(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 356 990**

(51) Int. Cl.:
H04L 12/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03721242 .0**
(96) Fecha de presentación : **25.04.2003**
(97) Número de publicación de la solicitud: **1529371**
(97) Fecha de publicación de la solicitud: **11.05.2005**

(54) Título: **Monitorización de contenido digital proporcionado por un proveedor de contenidos sobre una red.**

(30) Prioridad: **15.08.2002 SE 0202450**

(45) Fecha de publicación de la mención BOPI:
15.04.2011

(45) Fecha de la publicación del folleto de la patente:
15.04.2011

(73) Titular/es: **Telefonaktiebolaget LM Ericsson (publ)**
Grimstagatan 161
S-162 58 Vällingby, SE

(72) Inventor/es: **Näslund, Mats;**
Selander, Göran y
Björkengren, Ulf

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

DESCRIPCIÓN

CAMPO TÉCNICO

La presente invención generalmente se refiere a la gestión de los derechos digitales (DRM) para gestionar los contenidos digitales proporcionados sobre redes, y más particularmente a la monitorización del uso de contenidos digitales por un cliente en un sistema de DRM.

ANTECEDENTES

La distribución de contenidos digitales o datos de medios que usan las modernas tecnologías de comunicaciones digitales está creciendo constantemente, sustituyendo cada vez más los métodos de distribución más tradicionales. En particular, hay una tendencia en aumento de descargar o difundir de forma continua contenidos digitales desde un proveedor de contenidos a un cliente o usuario, el cuál entonces típicamente presenta el contenido usando un dispositivo de presentación de acuerdo con algunos derechos de usuario, o reglas de uso especificadas en una licencia asociada con los contenidos digitales. Debido a las ventajas de esta forma de distribución de contenidos, que incluye ser económica, rápida y fácil de realizar, las aplicaciones ahora se pueden facilitar para la distribución de todo tipo de medios, tales como audio, vídeo, imágenes, libros electrónicos y programas informáticos.

No obstante, con esta nueva forma de distribuir los contenidos de medios digitales llega la necesidad de proteger los activos digitales de los proveedores de contenidos contra el uso no autorizado y la copia ilegal. Los creadores y los titulares de los derechos de autor de los contenidos digitales naturalmente tienen un fuerte interés económico de proteger sus derechos, y esto ha conducido a una demanda que aumenta para la gestión de los derechos digitales (DRM). La DRM generalmente es una tecnología para proteger los activos de los proveedores de contenidos en un sistema de distribución de contenidos digitales, que incluye proteger, monitorizar y restringir el uso de los contenidos digitales así como la gestión del pago. Un sistema de DRM normalmente incluye de esta manera componentes para el cifrado, la autentificación, la gestión de claves, la gestión de reglas de uso y el cargo.

Las amenazas más básicas para un sistema de DRM incluyen el espionaje, el copiado ilegal, la modificación de las reglas de uso, y la repudiación de encargo o entrega de contenidos. La mayoría de estos problemas básicos de seguridad se resuelve mediante las técnicas criptográficas estándar, que incluyen el cifrado, la autentificación y la gestión de claves. No obstante, lo que básicamente distingue los problemas de seguridad de un sistema de DRM de otros problemas generales de seguridad es que ni siquiera la otra parte final de la comunicación (el usuario) es completamente de confianza. De hecho, el usuario final debería querer intentar extender fraudulentamente sus derechos de uso, por ejemplo presentando el contenido de los medios más veces que por las que ha pagado o copiar ilegalmente los contenidos digitales a otro dispositivo de presentación. Por lo tanto, se requiere alguna forma de aplicación de reglas en el dispositivo de presentación del usuario. Para este fin, comúnmente se usan un agente de DRM implementado como circuito a prueba de sabotajess en el dispositivo de presentación y algún lenguaje formal que exprese las reglas de uso junto con las técnicas criptográficas básicas mencionadas anteriormente.

No obstante, mientras el agente de DRM (al menos teóricamente) aplica las reglas de uso y mantiene el uso de acuerdo con la licencia, que por sí no garantiza que el usuario no repudiará el uso de los contenidos digitales. Por ejemplo, el usuario puede haber pagado para ver una película descargada tres veces, pero reclama que debido a algún mal funcionamiento solamente fue capaz de verla dos veces. El usuario entonces discrepa con el proveedor de contenidos sobre el número de presentaciones que ha consumido. Esto puede fácilmente escalar en un proceso legal, especialmente si se refiere a unos contenidos digitales de alto valor, por los cuales el usuario ha pagado una gran suma de dinero por los derechos de uso.

Los sistemas de DRM de la técnica previa y los dispositivos de presentación que incorporan los agentes de DRM no proporcionan ningún mecanismo para minimizar el riesgo de desacuerdo entre el usuario y el agente de DRM, tratado arriba, o en el caso de que ocurra, ningún mecanismo para soportar la defensa del agente de DRM y soportar por ello la defensa del proveedor de contenidos, el fabricante del dispositivo y el fabricante del sistema de DRM.

El documento US 2001 053 223 A1 de Ishibashi (de aquí en adelante conocido como Ishibashi) y otros revela el registro del uso de contenidos para propósitos de cargo. Ishibashi genera información de registro relacionada con la descarga de los contenidos usados en un dispositivo de usuario. Ishibashi, no obstante, no proporciona el registro de la presentación real de los contenidos ejemplares incluyendo la calidad de la presentación según se percibe por el usuario.

RESUMEN

La presente invención supera estas y otras desventajas de las adaptaciones de la técnica previa.

Es un objeto general de la presente invención proporcionar una funcionalidad de monitorización del uso de los contenidos digitales en un sistema de DRM para los datos descargados o difundidos de forma continua.

Es otro objeto de la invención disuadir a los usuarios de repudiar el uso de los contenidos digitales recibidos desde un proveedor de contenidos sobre una red.

Otro objeto de la invención es proporcionar un sistema cliente que incorpora un agente de registro para registrar la información de uso de los contenidos digitales recibidos de acuerdo con los criterios de registro.

Un objeto adicional de la invención es proporcionar la implementación y descarga flexible y eficaz de los agentes de registro en los sistemas clientes.

También es un objeto de la invención proporcionar una funcionalidad de monitorización del uso de contenidos digitales que es útil como base de cargo del uso de los contenidos digitales.

Estos y otros objetos se satisfacen por la invención como se define por las reivindicaciones de patente anexas.

Brevemente, la presente invención implica disponer o implementar un agente de registro en un módulo o sistema cliente empleado para usar los contenidos digitales encargados y recibidos desde un proveedor de contenidos sobre una red, por ejemplo Internet o una red inalámbrica para comunicación móvil. Este agente de registro monitoriza el uso de los contenidos, realizado por el cliente, registrando la información concerniente al uso individualmente para cada uso que va a ser monitorizado. La información de uso generada entonces se enlaza o asocia con el cliente o usuario, permitiendo la identificación desde qué cliente (usuario) se origina la información de uso.

Esta vinculación preferentemente se obtiene realizando una operación de seguridad, tal como la realización, al menos una parte de una autentificación de la información de uso. La información de uso generada y autentificada ahora se almacena entonces como una entrada de registro en un registro, o bien dispuesto en el sistema cliente o bien proporcionado externamente por una parte de confianza, por ejemplo un operador de red.

El uso realizable por el cliente incluye presentar o reproducir, guardar, enviar, copiar, ejecutar, borrar y/o modificar los contenidos digitales. Las reglas o derechos de uso de los métodos relevantes del uso del cliente que va a ser monitorizado preferentemente se especifican en una licencia o cupón asociado con los contenidos digitales.

