionando en un entorno fiable, por ejemplo mediante un protocolo de autenticación mutua. Este protocolo podría basarse en el conocimiento de la clave x, o en alguna otra información compartida entre el SIM y el dispositivo de presentación con el que está relacionado el SIM, por ejemplo otra clave y. Esto puede ser deseable en casos en que el SIM entero puede ser desplazado entre dispositivos, en cuyo caso existe una sola clave, y, para que cada dispositivo con el que se utiliza el SIM.

Cuando el usuario ha decidido qué medio quiere (y posiblemente ha pagado por él, si el pago no se realiza después de la sesión o durante la misma), notifica al operador de red que desea utilizar la aplicación DRM, y el operador lleva a cabo autenticación y gestión de claves utilizando una pregunta aleatoria RAND, otros datos de usuario opcionales, la clave x y opcionalmente asimismo la clave k. Opcionalmente, está autenticación podría haberse realizado antes, por ejemplo cuando se obtiene acceso a la red. La clave k se utiliza cuando es necesario o apropiado ligar la generación de la clave a la suscripción como tal. Este AKA se realiza utilizando algunas funciones criptográficas f y g las cuales, en caso de que se desee dependencia asimismo con k, pueden consistir parcialmente en algoritmos de autenticación SIM normal.

En otras palabras, el operador envía RAND (y opcionalmente [datos_de_usuario], si no son ya conocidos por las aplicaciones DRM del SIM) al SIM (ver (1) en la figura 12). Preferentemente, la información enviada es autenticada, por ejemplo mediante una clave derivada de k y/o x de manera similar. Los datos son recibidos por la aplicación DRM en el SIM, el cual, si está presente una etiqueta de autenticación, autentica primero los datos recibidos, y después ejecuta las mismas funciones f y g para obtener la clave de sesión, t y la respuesta, RES, respectivamente. La respuesta es devuelta al operador, de manera que el operador puede verificar que está en contacto con la aplicación correcta. A continuación, la aplicación realiza un encargo (protegido por la clave t) al operador, sobre qué medios y qué derechos desea obtener. Habitualmente, el encargo es generado por una aplicación de navegador en el dispositivo. Obsérvese que en este caso la aplicación de navegador es, asimismo, una aplicación fiable y autenticada, o el usuario debe recibir la posibilidad de confirmar el encargo realizado. El operador devuelve una clave s de sesión, junto con un ticket que describe el medio encargado y los derechos. La clave de sesión es para ser utilizada posteriormente para la protección del propio medio. El ticket y la clave s de sesión son enviadas por duplicado. Uno está protegido por la clave c (conocida solamente por el proveedor de contenidos y el operador), y la otra está protegida por la clave t (conocida solamente por el cliente y el operador). El cliente descifra el ticket y la clave s y verifica que el ticket corresponde al encargo realizado anteriormente.

A continuación, la clave s puede ser entregada a otra aplicación 130 (figura 12) en el dispositivo cliente (no necesariamente en el propio SIM), o a un dispositivo externo 130 completamente autónomo en el sistema cliente global, que utilizando la clave s descifra posteriormente el medio recibido y lo presenta al usuario. Obsérvese que puede darse el caso de que la propia presentación/descifrado se realicen en otro módulo inviolable diferente al SIM. En ese caso, tal como se ha mencionado anteriormente, puede ser aconsejable establecer una comunicación basada en la clave del dispositivo, entre el dispositivo y la aplicación DRM SIM, de manera que s pueda enviarse cifrada entre el SIM y el dispositivo (ver (2) en la figura 12), utilizando alguna de las soluciones propuestas anteriormente. Tal como se ha discutido anteriormente, esto habilita asimismo la aplicación SIM para autenticar que está en contacto con un dispositivo inviolable con funcionalidad DRM válida. El SIM podría basarse en autenticación implícita (es decir, solamente un dispositivo que conoce la clave y/y' del dispositivo puede descifrar la clave s de sesión), o llevar a cabo autenticación explícita en base a la clave y/y'. Si es deseable "ocultar" la propia clave, y, del dispositivo y en su lugar obtener una representación y' de la clave del dispositivo a utilizar para el cifrado, el descifrado y/o la autenticación, la pregunta común r ha de ser transferida desde la parte fiable al SIM y asimismo al dispositivo de presentación. Si el dispositivo 130 de presentación es "autónomo" se recomienda que tenga su propia aplicación de normas y reciba las normas de uso, por ejemplo en el ticket junto con el medio, de manera que pueda actuar como agente a favor del propietario/proveedor de contenidos e imponer el seguimiento de unas normas de uso. La aplicación de normas podría implementarse alternativamente en el SIM, o ser distribuida entre el SIM y el dispositivo de presentación.

A continuación, el cliente envía el ticket y la clave de sesión s (aún protegida por la clave c) al proveedor de contenidos (ver (3) en la figura 12). El proveedor de contenidos elimina la protección y extrae la clave s. Si esto es satisfactorio, el proveedor de contenidos sabe que el ticket se originó en un operador con el cual tiene un acuerdo. Si se requieren cualesquiera mensajes de configuración entre el cliente y el proveedor de contenidos antes del envío del medio, este tráfico se protege por medio de la clave s (o alguna otra clave derivada de s). Finalmente, el proveedor de contenidos cifra el medio mediante la clave s de sesión, y lo envía (lo descarga o lo emite en tiempo real) al dispositivo de presentación (ver (4) en la figura 12).

Asimismo, es posible permitir al dispositivo de presentación autenticar que la clave s de protección del medio procede realmente de un SIM que ha sido emparejado con el dispositivo de presentación a través de la información de la clave del dispositivo, y y/o y'.

Por supuesto, el anterior protocolo basado en ticket no es el único posible; existen muchas variaciones tal como apreciarán fácilmente los expertos en la materia.

La invención encaja asimismo en la versión actual del estándar emergente OMA (conocido anteriormente como estándar WAP/WAP-DRM). El protocolo de aplicación inalámbrica (WAP) está estandarizado por OMA/WAP-Forum. Actualmente existe trabajo en curso para obtener un modo de aplicar DRM en el ámbito de WAP [10, 11]. Actualmente, el trabajo de estandarización está dirigido principalmente a la descarga.

La solución WAP separa la descarga del medio de un objeto DRM en dos partes: el objeto del medio y los derechos del objeto. La descarga puede llevarse a cabo utilizando uno de tres métodos definidos:

- Bloqueo de reenvío: el cliente descarga solamente del objeto del medio. El objeto del medio tiene ciertos derechos por defecto simples, por ejemplo un "objeto de visión previa", y no puede ser reenviado a otro usuario.

- Descarga combinada: el cliente descarga tanto el objeto del medio como el objeto de derechos.

- Distribución separada: el cliente descarga el objeto del medio, que está cifrado con una clave CEK (Content Encryption Key, clave de cifrado de contenidos). Posteriormente (o simultáneamente), pueden pasarse al cliente el objeto de derechos y la CEK.

Se asume que el cliente es una entidad autorizada, es decir, el dispositivo en el que éste reside puede confiar en que el cliente procede de manera correcta, y cumple con cualesquiera derechos impuestos por un objeto de derechos. Ninguna entidad no autorizada, por ejemplo un editor de texto o un juego que esté instalado en el dispositivo, tiene acceso a los objetos DRM en forma no cifrada (posiblemente, ni siquiera en forma cifrada).

El cliente DRM WAP definido en [10, 11] puede implementarse como una aplicación en un entorno de aplicaciones de un módulo de identidad inviolable, tal como se ha descrito anteriormente. Sin embargo, el estándar WAP-DRM asume que el dispositivo de presentación de medios y el cliente de descarga residen ambos en la misma entidad física. Esta limitación puede relajarse sin violar el estándar WAP-DRM mediante el recurso de configurar el dispositivo de presentación y la aplicación DRM del módulo de identidad mediante una clave secreta compartida, y, (o un par de claves asimétricas configuradas adecuadamente) de manera que la clave CEK pueda enviarse de forma protegida entre el módulo de identidad y el dispositivo de presentación.