La operación de seguridad de la invención para permitir la identificación del cliente vinculando la información de uso registrada a la misma se puede realizar en un número de formas distintas. En primer lugar, como se mencionó arriba, al menos parte de una autentificación de la información de uso se puede realizar por el cliente. Esta autentificación podría ser una firma de la información de uso que usa una clave de firma privada de una pareja de claves asimétricas, en la que la clave de verificación pública junto con un certificado en la clave pública se certifica por una parte de confianza, por ejemplo el operador de red. Alternativamente, una etiqueta de autentificación basada en claves simétricas se puede adjuntar a la información de uso registrada, permitiendo la identificación de las que se deriva la información implicando una tercera parte de confianza que conoce la clave simétrica. El origen de la información de uso también se podría identificar, al menos implícitamente, cifrando o protegiendo criptográficamente la información de uso con una clave protegida. Alternativamente, el cliente podría enviar la información de uso generada a una tercera parte de confianza, que realiza la operación de seguridad real. Otra operación de seguridad posible es almacenar la información de uso registrada en un entorno que es inaccesible para el usuario, pero asociada al mismo o al sistema cliente. Un ejemplo típico es el entorno de un módulo de identidad de abonado (SIM). Para activar el entorno SIM el usuario típicamente introduce un código pin o código de seguridad personal. No obstante, aunque el entorno se activa y el agente de registro puede almacenar la información de uso registrada en este área segura, el usuario realmente no tiene acceso físico a la misma, es decir no es capaz de modificar o borrar el registro del SIM. Dado que el SIM se emite por un proveedor de servicios (red) y se asocia con un acuerdo de servicios (suscripción) entre el usuario y el proveedor de servicios, es, de esta manera, posible asociar posteriormente el SIM y consecuentemente el registro almacenado inmediatamente después con el usuario.

Registrando o grabando la información de uso del cliente, el agente de registro de acuerdo con la invención tiene un efecto disuasorio de repudiación en los usuarios, bajando el riesgo de que los usuarios violen las reglas de uso de los contenidos digitales encargados. El registro de uso generado también se puede usar si se presenta un desacuerdo entre el usuario y el proveedor de contenidos (a través de un agente de DRM implementado en el sistema cliente para aplicar el uso de acuerdo con las reglas de uso). Simplemente investigando el registro, la información sobre el número real de usos realizado por el cliente, cuando fueron realizados, la calidad de uso obtenida durante la sesión de presentación (dependiendo de qué se incluye en la información de uso) se puede recuperar y usar para ayudar a resolver cualquier disputa.

La información de uso registrada de la invención también se puede usar como una base para el cargo del uso de los contenidos digitales. La información entonces especifica o bien la cantidad que va a ser cargada o bien alguna otra información, por ejemplo el tiempo total de uso y un identificador de los contenidos digitales, que permite el cálculo de la cantidad que va a ser cargada. En tal caso, la información de uso registrada se transmite preferentemente al operador de red o a una entidad de facturación que gestiona los cargos de los contenidos digitales encargados. Debido a la operación de seguridad tratada arriba el operador o entidad puede identificar al usuario que va a ser cargado o una cuenta que va a ser cargada.

La información de uso incluye elementos, que conciernen al uso real de los contenidos digitales. Los elementos pueden comprender una representación de los contenidos digitales por ejemplo el nombre de archivo asociado o una huella digital del contenido, incluyendo el contenido en sí mismo o un valor función de generación de claves del mismo. Además, la información de la calidad de uso se puede incluir, por ejemplo especificando el ancho de banda y/o la

resolución de los contenidos y/o la velocidad de las muestras obtenidas si los contenidos se entrega como datos de difusión de forma continua. El tiempo de uso de los contenidos también se encuentra preferentemente en la información.

El agente de registro se implementa preferentemente en el programa informático, los componentes físicos o una combinación de los mismos en un agente de DRM del módulo o sistema cliente, o en conexión con un dispositivo de uso, que realiza el uso real de los contenidos digitales, asociados con el módulo. Para impedir que un atacante acceda ilegalmente y modifique la información general de uso, la información preferentemente se protege criptográficamente usando una clave de autentificación/cifrado. La clave de verificación/descifrado entonces se puede almacenar en una parte de confianza. No obstante, si se usan las claves criptográficas simétricas o claves públicas, la clave de verificación/descifrado típicamente se certifica meramente mediante esa parte de confianza y se almacena en otra parte.

La seguridad del agente de registro también se aumenta implementándola en un dispositivo a prueba de sabotajes, que se puede disponer de manera extraíble en el sistema cliente para permitir al dispositivo, que incluye el agente de registro, que sea movido entre distintos sistemas cliente. En tal caso, el sistema cliente, o el dispositivo de uso del sistema cliente, se configura preferentemente para no permitir el uso de los contenidos digitales sin que esté presente el agente de registro extraíble implementando a prueba de sabotajes. Un módulo a prueba de sabotajes preferente es un módulo de identidad de abonado (SIM) de red expedido por un proveedor de servicios (red), por ejemplo las tarjetas SIM estándar usadas en los teléfonos móviles GSM (Sistema Global para Comunicaciones Móviles) pero también pueden ser usadas la SIM (SIM) de LT-MTS (Sistema Universal de Telecomunicaciones Móviles), el WIM (Módulo de Identidad Inalámbrico), las tarjetas ISIM (Módulo de Identidad de Servicios Multimedia de Internet), y los módulos de UICC (Tarjeta Universal de Circuitos Integrados). Cuando se implementa en una SIM, el agente de registro puede usar la autentificación y las funciones criptográficas de la SIM para usar en la información de uso. Además, las claves asociadas con la suscripción SIM se pueden usar para realizar el cifrado y la autentificación de la información de uso y para propósitos de facturación.

Además, el agente de registro se puede implementar en un entorno de aplicaciones proporcionado por un juego de herramientas de aplicaciones asociado con el SIM, por ejemplo SAT (Juego de Herramientas de Aplicaciones del SIM) o USAT (SAT de UMTS). El SIM se puede prefabricar con el agente de registro o el agente de registro se puede descargar de manera segura (preferentemente autentificado y cifrado) desde un nodo de red, asociado con el operador de red o el proveedor de servicios asociado con el SIM. Los comandos, asociados con el interfaz del módulo cliente – SIM, se usan para descargar e implementar el agente de registro en el entorno de aplicaciones. Los mismos comandos también se pueden usar para recibir e implementar posteriormente actualizaciones del agente de registro y transferir la información de registro real a una parte de confianza.

El agente de registro de acuerdo con la presente invención se puede disponer en cualquier sistema cliente adaptado para recibir los contenidos digitales sobre una red, incluyendo ordenadores personales, unidades móviles, por ejemplo teléfonos móviles, asistentes personales digitales, comunicadores, reproductores de Mp3, etc.

La invención ofrece las siguientes ventajas:

- Proporciona defensa fortalecida para el fabricante de equipos, el operador de red y el proveedor de contenidos (y el emisor de derechos) en una situación en la que está presente una discusión, en si el uso de los contenidos digitales por un sistema cliente realmente ha sido realizado o no;

- Disuade a los usuarios de repudiar el uso de los contenidos digitales de acuerdo con las reglas de uso asociadas con los contenidos o intentando violar las reglas;

- Proporciona información que se puede usar para cargar a un cliente por el uso de los contenidos digitales encargados o descargados o difundidos de forma continua;

- Desde el punto de vista del usuario final, la invención puede proporcionar la implementación flexible y actualizable de los agentes de registro, así como la “portabilidad” entre distintos sistemas clientes;

- Fortalece la posibilidad del usuario final de ser reembolsado en caso en los que no reciba el servicio o la calidad por la que pagó;

- Un operador de red puede gestionar y actualizar eficientemente los agentes de registro conectados a la red, y la invención también abre nuevas posibilidades de negocio para el operador que actúa como un centro de confianza para la distribución de contenidos;

- Proporciona información útil de uso de los contenidos digitales, realizados por los clientes, cuya información se puede usar por los proveedores de contenidos cuando se deciden los modelos de negocio o como base robusta para estadísticas de los contenidos digitales descargados o difundidos de forma continua.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La invención junto con los objetos y ventajas adicionales de la misma, se puede entender mejor haciendo referencia a la siguiente descripción tomada junto con los dibujos adjuntos, en los que:

La Fig. 1 es una descripción de un ejemplo de un sistema de encargo y distribución de contenidos digitales que incorpora las partes relevantes y sus relaciones mutuas;

La Fig. 2 es un diagrama de bloques que ilustra esquemáticamente una realización de un módulo o sistema cliente de acuerdo con la presente invención;

La Fig. 3 es una descripción del sistema de encargo y distribución de contenidos digitales de la Fig. 1, que ilustra las partes relevantes en más detalle;

La Fig. 4 es un diagrama de bloques que ilustra esquemáticamente otra realización de un sistema cliente de acuerdo con la presente invención;

La Fig. 5 es un diagrama de bloques que ilustra un agente de registro de acuerdo con la presente invención con la funcionalidad de operación de seguridad;

La Fig. 6 es una descripción de un registro que almacena las entradas de registro con la información de uso del uso del cliente de los contenidos digitales;

La Fig. 7 es un diagrama de bloques que ilustra esquemáticamente otra realización de un módulo o sistema cliente de acuerdo con la presente invención;

La Fig. 8 es un diagrama de bloques que ilustra un dispositivo a prueba de sabotajes que comprende un agente de registro de acuerdo con la presente invención;

La Fig. 9 es un diagrama de bloques que ilustra esquemáticamente una realización adicional de un sistema cliente de acuerdo con la presente invención;

La Fig. 10 es un diagrama de flujo que ilustra los pasos de un método de monitorización de acuerdo con la presente invención;

La Fig. 11 es un diagrama de flujo que ilustra el paso de registro de la Fig. 10 en más detalle;

La Fig. 12 es un diagrama de flujo que ilustra el paso que realiza la operación de seguridad de la Fig. 10 en más detalle;

La Fig. 13 es un diagrama de flujo que ilustra pasos adicionales del método de monitorización de acuerdo con la invención; y

La Fig. 14 es un diagrama de flujo que ilustra los pasos de un método de gestión de los derechos digitales de acuerdo con la presente invención.

DESCRIPCIÓN DETALLADA

La presente invención generalmente es aplicable a la gestión de los derechos digitales (DRM) usada en un sistema de encargo y distribución de contenidos digitales. En tal sistema de encargo y distribución, los medios o contenidos digitales se proporcionan, directa o indirectamente, desde un proveedor de contenidos a un cliente sobre una red, por ejemplo Internet o una red inalámbrica para comunicaciones móviles, gestionada por un operador de red. Para facilitar la comprensión de la invención, una breve discusión de las funcionalidades generales de DRM sigue. Como se mencionó en la sección de antecedentes, la DRM se usa para proteger los activos de los titulares de los derechos de autor en un sistema de encargo y distribución de contenidos digitales. En este sistema, la DRM típicamente considera la gestión de claves y autentificación, la gestión de los derechos de uso y el cargo. Estas funcionalidades de DRM se implementan en módulos de DRM dispuestos en las partes relevantes, es decir por ejemplo en un módulo o sistema cliente, en un servidor del operador de red y en un servidor de contenidos o medios del proveedor de contenidos.

Comenzando con la gestión de claves y autentificación, la autentificación se usa para identificar las partes en el proceso de encargo y distribución de los contenidos digitales. Las técnicas bien conocidas en la técnica, tales como la autentificación de usuarios y las firmas digitales que usan claves criptográficas [1], se pueden usar para la autentificación. Además, se pueden usar técnicas para marcar o sellar los contenidos digitales de manera que se les pueda seguir la pista durante el proceso de entrega y el uso posterior. Marcar al agua o tomar huellas son dos técnicas que normalmente se emplean para marcado de contenidos. Los módulos de DRM en el sistema también transportan, almacenan y generan, de una forma segura, claves criptográficas para usar en el proceso de encargo y distribución de contenidos digitales. Las claves se emplean para proteger criptográficamente los mensajes, incluyendo los contenidos digitales reales, durante la entrega sobre la red.

Los módulos de DRM también realizan la aplicación y gestión de las reglas de uso. Los contenidos digitales encargados se asocian con un cupón, licencia o permiso digital que especifica los derechos y las reglas de uso del cliente de los medios digitales obtenidos. Esta forma de gestión es sobre los contenidos digitales en sí mismos y se ocupa de cuestiones tales como, quién los adquiere, como se entregan, cómo pueden ser usados (presentados, guardados, enviados, copiados, ejecutados, borrados y/o modificados), cuántas veces pueden ser usados, cuánto tiempo duran los derechos, quién hace el pago, cuánto pagan y cómo. Algunas o todas estas cuestiones se especifican en la licencia o cupón, que se puede entregar junto con los contenidos digitales. Para describir las reglas de uso, se han desarrollado lenguajes especiales llamados lenguajes de derechos. Dos de los lenguajes de derechos más frecuentes usados hoy son el Lenguaje de Marcado de Derechos extensible (XrML) y el Lenguaje de Derechos Digitales Abiertos (ODRL). En el dispositivo de uso del cliente, el módulo de DRM se implementa para asegurar que el uso, más a menudo la presentación, sigue lo que se describe en las reglas de uso e impide la repudiación del uso de los contenidos digitales.

Finalmente, el cargo generalmente se refiere al procedimiento del pago real para el uso de los contenidos digitales. Se usan varias técnicas distintas, tales como las técnicas de tarjeta de crédito para el pago en Internet, pago a través de una suscripción o débito en una cuenta.

Un sistema de encargo y distribución de contenidos digitales 1 que incorpora las funcionalidades de DRM se representa esquemáticamente en la Fig. 1, la cual ilustra las partes relevantes y sus relaciones mutuas. El sistema 1 típicamente incluye un cliente 10 que tiene acceso a una red a través de un acuerdo, por ejemplo una suscripción, con un operador de red 20. Esta relación de confianza cliente-operador normalmente se manifiesta en una relación criptográfica, es decir compartir claves simétricas o usar claves públicas, certificadas por una parte de confianza común, si se usa la criptografía asimétrica. Una relación de confianza también se presenta entre el operador de red 20 y un proveedor de contenidos 30, pero en forma de un acuerdo de negocios. Este acuerdo se podría manifestar por una compartición de clave similar y/o acceso de clave como se describe para el cliente 10 y el operador de red 20 arriba. No obstante, entre el cliente 10 y el proveedor de contenidos 30, se establece una relación de confianza inducida cada vez que el cliente 10 obtiene contenidos digitales desde el proveedor de contenidos 30. Esta confianza inducida se manifiesta en una clave de sesión usada para proteger criptográficamente los contenidos digitales según se transmiten al cliente 10 sobre la red.

En un proceso típico de encargo y distribución de contenidos, el cliente 10 en primer lugar se conecta al operador de red 20. El operador 20 entonces autentifica el cliente 10 y posiblemente verifica que el cliente 10 tiene un agente de DRM válido para gestionar los metadatos de DRM, tal como las reglas de uso, las claves y los datos cifrados, asociados con los contenidos digitales. El cliente 10 elige los medios o contenidos digitales y especifica algunas reglas de uso seleccionables por el cliente que van a ser válidas para los medios, por ejemplo presentar los medios un número seleccionado de veces o durante un periodo de tiempo dado. En la presente descripción, los contenidos digitales se refieren a los datos digitales que se pueden descargar o difundir de forma continua sobre una red para el uso en un módulo o sistema cliente, y de esta manera incluye por ejemplo audio, vídeo, imágenes, libros electrónicos y otro material de texto electrónico así como programas informáticos.

Un encargo se sitúa entonces en el operador 20, el cual escribe y cifra un cupón que especifica los contenidos encargados y las reglas de uso. El cupón se envía al cliente 10, donde el agente de DRM descifra el cupón y extrae una clave de sesión a partir del cupón recibido. El cupón se puede descifrar mediante medios criptográficos convencionales, por ejemplo usando una clave de una pareja de claves simétricas o asimétricas, asociadas con el cliente 10 y el operador de red 20. Esta clave de descifrado preferentemente es la clave de suscripción cliente-operador, una clave de DRM especial asociada con el agente de DRM, o una clave derivada de cualquiera de estas claves. La clave de sesión extraída se usará eventualmente para descifrar los medios digitales desde el proveedor de contenidos 30. El cliente 10 también recibe una copia del cupón cifrado con la clave de acuerdo del proveedor de contenidos-operador (o una clave derivada de allí). Esta copia del cupón se envía al proveedor de contenidos 30, en el que se extrae la clave de sesión. A partir de entonces, el proveedor de contenidos 30 entrega los contenidos digitales encargados protegidos criptográficamente por la clave de sesión al cliente 10, o bien como datos descargados o bien como datos emitidos. Finalmente, el agente de DRM en el cliente 10 descifra los contenidos digitales mediante la clave de sesión previamente extraída. Los contenidos digitales se pueden usar, por ejemplo presentar, en el módulo cliente o un dispositivo asociado de acuerdo con las reglas de uso. Información adicional respecto a los sistemas de DRM y encargo y distribución de contenidos digitales se puede encontrar en [2; 3].