Los modelos de Bloqueo de reenvío y de Descarga combinada especifican que el medio y los derechos son descargados al cliente DRM. Según la invención, el objeto de derechos puede incluirse en el ticket, y el objeto del medio puede ser descargado al dispositivo de presentación. A este respecto, obsérvese que no existe diferencia real entre descarga y emisión en tiempo real. En las referencias [10, 11], que están dirigidas principalmente a descarga, existe una sugerencia para llevar a cabo emisión en tiempo real descargando una descripción SDP de la emisión en tiempo real en el objeto del medio, y utilizar a continuación dicha descripción para configurar la sesión de emisión en tiempo real. No plantea ningún problema incorporar esto a la solución propuesta por la invención, simplemente se pasa la descripción SDP dentro del ticket. Para información sobre SDP, se hace referencia a [12]. Preferentemente, el cliente DRM implementado en el entorno de aplicaciones del SIM incluye asimismo funcionalidad para verificar que no se viola la función de bloqueo de reenvío del protocolo WAP.

El modelo de Distribución separada especifica una manera de descargar primero el objeto del medio, y a continuación descargar por separado, o pasar desde el servidor, el objeto de derechos al cliente. La invención puede utilizarse asimismo en la implementación de este modelo. El objeto del medio está protegido por una clave de cifrado de contenidos (CEK, Content Encryption Key). Con la notación utilizada en el protocolo de la invención, la clave s de protección del medio es una materialización de la CEK. La invención da a conocer asimismo una manera de autenticar el cliente de descarga al dispositivo y viceversa, por ejemplo en base a la clave x y/o y(y'). Esta autenticación se deja como "fuera de ámbito" en [10, 11].

REFERENCIAS

[1] A. J. Menezes, P.C. van Oorschot y S.C. Vanstone, "Handbook of Applied Cryptography" (“manual de criptografía aplicada”), capítulos 1, 10 y 11, CRC Press.

[2] L. Kaati, "Cryptographic Techniques and Encodings for Digital Rights Management" (“técnicas criptográficas y codificaciones para gestión de derechos digitales”), Master's Thesis in Computer Science, Department of Numerical Analysis and Computer Science, Royal Institute of Technology, Universidad de Estocolmo, 2001.

[3] Solicitud de patente sueca número 0101295-4, presentada el 10 de abril de 2001.

[4] "Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface" (“especificación del conjunto de herramientas de la aplicación SIM para la interfaz módulo de identidad de abonado-equipamiento móvil (SIM - ME)”), 3GGP TS 11.14, ETSI TS 101 267, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, versión 8.10.0, 1999.

[5] "USIM Application Toolkit (USAT)" (“conjunto de herramientas de aplicación USIM (USAT)”), 3GGP TS 31.111, ETSI TS 131 111, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, versión 4.4.0, publicación 4.

[6] "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface" (“explicación de la interfaz módulo de identidad de abonado - equipo móvil (SIM - ME”) 3GPP TS 11.11, ETSI TS 100 977, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, versión 8.5.0, 1999.

[7] "GSM API for SIM Toolkit, Stage 2" (“API GSM para conjunto de herramientas SIM, etapa 2”), 3GGP TS 03.19, ETSI TS 101 476, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, versión 8.4.0, 1999.

[8] "Security Mechanism for SIM Application Toolkit, Stage 2" (“mecanismo de seguridad para el conjunto de herramientas de aplicación SIM, etapa 2”), 3GGP TS 03.48, ETSI TS 101 181, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, versión 8.8.0, 1999.

[9] "Subscriber Identity Modules (SIM), Functional Characteristics" (“módulos de identidad de abonado (SIM), características funcionales”), ETSI TS 100 922, GSM 02.17, Technical Specification Digital Cellular Telecommunications system, versión 3.2.0, febrero de 1992.

[10] "Download Architecture Version 1.0" (“arquitectura de descarga versión 1.0”), versión propuesta, 10 de junio de 2002, Open Mobile Alliance.

[11] "Digital Rights Management Version 1.0" (“versión de gestión de derechos digitales 1.0”), versión propuesta, 28 de junio de 2002, Open Mobile Alliance.

[12] M. Handley, V. Jacobson, "SDP: Session Description Protocol" (“SDP:protocolo de descripción de sesión”), RFC 2327, abril de 1998.

REIVINDICACIONES

1. Un módulo (120) de identidad inviolable adaptado para la conexión física con un sistema (100) cliente que tiene un medio (110) para recibir contenido digital sobre una red y un dispositivo de presentación, teniendo dicho módulo de identidad inviolable un medio para llevar a cabo, por lo menos, parte de un procedimiento de autenticación y gestión de claves con la red en base a una clave simétrica almacenada en el módulo de identidad inviolable, produciendo de ese modo información de seguridad, **caracterizado por** un agente (125) de gestión de derechos digitales DRM para permitir el uso de dicho contenido digital, comprendiendo dicho agente DRM (125) un medio para llevar a cabo un proceso DRM en base a dicha información de seguridad procedente del procedimiento de autenticación y gestión de claves.

2. El módulo (120) de identidad inviolable acorde con la reivindicación 1, en el que dicho agente DRM (125) está implementado como una aplicación en un entorno (124) de aplicaciones de dicho módulo (120) de identidad inviolable.

3. El módulo (120) de identidad inviolable acorde con la reivindicación 1, en el que dicho agente DRM (125) incluye un medio para extraer una clave (s) de protección de contenidos a utilizar para descifrar contenido digital cifrado proporcionado desde un proveedor de contenidos, en base a información procedente de dicho procedimiento de autenticación y gestión de claves.

4. Un módulo de gestión de derechos digitales DRM **caracterizado por**:

- un primer agente DRM (125) implementado en un módulo (120) de identidad inviolable para la conexión con un sistema (100) cliente, comprendiendo dicho primer agente DRM (125) un medio para llevar a cabo un primer proceso DRM asociado con el contenido digital en base a información de seguridad obtenida a partir de un procedimiento de autenticación y gestión de claves entre el módulo (120) de identidad inviolable y una red sobre la cual puede ser recibido dicho contenido digital, estando basado el procedimiento de autenticación y gestión de claves en una clave simétrica almacenada en el módulo de identidad inviolable;

- un segundo agente DRM (135) implementado en un dispositivo de uso de contenido digital adaptado para usar dicho contenido digital, comprendiendo dicho agente DRM (135) un medio para llevar a cabo un segundo proceso DRM asociado con dicho contenido digital para permitir el uso de dicho contenido digital, y

- un medio de comunicación para la comunicación entre dicho primer agente DRM (125) y dicho segundo agente DRM (135).

5. El módulo DRM acorde con la reivindicación 4, en el que dicho medio para llevar a cabo el primer proceso DRM incluye un medio para extraer una clave (s) de protección de contenidos a utilizar para descifrar contenido digital protegido procedente de un proveedor de contenidos, en base a información procedente de dicho procedimiento de autenticación y gestión de claves.

6. El módulo DRM acorde con la reivindicación 5, en el que dicho medio de comunicación es operativo para asegurar que dicha clave (s) de protección de contenidos es accesible solamente mediante un segundo agente DRM que aplica apropiadamente las normas de uso asociadas a dicho contenido digital.

7. El módulo DRM acorde con la reivindicación 6, en el que dicho medio para llevar a cabo el segundo proceso DRM comprende un medio para descifrar contenido digital cifrado mediante dicha clave (s) de protección de contenidos.

8. El módulo DRM acorde con la reivindicación 4, en el que el medio de comunicación está adaptado para una comunicación entre el primer agente DRM (125) y el segundo agente DRM (135) en base a información (y) de la clave específica del dispositivo de uso.

9. El módulo DRM acorde con la reivindicación 8, en el que dicho agente DRM (125) comprende:

- un medio para autenticar dicho dispositivo de uso de contenido digital en base a dicha información (y) de la clave específica del dispositivo de uso, con objeto de verificar que dicho dispositivo de uso del contenido digital tiene una funcionalidad DRM válida; y

- un medio para enviar a dicho segundo agente DRM (135) datos DRM que permiten el uso de dicho contenido digital, en respuesta a la autenticación satisfactoria de un dispositivo de uso con una funcionalidad DRM válida.

10. El módulo DRM acorde con la reivindicación 9, en el que dicho agente DRM (125) comprende:

- un medio para cifrar datos DRM que permiten el uso de dicho contenido digital, en base a dicha información (y) de la clave específica del dispositivo de uso; y

un medio, que forma parte de dicho medio de comunicación, para enviar dichos datos DRM cifrados a dicho segundo agente DRM (135); y dicho segundo agente DRM (135) comprende un medio para descifrar dichos datos DRM cifrados con objeto de permitir el uso de dicho contenido digital, en base a dicha información (y) de la clave específica del dispositivo de uso.

11. El módulo DRM acorde con la reivindicación 4, en el que dicho módulo (120) de identidad inviolable y dicho dispositivo de uso de contenido digital están configurados de modo inviolable con información (y) de la clave específica del dispositivo de uso.