El proceso de encargo y distribución de contenidos total tratado arriba se da meramente como un ejemplo simplificado para trasladar una imagen general de tales procesos. Para aumentar la seguridad, se pueden introducir más pasos criptográficos y autentificación. Además, el cliente debería pagar por los contenidos encargados, de manera que los pasos de facturación y cargo están más a menudo presentes en el proceso de encargo. Tal cargo se puede realizar por una suscripción al operador de red, debitando en una cuenta del cliente (usuario) con el operador de red o proveedor de contenidos, enviando el número de tarjeta de crédito del usuario al operador de red o una entidad de facturación dedicada, que gestiona el cargo de los contenidos digitales, o por algún otro medio. Además, el operador de red puede proporcionar tanto la red como los contenidos digitales y de ahí actúa tanto como operador como proveedor al mismo tiempo. No obstante, el operador entonces típicamente tiene un servidor de contenidos dedicado y un servidor de operador dedicado, de manera que las partes ilustradas en la Fig. 1 están presentes aunque el operador de red también maneje los servicios que proporcionan los contenidos.

La presente invención también es aplicable a otros sistemas de encargo y distribución de contenidos (y licencias) distintos al sistema de la Fig. 1. Por ejemplo, se ha propuesto un sistema en el que los contenidos digitales y la información de la licencia está pre-empaquetada por un proveedor de contenidos y entonces se almacena en un emisor de derechos. Es, de esta manera, a este emisor de derechos al que el cliente está girando la compra y la recuperación de los contenidos digitales y las licencias. En tal sistema, se establece una relación de confianza inducida directamente entre el cliente y el emisor de derechos, a favor del proveedor de contenidos. El proveedor de contenidos y el emisor de derechos han establecido previamente un acuerdo de negocios, es decir hay una relación de confianza entre medias. Tal acuerdo puede establecer cuáles de los contenidos del proveedor de contenidos el emisor de derechos tiene permitido distribuir a los clientes, bajo qué condiciones tal distribución puede tener lugar, los precios para los contenidos, cualquier restricción de agrupamiento, a qué categoría de clientes (usuarios) se puede entregar los contenidos, etc. De esta manera, en tal sistema, el proveedor de contenidos no se implica directamente en la interacción con el cliente, es decir no autentifica los clientes ni gestiona las transacciones de pago y los contenidos digitales desde y hacia los clientes, respectivamente. En su lugar, tal interacción del cliente se delega al emisor de derechos. Esta separación en las tareas es atractiva tanto desde el punto de vista del proveedor de contenidos como del emisor de derechos. El proveedor de contenidos tiene un canal de distribución para los contenidos digitales sin estar implicado directamente. En una implementación típica, un operador de red a menudo cubre el papel del emisor de derechos. En tal caso, la separación de tareas puede ser muy atractiva para el operador de red (emisor de derechos), permitiendo al operador entregar los contenidos sobre una base de clientes y ser capaz de ofrecer contenidos y servicios interesantes. Al mismo tiempo, el operador obtiene ingresos de los servicios de contenidos y no solo de los servicios de transporte tradicionales. La presente invención de esta manera también se puede emplear en tal sistema de encargo y distribución de contenidos. Realmente, la enseñanza de la presente invención no depende del sistema real o los mecanismos para el encargo y distribución de los contenidos y de esta manera se puede usar en conexión con cualquiera de tales sistemas.

En algunas aplicaciones también es posible que otro cliente pueda actuar como un proveedor de contenidos. No obstante, las reglas de uso entonces se trasladan al cliente que recibe los contenidos desde el operador de red o el proveedor de contenidos.

Un aspecto de la presente invención se dirige generalmente hacia impedir o disuadir al usuario de repudiar el uso de los contenidos digitales encargados de acuerdo con las reglas de uso asociadas con los contenidos o que intentan violar las reglas. Por ejemplo, al usuario se le puede haber permitido, de acuerdo con la licencia, presentar unos contenidos digitales específicos dos veces, pero está en desacuerdo con el agente de DRM en el módulo o sistema cliente que se han realizado dos presentaciones realmente. La presente invención reduce este riesgo monitorizando el uso de los contenidos digitales y registrando la información que concierne al uso individualmente para cada uso que va a ser monitorizado. La información de uso registrada se enlaza al usuario/cliente, permitiendo una identificación desde qué usuario/cliente se origina la información de uso. Esta vinculación se obtiene preferentemente realizando una operación de seguridad, tal como realizar al menos una parte de la autentificación de la información de uso, que se trata en más detalle abajo. Registrando o grabando la información del uso del cliente y estableciendo una conexión o relación entre el cliente y la información o asociando de otro modo la información de uso con el cliente, la invención tiene un efecto de disuasión de repudiación de uso en los usuarios, que baja el riesgo de que los usuarios violen las reglas de uso de los contenidos digitales encargados. La información de uso generada también se puede usar si está presente un desacuerdo entre el usuario y el proveedor de contenidos (agente de DRM). Simplemente investigando el registro, la información sobre el número real de usos realizado por el cliente, cuándo fueron realizados, la calidad obtenida durante las sesiones de uso (dependiendo de que esté incluida en la información de uso) se puede identificar y recuperar, y usar para resolver discusiones.

Además, el registro de la información de uso de acuerdo con la presente invención también se puede emplear como una base para cargar los contenidos digitales encargados y proporcionados, en particular si se usa el pago posterior. En tal caso, la información en el registro se usa por el operador de red, el proveedor de contenidos o alguna entidad de facturación para determinar la cantidad para cargar una cuenta del usuario por el uso de los contenidos digitales encargados. Esta cuenta podría ser una cuenta bancaria del usuario o una cuenta dedicada del usuario establecida con el operador de red o el proveedor de contenidos. También, una cuenta asociada con un número de tarjeta de crédito del usuario es cargable de acuerdo con la invención. En cualquiera de los dos casos, la cuenta se asocia típicamente con un individuo, que podría ser la persona que encarga o que usa los contenidos digitales. Alternativamente, el individuo es un grupo de clientes o usuarios, que incluye compañías y otras asociaciones. Realizando adecuadamente la operación de seguridad de acuerdo con la invención será posible permitir la identificación de una cuenta y la vinculación de la cuenta a la información de uso registrada. En otras palabras, debido a la operación de seguridad es posible identificar la información de uso registrada como que está asociada con una cuenta, incluyendo el identificador de pago asociado del usuario/cliente, en lugar de, o además de, un cliente o un individuo.

La operación de seguridad de la invención para permitir la identificación de una cuenta o individuo (cliente) vinculando la información de uso registrada a la misma se puede realizar de una serie de formas distintas. En primer lugar, al menos parte de una autentificación de la información de uso se puede realizar por el cliente. Esta autentificación podría ser una firma de la información de uso que usa una clave de firma privada de un par de claves asimétricas, donde la clave de verificación pública asociada junto con un certificado en la clave pública se certifica por una parte de confianza, por ejemplo el operador de red. Alternativamente, se puede adjuntar una etiqueta de autentificación basada en claves simétricas a la información de uso registrada, que permite la identificación de las

cuales se deriva la información implicando a una tercera parte de confianza que conoce la clave simétrica. El origen de la información de uso también se podría identificar, al menos implícitamente, cifrando o protegiendo criptográficamente la información de uso con una clave protegida. Una copia de la clave, junto con o asociada con la información que identifica una cuenta o cliente/usuario, se almacena en una parte de confianza. No obstante, tal cifrado básicamente da solamente autentificación implícita, confiando suficiente redundancia en la información registrada. En cualquier caso, el cifrado podría ser deseable todavía, por ejemplo para proteger la privacidad de los usuarios, sin revelar qué contenidos consume el usuario.