12. El módulo DRM acorde con la reivindicación 4, en el que dicho primer agente DRM (125) está implementado como una primera aplicación en un entorno (124) de aplicaciones de dicho módulo (120) de identidad inviolable.

13. El módulo DRM acorde con la reivindicación 4, en el que dicho agente DRM (135) está implementado como una segunda aplicación en un entorno de aplicaciones inviolable en dicho dispositivo de uso del contenido digital.

14. El módulo DRM acorde con la reivindicación 4, en el que el dispositivo de uso del contenido digital es un dispositivo de presentación.

15. Un sistema (100) cliente, que comprende:

- un medio para recibir contenido digital sobre una red;

- un dispositivo de uso de contenido digital; y **caracterizado por**

- un módulo (120) de identidad inviolable implementado con un agente DRM de gestión de derechos digitales para permitir el uso de dicho contenido digital por dicho dispositivo de uso de contenido digital, en donde el módulo de identidad inviolable comprende un medio para llevar a cabo, por lo menos, parte de un procedimiento de autenticación y gestión de claves entre el módulo de identidad inviolable y una red en base a una clave simétrica almacenada en el módulo de identidad inviolable, y dicho agente DRM incluye un medio para llevar a cabo un proceso DRM en base a información procedente de dicho procedimiento de autenticación y gestión de claves.

16. El sistema cliente acorde con la reivindicación 15, en el que dicho agente DRM está implementado como una aplicación en un entorno de aplicaciones de dicho módulo de identidad inviolable.

17. El sistema cliente acorde con la reivindicación 15, en el que dicho agente DRM incluye un medio para extraer una clave (s) de protección de contenidos a utilizar para descifrar contenido digital cifrado proporcionado desde un proveedor de contenidos, en base a información procedente de dicho procedimiento de autenticación y gestión de claves.

18. El sistema cliente acorde con la reivindicación 16, en el que el dispositivo de uso de contenido digital es un dispositivo de presentación.

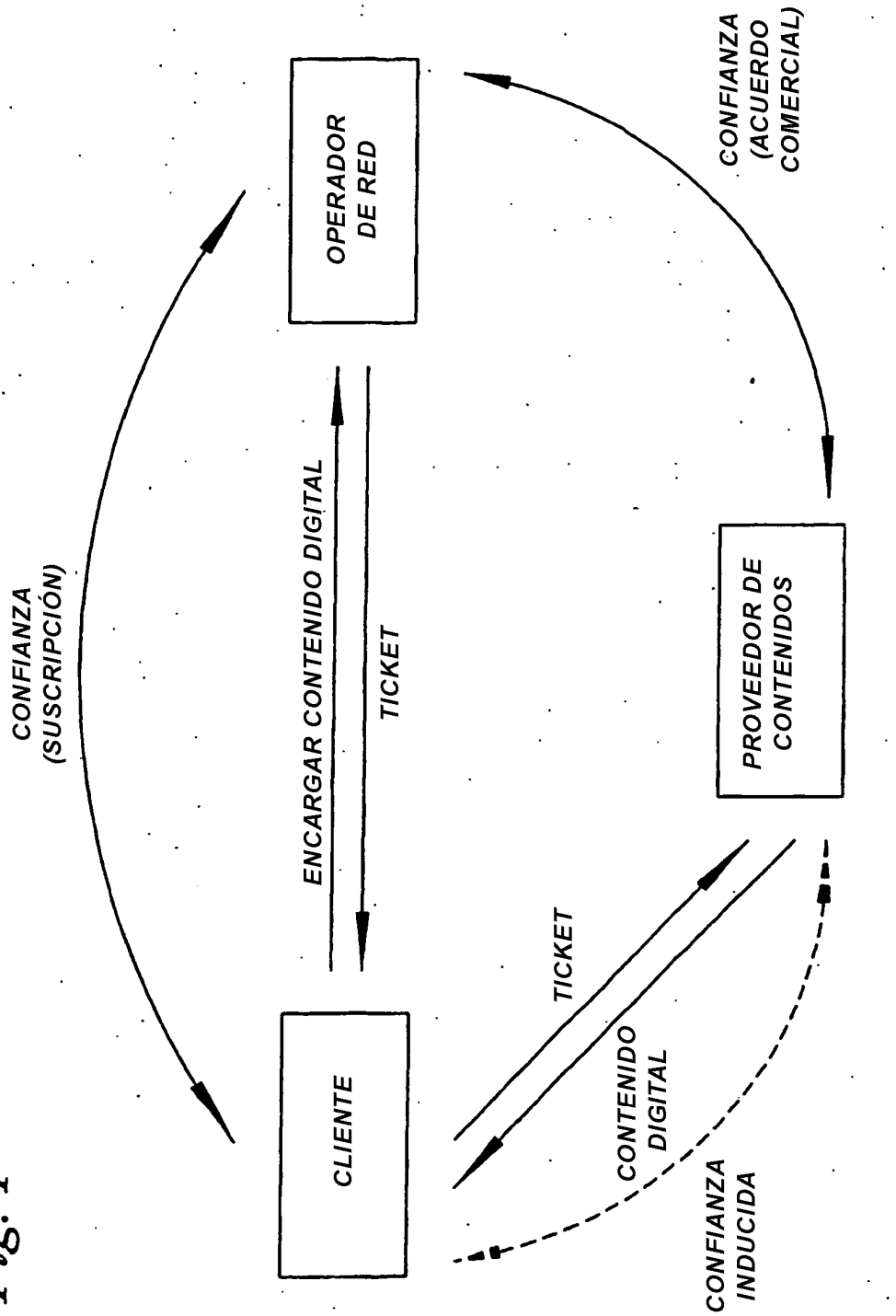
OPERADOR DE RED
CONFIANZA (ACUERDO COMERCIAL)
CONFIANZA (SUSCRIPCIÓN)
ENCARGAR CONTENIDO DIGITAL
TICKET
PROVEEDOR DE CONTENIDOS
CLIENTE
TICKET
CONTENIDO DIGITAL
CONFIANZA INDUCIDA

Fig. 1

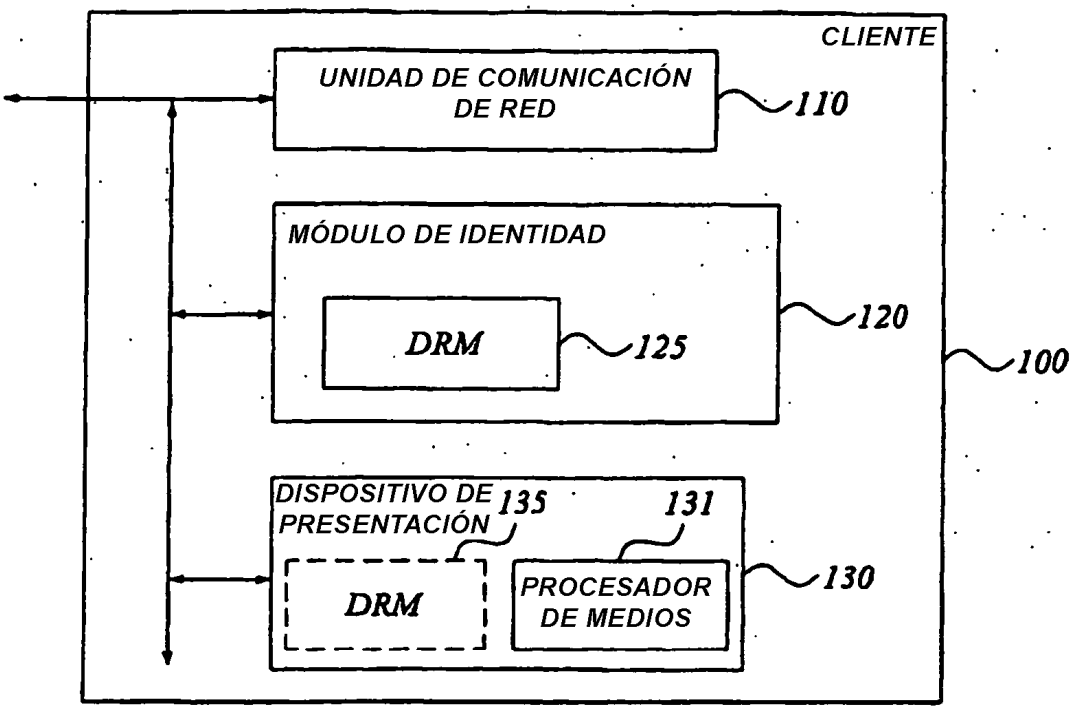
CLIENTE
UNIDAD DE COMUNICACIÓN DE RED
110
MÓDULO DE IDENTIDAD
DRM
125
120
100
DISPOSITIVO DE PRESENTACIÓN
135
131
DRM
PROCESADOR DE MEDIOS
130