Alternativamente, el cliente podría enviar la información de uso generada a una tercera parte de confianza que realiza la operación de seguridad real.

Otra posible operación de seguridad es almacenar la información de uso registrada en un entorno que es inaccesible para el usuario, pero asociado al mismo o al sistema cliente. Un ejemplo típico es el entorno de un módulo de identidad de abonado (SIM). Para activar el entorno del SIM el usuario típicamente introduce un código pin o código de seguridad personal. No obstante, aunque se activa el entorno y el agente de registro puede almacenar la información de uso registrada en este área segura, el usuario realmente no tiene acceso físico a la misma, es decir no es capaz de modificar o eliminar el registro del SIM. Dado que el SIM se emite por un proveedor de servicios (red) y se asocia con un acuerdo de servicio (suscripción) entre el usuario y el proveedor de servicios, es, de esta manera, posible posteriormente asociar el SIM y consecuentemente el registro almacenado inmediatamente después con el usuario.

Las operaciones de seguridad identificadas arriba se dan meramente como ejemplos ilustrativos, y otras operaciones que permiten la identificación de la cuenta y/o el individuo asociado con la información de uso también están dentro del alcance de la invención como se define por las reivindicaciones adjuntas. Por ejemplo las operaciones de seguridad y los métodos de no repudiación, o variantes de los mismos, mencionados en las referencias [4-6] se podrían emplear de acuerdo con la invención.

Se anticipa por la invención que la persona real que usa los contenidos digitales encargados puede ser diferente del individuo que encarga y paga los contenidos digitales. No obstante, desde el punto de vista de la DRM es el individuo real que encarga, o el pagador real, que reconoce las reglas de uso en la licencia o el cupón asociado con los contenidos digitales el que va a ser responsable para el proveedor de contenidos, si hay un desacuerdo o discusión sobre el uso de los contenidos digitales.

En la presente invención, el uso de los contenidos digitales proporcionados se dirige hacia los métodos de usar los contenidos por el cliente. Este uso podría incluir: la presentación de los contenidos por el cliente, por ejemplo reproducir audio o vídeo, visualizar imágenes o texto y/o imprimir los contenidos digitales; guardar los contenidos en el sistema cliente o algunos otros medios adecuados; enviar los contenidos digitales, por ejemplo a otro cliente o sistema cliente; hacer copias de los contenidos; borrar los contenidos obtenidos; ejecutar los elementos de código de los contenidos digitales (que están en forma de programas informáticos) y/o modificar los contenidos digitales. En una aplicación preferente, las reglas o derechos de uso de los métodos relevantes de uso se especifican en el cupón y/o la licencia asociada con los contenidos digitales.

A continuación, se describen las realizaciones de la presente invención con el uso de los contenidos digitales en la forma de la presentación de los contenidos. Un sistema cliente entonces incorpora o se asocia, por ejemplo directa o indirectamente conectado, con un reproductor o dispositivo de presentación para presentar los contenidos digitales. Adicionalmente, la operación de seguridad de acuerdo con la invención para identificar la cuenta o el individuo asociado con la información de uso generada es ejemplificada, a continuación, como la autentificación de la información de uso. No obstante, como el experto en la técnica comprende, la invención no se limita a las realizaciones de autentificación y/o presentación, sino que comprende cualquier otro método de uso de los contenidos por un cliente y cualquier operación de seguridad que permita la identificación del usuario/cliente, incluyendo las operaciones de seguridad y uso descritas arriba. En tal caso, el dispositivo de presentación se cambia de la misma manera con la función, dispositivo o medios de uso relevantes, y la unidad de autentificación de la información de uso se cambia por consiguiente. También es posible tener un dispositivo de uso que puede realizar alguno o todos los usos anteriores, por ejemplo es capaz tanto de presentar, copiar, guardar, eliminar como enviar los contenidos digitales. El sistema del cliente también puede incluir, o en su lugar, varios dispositivos de uso autónomos, tales como un dispositivo de presentación, un dispositivo de envío, etc.

Un módulo o sistema cliente 10 de acuerdo con la presente invención se ilustra en la Fig. 2. El módulo cliente 10 puede ser cualquier forma de aplicación, que puede encargar y obtener contenidos digitales sobre una red, por ejemplo un ordenador personal (PC) o una unidad móvil, incluyendo teléfonos móviles, asistentes digitales personales o comunicadores. El módulo 10 comprende una unidad de comunicación de entrada/salida (I/O) 110 para gestionar la comunicación entre el módulo cliente 10 y las unidades externas, incluyendo el proveedor de contenidos. Adicionalmente, la unidad I/O 110 incluye la funcionalidad para descargar o difundir de forma continua los contenidos digitales desde un proveedor de contenidos al módulo 10, donde un reproductor o dispositivo de presentación 300 presenta los contenidos. El dispositivo de presentación 300 se podría implementar en programas informáticos, componentes lógicos o una combinación de los mismos. Preferentemente, el dispositivo de presentación 300 incluye un procesador de medios 340, el cual puede ser implementado en programas informáticos, para la presentación de los contenidos digitales usando por ejemplo una pantalla 342 y/o un altavoz 344, dependiendo del tipo de contenidos

digitales. El dispositivo de presentación 340 se puede integrar en la unidad móvil o PC 10, como se ilustra en la Fig. 2, pero también se puede proporcionar como un dispositivo autónomo, directa o indirectamente conectado al mismo.

El módulo del cliente 10 también se proporciona con un agente de DRM 130 para gestionar los metadatos de DRM asociados con los contenidos digitales. Este agente de DRM 130 se implementa para descifrar los contenidos digitales obtenidos desde el proveedor de contenidos usando claves de sesiones e imponiendo la presentación solamente de acuerdo con las reglas de uso. Una parte de esta funcionalidad de DRM 330 se puede implementar en el dispositivo de presentación 300, donde se realiza la presentación de los contenidos reales. Esta funcionalidad de DRM 330 asociada al dispositivo de presentación se puede gestionar por ejemplo imponiendo reglas y típicamente también el descifrado de los contenidos digitales protegidos previos a las presentaciones de los mismos.

De acuerdo con la presente invención, se proporciona un agente de registro 150 en el módulo cliente 10, preferentemente en el agente de DRM 130, para monitorizar el uso, en esta presentación de la realización, de los contenidos digitales descargados, emitidos o difundidos de forma continua. Este agente de registro 150 genera y registra la información de uso que concierne a las presentaciones de los contenidos digitales individualmente para cada presentación que va a ser monitorizada. Una unidad de autentificación 160 también se proporciona en el módulo cliente 10, tal como en el agente de DRM 130, para realizar al menos una parte de la autentificación de la información de uso generada desde el agente de registro 150. La unidad de autentificación 160 preferentemente usa una clave asociada con el módulo cliente 10 y/o el agente de DRM 130 para los propósitos de autentificación. La autentificación, tal como la firma, de la información de uso con la clave permite la identificación del individuo que posee el módulo cliente 10, o de otro modo se asocia con ello. La unidad de autentificación 160 se puede configurar para autentificar la información de uso una vez que se genera por el agente de registro 150. La información generada y autentificada se envía entonces a los medios de almacenamiento para almacenar como una entrada de registro en un registro 170, 175. Este registro de uso 170, 175 se puede disponer localmente en el módulo del cliente 10 o externamente. En el primer caso, el registro 175 se almacena preferentemente de tal manera que es difícil para un atacante modificar o eliminar la información de uso en el registro 175. Esto se puede consumar almacenando el registro 175 en un dispositivo a prueba de sabotajes, al que por ello es más difícil de acceder y modificar. Otra solución podría ser almacenar el registro 175 en algún lugar en el módulo cliente 10, en el que es difícil de localizar para un atacante, y/o usar un formato del registro 175, que no da información o pistas sobre su contenido. El registro almacenado localmente 175 se puede disponer en el agente de registro 150, en el agente de DRM 130 y/o en algún otro lugar en el módulo cliente 10. No obstante, la información de uso se envía preferentemente desde el agente de registro 150 y la unidad de autentificación 160 en el módulo del cliente 10 a un registro externo 170 proporcionado por una parte de confianza, por ejemplo un nodo de red. Esta parte de confianza podría ser el operador de red o alguna otra parte, que el cliente y el proveedor de contenidos confíen ambos.

Alternativamente, la información de uso generada desde el agente de registro 150 se puede enviar, al menos temporalmente, al registro local del cliente 175 para el almacenaje allí dentro, sin ser primero autentificado. No obstante, si la información de uso va a ser transmitida posteriormente al registro externo 170 en (un nodo de) la parte de confianza, preferentemente se autentifica primero por la unidad de autentificación 160 previo a la transmisión.

Si la información de uso se envía al registro externo 170, la información se puede enviar como se genera y autentifica. La información de uso en su lugar se puede almacenar temporalmente en el agente de registro 150 o en el registro local 175 y entonces enviar intermitentemente al registro externo 170. La información también se podría enviar una vez que se han consumido todas las presentaciones asociadas con unos contenidos digitales, es decir cuando se han consumido el número de presentaciones especificadas en las reglas de uso o cuando ha trascurrido el tiempo de presentación permitido. Además, la información de uso generada se puede enviar tras una petición desde el proveedor de contenidos y/o el operador de red. La información de uso generada y autentificada se puede almacenar inicialmente en el registro local 175 y solamente se transmite al registro externo 170, cuando la memoria del registro del cliente 175 está llena, o casi llena.

También se pueden usar dos registros 170, 175, un registro local 175 almacenado en el módulo del cliente 10 y un registro externo 170 almacenado en la parte de confianza.

El agente de registro 150 y/o la unidad de autentificación 160 se puede implementar en el módulo cliente 10 en los programas informáticos, componentes físicos o una combinación de los mismos. El módulo cliente 10 se puede prefabricar con el agente de registro 150, o el agente de registro 150 se puede descargar sobre la red desde por ejemplo el operador de red e implementar en el módulo del cliente 10, lo cual se trata en más detalle debajo.

La Fig. 3 ilustra esquemáticamente el sistema de encargo y distribución 1 de la Fig. 1 y las partes relevantes en más detalle. El módulo o sistema cliente 10 comprende, como se trató arriba, una unidad de comunicación de entrada/salida 110 para descargar o difundir de forma continua los contenidos digitales desde un proveedor de contenidos 30 sobre una red 40 gestionada por un operador de red 20. El proveedor de contenidos 30 incluye un servidor 34 o base de datos con los contenidos digitales que van a ser proporcionados a los clientes. De la misma manera al sistema cliente 10, el proveedor de contenidos 30 comprende los medios 32 para descargar, emitir o difundir de forma continua los contenidos al cliente, en el que se presenta por un dispositivo de presentación 300. La información de uso que concierne a la presentación se genera en un agente de registro 150 y se autentifica 160 antes de ser transmitida a una parte externa. Esta parte externa se representa en la Fig. 3 mediante el operador de red 20, el cual recibe, por medio de su unidad de comunicación de entrada/salida 22, la información de uso autentificada y la

almacena como una entrada de registro en un registro de uso 170 proporcionado en una ubicación de almacenamiento 180.

Como se mencionó anteriormente, el dispositivo de presentación se puede integrar en el módulo cliente, es decir por ejemplo el ordenador personal (PC) o unidad móvil. No obstante, el sistema cliente alternativamente puede comprender dos unidades separadas, una unidad para realizar la recepción (por ejemplo descargar o difundir de forma continua) de los contenidos digitales y una unidad que realmente presenta los contenidos digitales, es decir el dispositivo de presentación. En tal caso, la unidad de recepción está físicamente separada de la unidad autónoma que realmente presenta los contenidos digitales. Este dispositivo de presentación autónomo no obstante está directamente (a través del puerto de comunicación adecuado) o indirectamente conectado con la unidad de recepción. La unidad de recepción puede ser por ejemplo un PC o una unidad móvil con los componentes físicos/programas informáticos adecuados para recibir los contenidos digitales. Los contenidos entonces se transmiten preferentemente al dispositivo de presentación a través de cables ordinarios o mediante comunicación inalámbrica con o sin la implicación de una red. Alternativamente, el PC o unidad móvil puede almacenar los contenidos digitales recibidos en algún medio portátil adecuado, incluyendo discos flexibles, discos duros, discos MD, discos CD-ROM, discos DVD, tarjetas rápidas compactas, tarjetas inteligentes, etc. El usuario entonces puede mover el medio portátil con los contenidos digitales al dispositivo de presentación para la presentación en los dispositivos de presentación autónomos de contenidos Típicos incluidos los reproductores Mp3, los reproductores MD, los reproductores CD, los reproductores DVD, otras unidades móviles o PC.

Con referencia a la Fig. 4, el sistema del cliente 10 comprende un dispositivo de recepción 200 para descargar y/o difundir de forma continua los contenidos digitales desde un proveedor de contenidos, y/o proporcionar los contenidos como datos emitidos. Además, se proporciona un dispositivo de presentación autónomo 300 que incluye el procesador de medios 340 y los medios que interactúan con el usuario, por ejemplo la pantalla 342 y/o el altavoz 344, en el sistema del cliente 10. El dispositivo de recepción 200 incluye una unidad de comunicación de entrada/salida (I/O) 210 para gestionar la comunicación por una parte con el proveedor de contenidos sobre una red, por ejemplo la descarga o difusión de forma continua de los contenidos digitales de allí, y para proporcionar los contenidos digitales recibidos al dispositivo de presentación 300. La unidad de I/O 210 puede transmitir los contenidos digitales a través de un cable a una unidad de I/O 310 correspondiente en el dispositivo de presentación 300. Alternativamente, los contenidos se podrían transmitir sobre una red a la unidad de I/O 310 o grabar en un medio adecuado y entonces transferir manualmente al dispositivo de presentación 300, en el que la unidad de I/O 310 lee los contenidos digitales. Adicionalmente, un agente de DRM 230 se dispone preferentemente en el dispositivo de recepción 200 para gestionar los metadatos de DRM asociados con los contenidos digitales.

El dispositivo de presentación 300 en la Fig. 4 se proporciona del mismo modo con un agente de DRM 330 que gestiona el descifrado de los contenidos digitales y que impone las reglas de uso asociadas. En la presente realización, se implementa un agente de registro 150 de acuerdo con la presente invención en el dispositivo de presentación 300, preferentemente en el agente de DRM 330 del dispositivo de presentación 300. Este agente de registro 150 genera la información de uso que concierne a las presentaciones de los contenidos digitales individualmente. La información de uso generada se puede almacenar entonces como una entrada de registro en un registro de uso 175-1 proporcionada en el dispositivo de presentación 300. En tal caso, la información de uso se puede almacenar sin ser primero autentificada. Alternativamente, o además, la información de uso se transmite al dispositivo de recepción 200 que usa las unidades de I/O 210 y 310, respectivamente. Una vez recibida, la información de uso se puede almacenar en un registro local 175-2. No obstante, la información de uso preferentemente se autentifica usando una unidad de autentificación 160 implementada en el dispositivo de recepción 200, tal como en el agente de DRM 230 asociado. La información de uso autentificada ahora se puede almacenar en el registro 175-2 y/o transmitir a una parte de confianza para almacenar en un registro externo 170.

Aunque, la unidad de autentificación 160 es implementada en el dispositivo de recepción 200 del sistema del cliente 10 en la Fig. 4, se prevé por la invención en lugar de implementar la unidad de autentificación 160, o además de implementar una unidad de autentificación correspondiente, en el dispositivo de presentación 300, preferentemente en el agente de DRM 330 del dispositivo de presentación 300. En tal caso, la información de uso a partir del agente de registro 150 se puede autentificar en conexión con la generación de la misma.