Fig. 2A

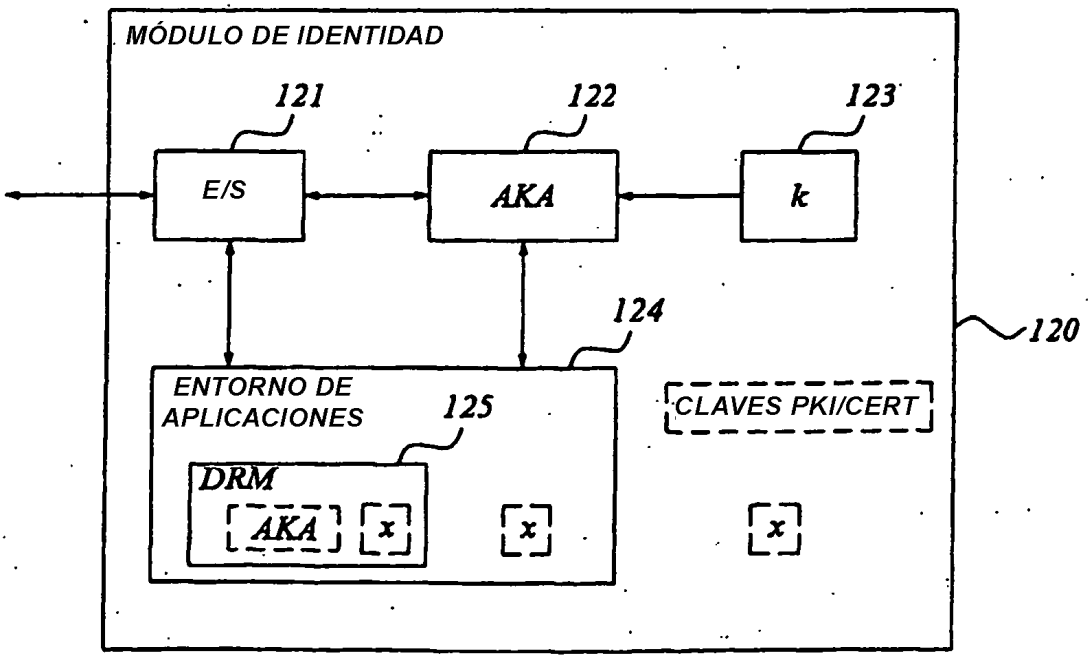
MÓDULO DE IDENTIDAD
121
122
123
E/S
AKA
k
124
120
ENTORNO DE APLICACIONES
125
CLAVES PKI/CERT
DRM
AKA
x
x
x

Fig. 2B

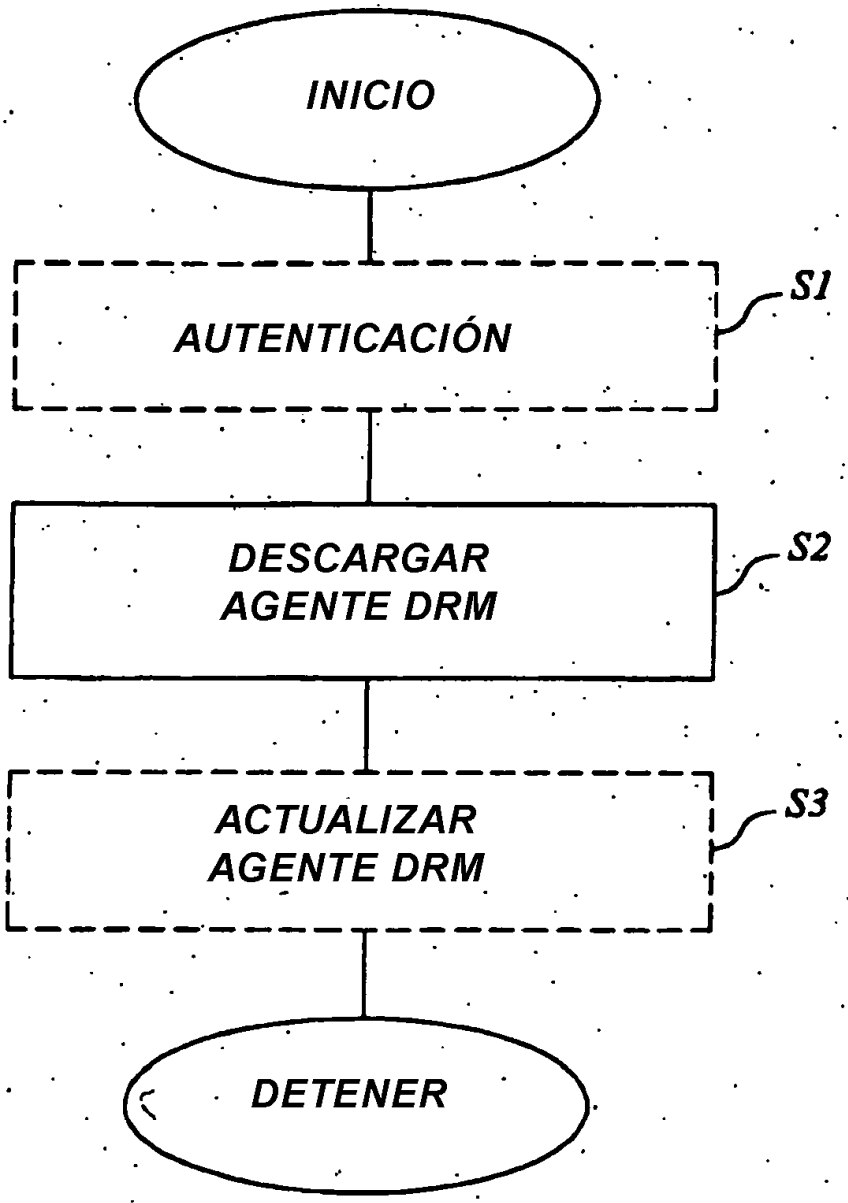
INICIO
AUTENTICACIÓN
S1
DESCARGAR AGENTE DRM
S2
ACTUALIZAR AGENTE DRM
S3
DETENER

Fig. 3

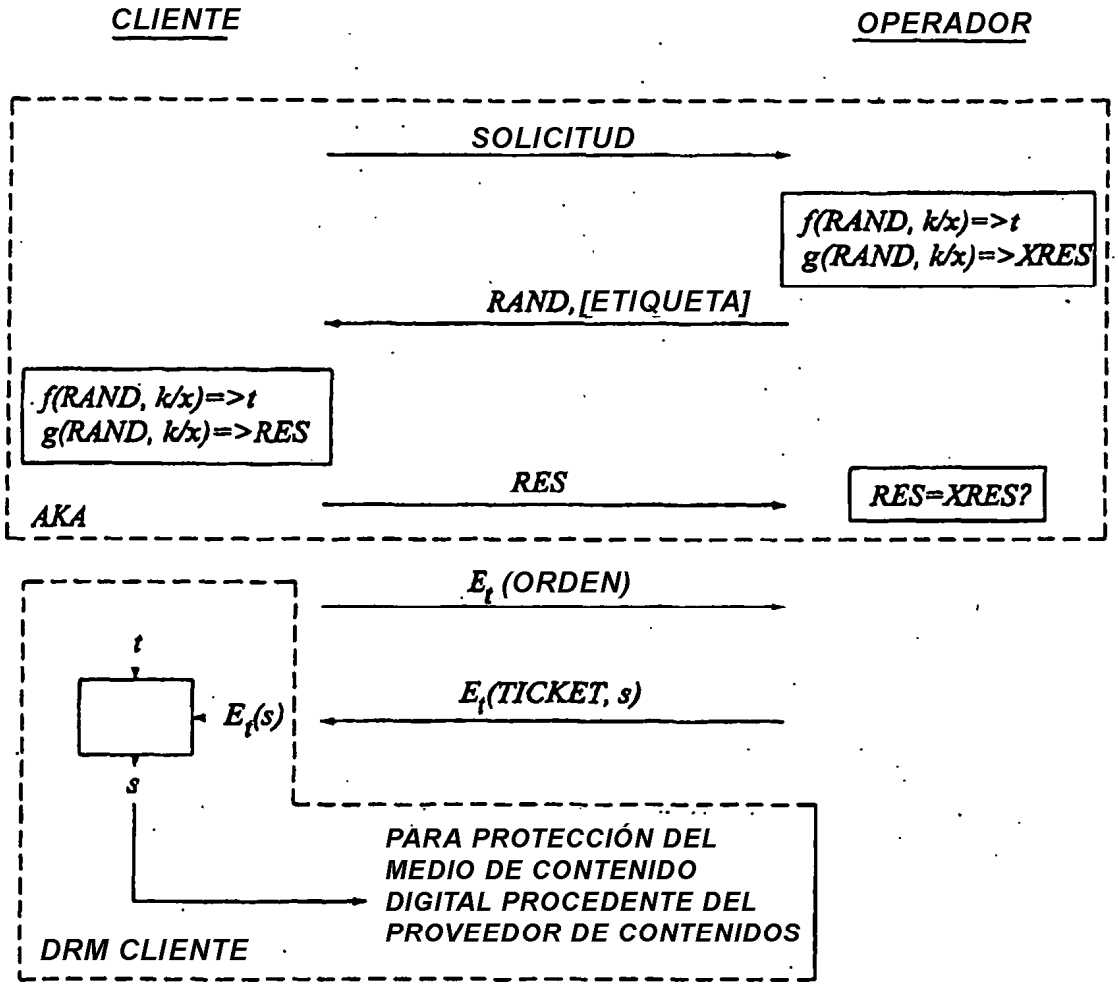
CLIENTE
OPERADOR
SOLICITUD
f(RAND, k/x)=>t
g(RAND, k/x)=>XRES
RAND,[ETIQUETA]
f(RAND, k/x)=>t
g(RAND, k/x)=>RES
RES
RES=XRES?
AKA
E_t (ORDEN)
t
E_t(s)
E_t(TICKET, s)
s
PARA PROTECCIÓN DEL MEDIO DE CONTENIDO DIGITAL PROCEDENTE DEL PROVEEDOR DE CONTENIDOS
DRM CLIENTE

Fig. 4

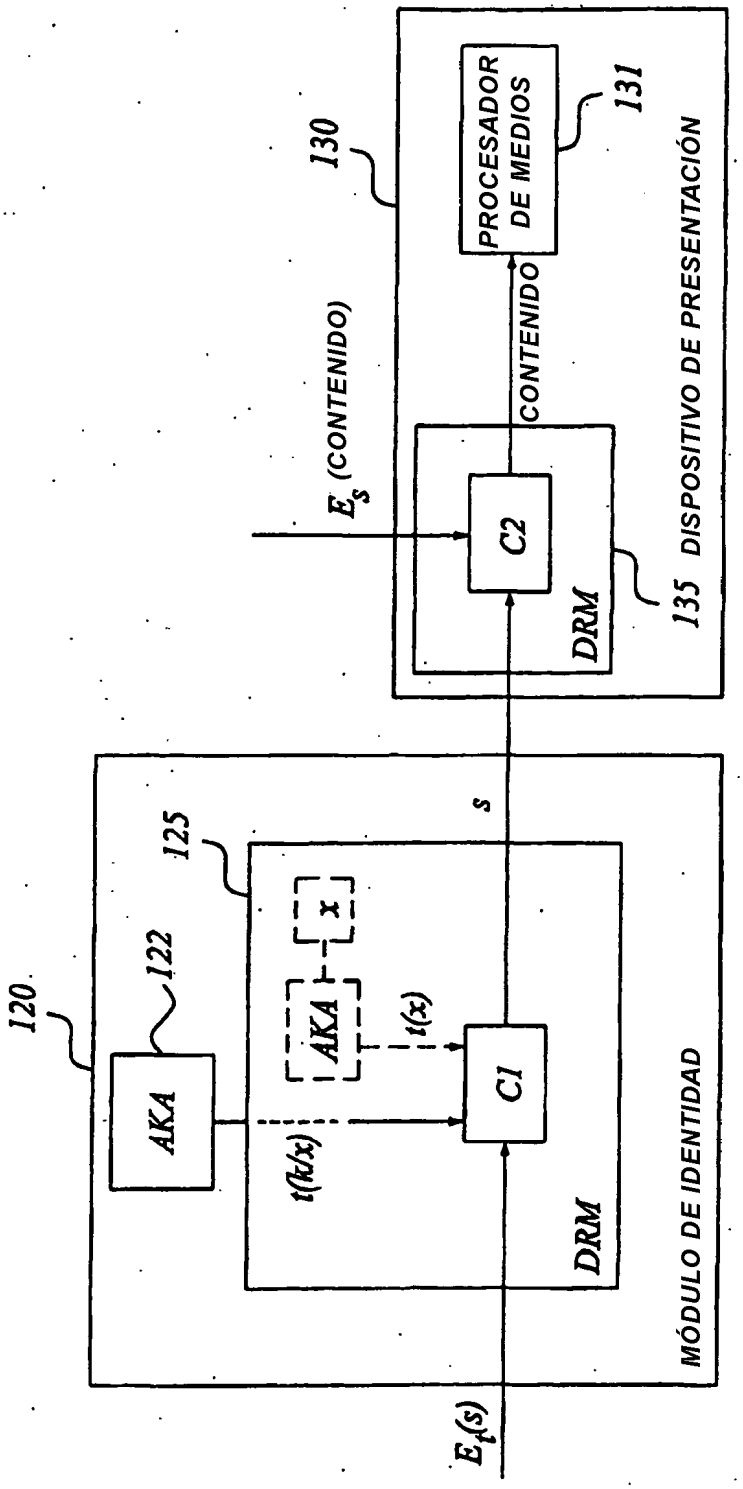
120
122
AKA
125
AKA
x
t(x)
t(k/x)
C1
DRM
MÓDULO DE IDENTIDAD
s
$E_t(s)$
130
E_s (CONTENIDO)
C2
DRM
135 DISPOSITIVO DE PRESENTACIÓN
CONTENIDO
PROCESADOR DE MEDIOS
131

Fig. 5

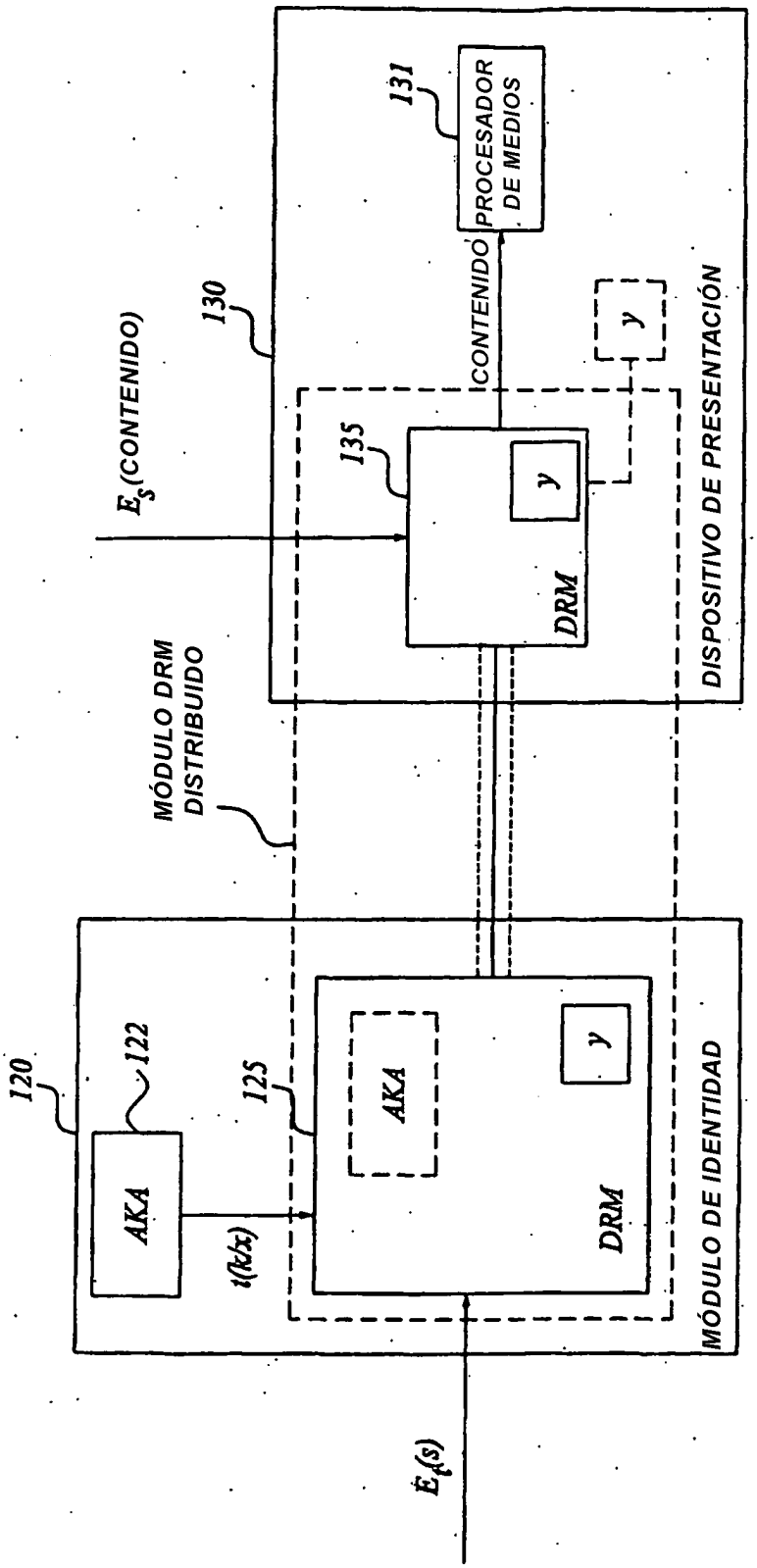
131
PROCESADOR DE MEDIOS
CONTENIDO
130
y
E_S(CONTENIDO)
135
y
DRM
DISPOSITIVO DE PRESENTACIÓN
MÓDULO DRM DISTRIBUIDO
120
122
125
AKA
AKA
y
DRM
t(k/x)
MÓDULO DE IDENTIDAD
$E_I(s)$