Una implementación típica de un agente de registro 150 y una unidad de operaciones de seguridad 160, que ilustran sus elementos de inclusión, se muestra en la Fig. 5. El agente de registro 150 comprende un generador 152 para generar la información de uso que concierne al uso de los contenidos digitales individualmente para cada uso. Este generador 152 recibe los datos de entrada desde distintos medios externos, dependiendo de qué información de uso va a ser generada y registrada. En un caso típico, el generador 152 recibe los datos de entrada desde por ejemplo los medios de uso, o más precisamente desde el agente de DRM que gestiona el uso de los contenidos digitales, la licencia o el cupón asociado con los contenidos digitales recibidos, etc. A partir de esta entrada, el generador de información 152 crea la información de uso relevante, más de la cual a continuación, y la almacena temporalmente en una caché 154 o memoria temporal similar.

La información de uso entonces preferentemente se envía, preferentemente de una manera segura, por ejemplo usando cifrado/autentificación o un canal seguro, a la unidad de operaciones de seguridad 160 para que se

conecte o asocie con una cuenta o individuo, típicamente el propietario del sistema del cliente o el abonado a un operador de red, permitiendo la identificación a partir de la cual se origina la información de uso.

En esta realización, se proporciona un motor de cifrado 164 para impedir criptográficamente el acceso no autorizado a la información de uso generada desde el agente de registro 150 en la unidad de operaciones de seguridad 160. Este motor de cifrado 164 se dispone para cifrar la información de uso usando una clave de cifrado 166. La clave de cifrado 166 puede ser una clave simétrica compartida, una copia de la cual se almacena en una parte de confianza, por ejemplo el operador de red, el proveedor de contenidos o alguna otra parte de confianza. Alternativamente, se pueden usar una pareja de claves asimétricas para cifrar el cifrado de la información de uso. La unidad de operaciones de seguridad 160 entonces comprende una clave pública 166 de una parte de confianza junto con un certificado en la clave pública. La información de uso cifrada solamente se puede leer entonces por la parte de confianza usando su clave privada para el descifrado de la información protegida criptográficamente.

Además de proteger criptográficamente la información de uso generada a partir del agente de registro 150, la información de uso también se puede autentificar permitiendo la identificación de la cual se deriva la información. De esta manera se proporciona una unidad de autentificación 162 para autentificar la información de uso en la unidad de operaciones de seguridad 160. La unidad de autentificación 162 puede añadir una etiqueta de autentificación a la información de uso. La etiqueta podría ser una firma digital añadida a la información usando una clave de firma privada 166 de una pareja de claves asimétricas. La clave de verificación pública asociada junto con un certificado sobre la clave pública se almacena en una parte de confianza. También se puede usar la autentificación de mensajes, por ejemplo usando claves simétricas 166, para autentificar e identificar el origen de la información de uso.

Una forma de hacer esta autentificación del registro de la información de uso de acuerdo con la invención es dejando el agente de DRM en el visualizador del sistema cliente una petición en el interfaz de usuario del sistema del cliente cuando el dispositivo de uso asociado con el sistema cliente ha usado los contenidos digitales. Esta petición incita al usuario (o posible cliente en sí mismo) a confirmar que ha sido realizado un uso. En este caso, para evitar la situación de no dar respuesta del todo, el agente de DRM se puede implementar para prohibir el uso adicional de los contenidos digitales hasta que se da una respuesta, sea positiva o negativa, a la petición de autentificación. Si se da una respuesta positiva, la información de uso se autentifica y almacena como una entrada de registro en el registro de uso. No obstante, una respuesta negativa, es decir que el usuario no acepta el uso como que se realiza exitosamente ni que la información de uso se debería introducir en el registro, puede iniciar distintas actividades del agente de DRM. La estrategia a seguir por el agente de DRM podría ser fijada o podría ser especificada en la licencia o cupón asociado con los contenidos digitales. En el último caso, el proveedor de contenidos tiene la posibilidad de ajustar la estrategia para hacer coincidir los contenidos y las propiedades del sistema del cliente. Por ejemplo, para contenidos digitales de bajo valor, uno o más usos adicionales podrían ser aceptables para una respuesta de autentificación de registro negativa, mientras que para contenidos digitales de alto valor el agente de DRM envía un mensaje automático al proveedor de contenidos, para que el proveedor de contenidos resuelva la cuestión. De esta manera, en caso de que esta estrategia sea parte de la licencia o cupón, la estrategia tendrá que ser protegida de ser accesible al usuario, ya que de otro modo podría adoptar su estrategia de respuesta en consecuencia, por ejemplo siempre responder negativamente y obtener por ello usos adicionales (libres de cargo) si se emplea tal estrategia. El cifrado de la estrategia que contiene parte de la licencia podría dar esta protección.

La información de uso generada desde el agente de registro 150 puede, de esta manera, ser cifrada, autentificada o cifrada y autentificada. La(s) clave(s) usada(s) para proteger criptográficamente y/o autentificar la información de uso podrían ser clave(s) de suscripción asociada(s) con una suscripción entre el cliente y el operador de red, o clave(s) derivada(s) de allí. Por ejemplo, el cliente puede tener un módulo de identificación de suscripción de red, expedido por el operador de red, dispuesto en el sistema cliente. Este módulo de identificación de suscripción de red a su vez comprende una clave usada para autentificar el cliente al operador. Tal clave de suscripción también se podría usar para protección criptográfica y/o autentificación de la información de uso. Las claves específicas asociadas con el agente de DRM en el sistema cliente y usadas en el sistema de DRM también se pueden usar para propósitos de cifrado y/o autentificación respecto a la información de uso. Además, las claves específicas asociadas con el sistema del cliente como tal, que incluyen las claves del dispositivo, se pueden usar para el cifrado y/o autentificación de los contenidos digitales. También, los nombres de usuario y las contraseñas asociadas a la suscripción se pueden usar en este contexto. Si el cliente tiene una, o varias direcciones IP asociadas al mismo, tal(es) dirección(es) se puede(n) usar, también en algunos casos, para la autentificación de la información.

La información de uso autentificada y cifrada o posiblemente cifrada/autentificada y generada se envía entonces desde la memoria caché temporal 154 o bien a un registro almacenado en el sistema cliente o bien a través de un expedidor 156 adaptado para enviar la información de uso a un registro externo en una parte de confianza.

Aunque la unidad de operaciones de seguridad 160 en la Fig. 5 se ha ilustrado como una unidad autónoma conectada al agente de registro 150, su funcionalidad, en particular la funcionalidad de autentificación de la unidad de operaciones de seguridad 160 se podría implementar en el agente de registro 150. En caso de una implementación distribuida, es decir la unidad de operaciones de seguridad 160 autónoma, la comunicación entre la unidad 160 y el agente de registro 150 se asegura preferentemente.

La Fig. 6 ilustra un registro 170 y los ejemplos de información de uso que se puede encontrar en una entrada de registro 172. Como se mencionó en lo anterior, el registro 170 se almacena o bien localmente en el módulo o sistema cliente y/o externamente en una parte de confianza en alguna memoria o medios de almacenamiento 180. Si se almacena en una parte de confianza, cada registro 170 se puede asociar con un cliente específico, que contiene solamente las informaciones de uso de ese cliente. Puede ser posible, no obstante, almacenar la información de uso de varios clientes distintos en un registro 170. La información entonces se autentifica, identificando desde qué cliente se deriva la información.

Las entradas de registro 172 en el registro 170 comprenden la información de uso asociada con el uso, por ejemplo las presentaciones, de los contenidos digitales por un sistema cliente. La información del uso puede incluir una representación 172-1 o descripción de los contenidos digitales usados, por ejemplo una huella que identifica los contenidos o el nombre del archivo asociado con los contenidos. Típicamente las huellas podrían ser los contenidos en sí mismos, una copia o parte de los mismos. También se puede usar un valor de la función de generación de claves de los contenidos digitales o una parte de los mismos para obtener una representación de los contenidos. Otra representación de contenidos posible es un URI (Identificador Universal de Recursos) o URL (Localizador Uniforme de Recursos), el cual especifica la dirección y el nombre posible del contenido) de los contenidos digitales, por ejemplo la dirección en el servidor del proveedor de contenidos, desde el cual se pueden traer los contenidos.