Fig. 6

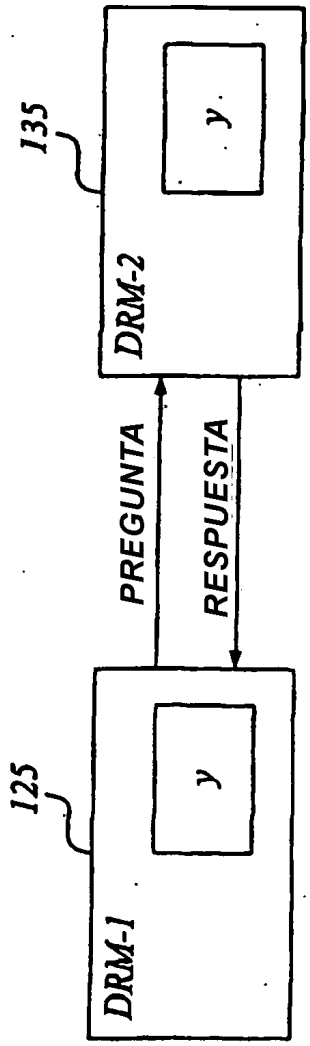
135
y
DRM-2
PREGUNTA
RESPUESTA
125
y
DRM-1

Fig. 7A

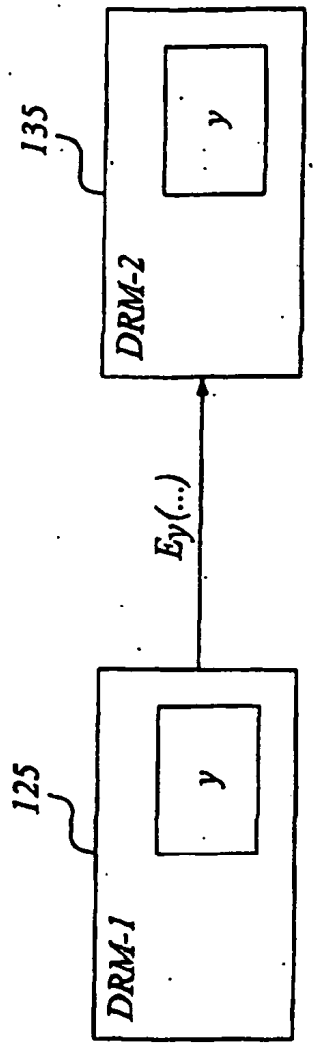
135
y
DRM-2
Ey(...)
125
y
DRM-1

Fig. 7B

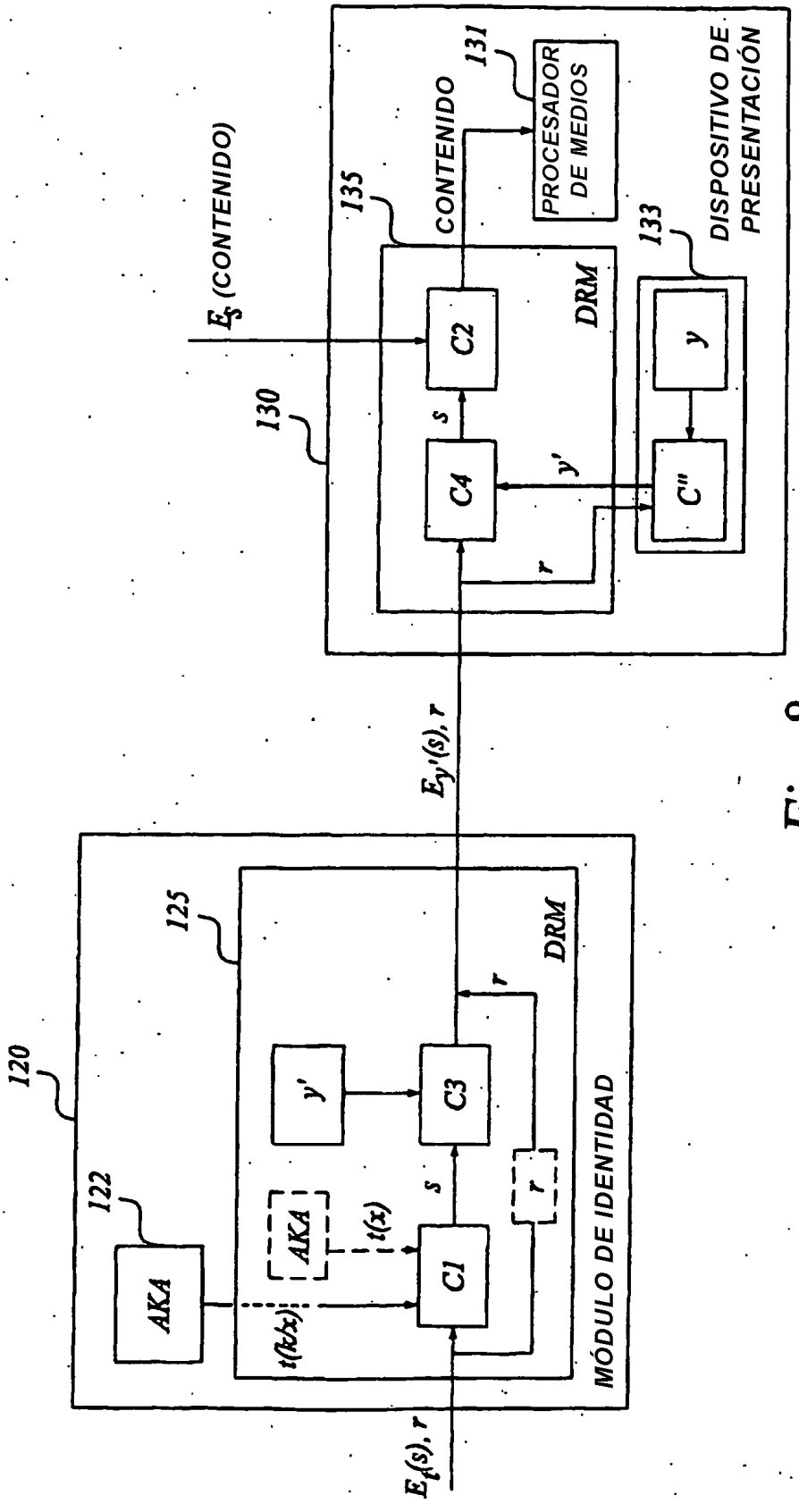
120
MÓDULO DE IDENTIDAD
122
AKA
AKA
t(kx)
t(x)
125
DRM
y'
C1
C3
s
r
r
$E_f(s), r$
$E_{y'}(s), r$
130
135
DRM
C2
C4
s
y'
r
CONTENIDO
131
PROCESADOR DE MEDIOS
E_S (CONTENIDO)
133
DISPOSITIVO DE PRESENTACIÓN
y
C''

Fig. 8

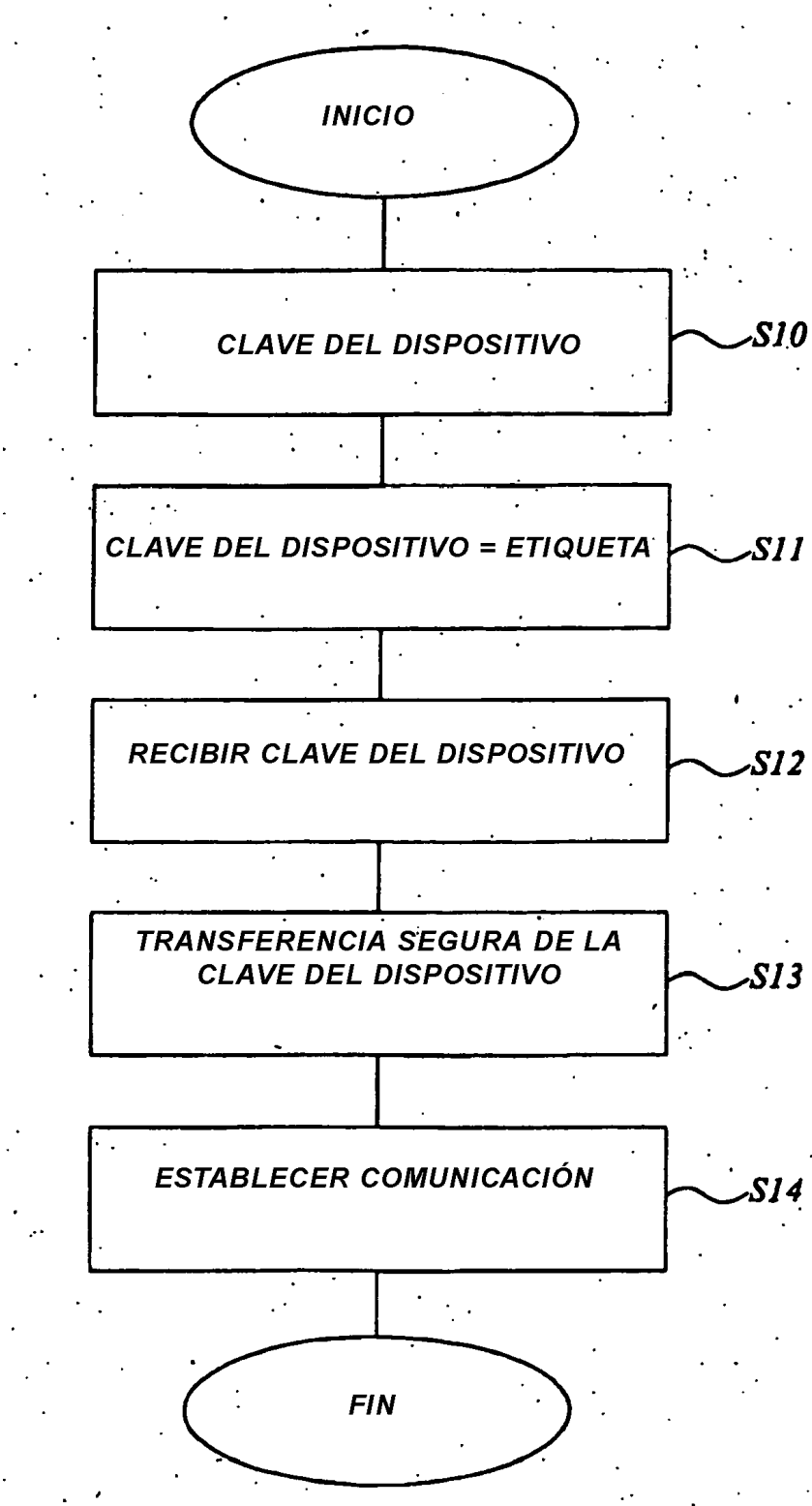
INICIO
CLAVE DEL DISPOSITIVO
S10
CLAVE DEL DISPOSITIVO = ETIQUETA
S11
RECIBIR CLAVE DEL DISPOSITIVO
S12
TRANSFERENCIA SEGURA DE LA CLAVE DEL DISPOSITIVO
S13
ESTABLECER COMUNICACIÓN
S14
FIN

Fig. 9

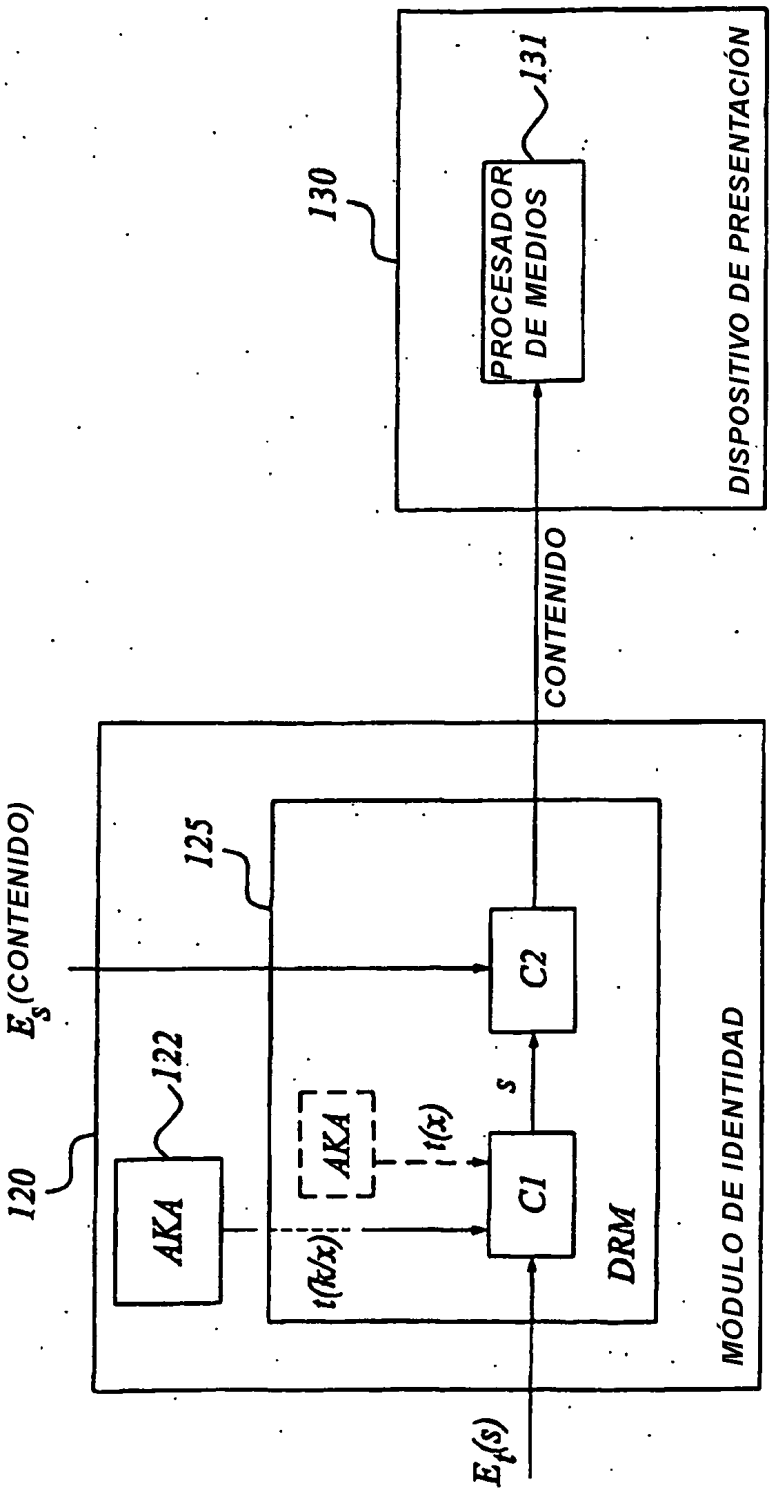
130
131
PROCESADOR DE MEDIOS
DISPOSITIVO DE PRESENTACIÓN
CONTENIDO
125
E_S(CONTENIDO)
120
122
AKA
AKA
t(k/x)
t(x)
s
C1
C2
DRM
MÓDULO DE IDENTIDAD
E_I(s)

Fig. 10

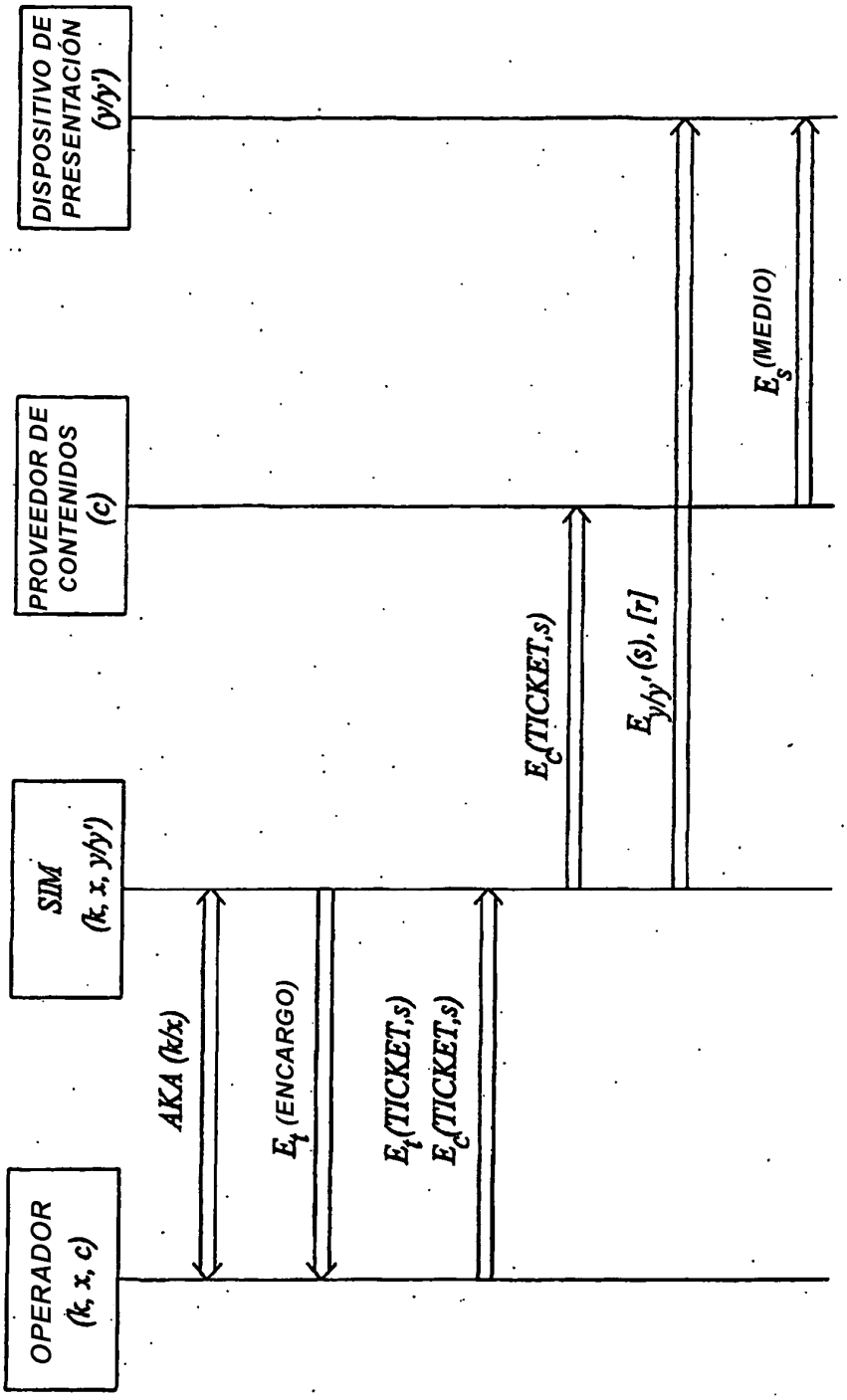
DISPOSITIVO DE PRESENTACIÓN (y/y')
PROVEEDOR DE CONTENIDOS (c)
SIM (k, x, y/y')
OPERADOR (k, x, c)
AKA (k/k)
E_t (ENCARGO)
E_t(TICKET,s)
E_c(TICKET,s)
E_c(TICKET,s)
E_y/y'(s), [r]
E_s (MEDIO)

Fig. 11

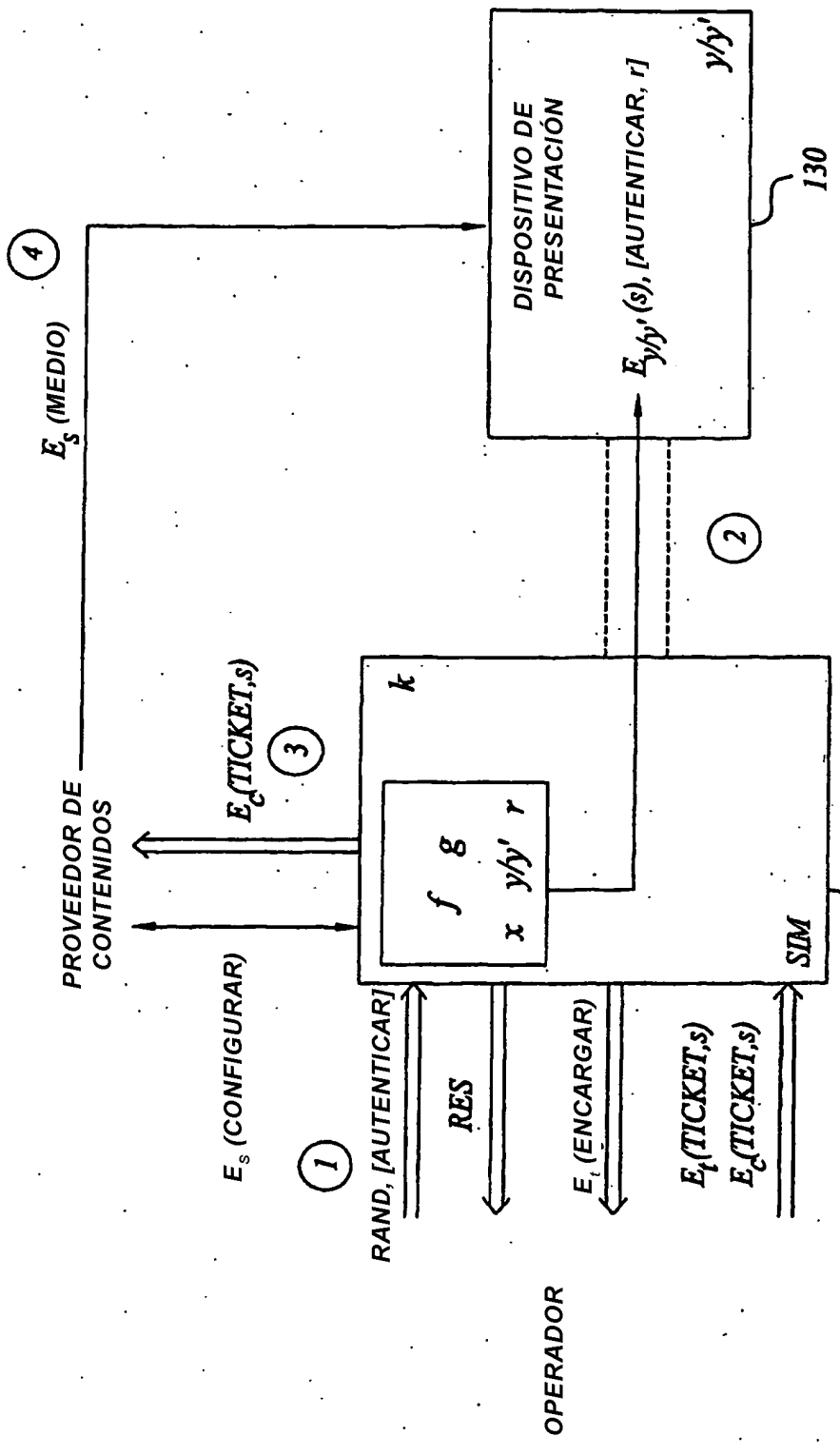
DISPOSITIVO DE PRESENTACIÓN
130
$E_{y/y'}(s)$, [AUTENTICAR, r]
y/y'
4
E_s (MEDIO)
PROVEEDOR DE CONTENIDOS
E_c(TICKET,s)
3
k
f g
x y/y' r
SIM
120
2
E_s (CONFIGURAR)
1
RAND, [AUTENTICAR]
RES
E_l (ENCARGAR)
E_l(TICKET,s)
E_c(TICKET,s)
OPERADOR

Fig. 12