La información de uso también podría comprender la información que concierne a la calidad 172-2 de los contenidos o el uso de los contenidos. Esta forma de información se puede usar para comprobar si el uso ha sido realizado de acuerdo con la calidad de uso especificada en las reglas de uso de la licencia, es decir el uso debería tener la calidad por la que el cliente ha pagado realmente. Distintas cantidades se pueden usar para definir y expresar la calidad de presentación. Ejemplos típicos son el ancho de banda o la resolución de los contenidos digitales. También la velocidad de la muestras de los contenidos digitales, la velocidad de compresión de los datos, etc., se puede usar como una cantidad de la calidad. Los contenidos digitales en sí mismos, o una representación de los mismos, también podrían constituir una cantidad de la calidad. Por ejemplo, si el cliente encarga y recibe contenidos digitales que especifican el precio de las participaciones de una empresa, para el propósito de adquirir acciones en esa compañía, es muy importante que los contenidos recibidos (precio de las participaciones) esté correcto y actualizado. En tal caso, los contenidos, una representación de los mismos y/o el tiempo de recepción de los contenidos se pueden incluir como calidad de uso en la información de uso. Si el cliente posteriormente reclama que ha recibido un precio de las participaciones incorrecto o muy retardado, el proveedor de contenidos simplemente puede recuperar el precio de las participaciones, obtenido por el cliente, a partir del registro. También, la información de cualquier interrupción que ocurra durante el uso de los contenidos digitales es una cantidad de la calidad de acuerdo con la invención. Esta información de interrupción podría fijar cuántas interrupciones hubo durante el uso, cuándo ocurrieron las interrupciones, durante cuánto tiempo duraron las interrupciones, etc.

También la información sobre la cantidad de uso se puede introducir en la información de uso. Tal cantidad podría especificar cuántos usos de los contenidos digitales que han sido realizados por el cliente y/o cuántos usos restan de acuerdo con las reglas de uso.

La forma de uso, es decir la identificación de qué tipo de uso que se realiza, incluyendo presentación, envío, copia, ejecución, modificación, eliminación, etc., se puede encontrar en la información de uso.

La información de uso preferentemente comprende información sobre el tiempo de uso 172-N. Tal tiempo preferentemente especifica la hora cuando se completa el uso, pero también o en su lugar podría especificar la hora de inicio de la descarga o la recepción de los contenidos, la hora de inicio del uso o alguna otra hora, durante la cual el uso está en curso. En particular para aplicaciones de presentación, pero también para otros métodos de uso, el tiempo total que el uso (presentación) ha mantenido o seguido podría constituir información de uso valiosa y se podría introducir por lo tanto en el registro. Este tiempo de uso total se mide o estima fácilmente usando el agente de DRM, permitiendo el uso de los contenidos digitales en el sistema cliente.

Además, la información de uso de acuerdo con la presente invención se adapta bien para el uso con el servicio basado en la ubicación. Tales servicios se proporcionan mediante por ejemplo los operadores de red, que entonces también actúan como proveedores de contenidos. Típicamente el servicio basado en la ubicación incluye encontrar el pub, restaurante, cine, cajero, hospital, comisaría, etc., más cercanos. También se podría dar la distancia actual y/o la dirección para la ubicación relevante solicitada. En tales aplicaciones, la información de uso puede incluir una representación de la ubicación del cliente cuando encarga el servicio basado en la ubicación, posiblemente junto con los contenidos digitales recibidos (dirección, distancia). Se debería señalar que los servicios basados en la ubicación podrían entrar en conflicto con el interés de privacidad del usuario y preferentemente debería ser posible para el usuario dar consentimiento a la inclusión de los datos de ubicación en la información de uso.

Para juegos y otros contenidos digitales de programas informáticos similares, la puntuación o nivel obtenido por el usuario cuando presenta el juego se puede incluir en la información de uso. Esto puede ser especialmente importante en situaciones en las que el cliente, de acuerdo con la regla de uso, se le permite presentar el juego un número fijado de veces, pero obtiene una o varias presentaciones adicionales gratis si el usuario logra una cierta puntuación o nivel asociado con el juego. Esta puntuación del juego o nivel se introduce preferentemente entonces en el registro de uso.

La presente invención es especialmente atractiva para usar en combinación con juegos asociados con un precio de adjudicación.

Adicionalmente, la entrada en el registro de uso podría comprender un registro de la información sobre el agente de DRM implementado en el sistema del cliente. Tal registro de DRM preferentemente da información de qué, y posiblemente cómo, el agente de DRM se implica en el uso de los contenidos digitales. La información relevante de DRM típica podría ser un número de versión, la representación de una clave asociada con el agente de DRM, o una clave derivada de allí. A partir de la información de DRM entonces es posible controlar y verificar que el sistema cliente realmente incluye un agente de DRM correcto y certificado. De esta manera, la información del uso puede proporcionar una fuente valiosa para controlar continuamente los agentes de DRM de los clientes para detectar cualesquiera fallos de seguridad tan pronto como sea posible.

Como se trató brevemente en conexión con la Fig. 1, cuando un cliente encarga contenidos digitales, típicamente recibe un cupón que comprende las claves de las sesiones usadas para descifrar los contenidos digitales reales. La información asociada con el cupón, tal como el cupón en sí mismo, un valor de la función para generar claves del cupón o un número o código de identificación del cupón se pueden incluir en la información de uso. Además, una vez que el cliente ha recibido el cupón es posible que el usuario desee dar uno o varios de los usos de los contenidos digitales especificados en el cupón a un amigo. En tal caso, el cliente o bien transmite el cupón al sistema cliente del amigo, o bien genera un nuevo cupón, el cual se firma y transmite al amigo, por ejemplo como un SMS (Servicio de Mensajes Cortos), MMS (Servicio de Mensajería Multimedia) o correo electrónico. Adicionalmente, el cupón del cliente se actualiza en consecuencia, es decir reduciendo los usos enviados al amigo del número total de usos especificados en el cupón original. La información de uso entonces incluye preferentemente un identificador del amigo que recibe los usos y la información de los usos dados, por ejemplo cuántos usos, qué tipo de usos. Un registro correspondiente del sistema cliente del amigo incluye entonces un identificador del cliente a partir del cual recibió el cupón o la licencia.

Cuando el proveedor de contenidos va a transmitir los contenidos digitales a un cliente puede incluir información de la hora en la transmisión de los contenidos. Tal información de la hora fija o permite la identificación de una hora cuando se inició o finalizó la transmisión de los contenidos digitales. Además, el proveedor de contenidos preferentemente almacena el tiempo de transmisión en una base de datos o registro o lo proporciona a una tercera parte para almacenar allí dentro. Esta información podría ser una secuencia, número marcado temporal u otro sello de tiempo. La secuencia se puede generar usando una función o algoritmo con el tiempo de transmisión como entrada. Entradas adicionales, pueden ser un identificador del cliente que recibe los contenidos digitales, incluyendo el número de versión, la representación de una clave asociada con el cliente, y un identificador de los contenidos digitales. Una vez recibida la información temporal se incluye en la información de uso. Esta información marcada temporal se puede usar para investigar si el usuario ha manipulado la información de uso. Una vez que se proporciona la información de uso registrada al proveedor de contenidos, o una parte de confianza, el tiempo de transmisión de los contenidos digitales se extrae o se calcula de otro modo a partir de la información marcada temporal. El proveedor de contenidos (o tercera parte) compara entonces esta información temporal extraída con la contraparte almacenada, tratada anteriormente. Si se concluye que este tiempo de transmisión extraído es distinto del tiempo de transmisión real según lo almacenado en el proveedor de contenidos, entonces el usuario probablemente ha manipulado la información de uso.

Información de uso útil adicional de acuerdo con la invención es un identificador de pago de los contenidos digitales. Tal identificador podría expresar que el usuario ya ha pagado por los contenidos digitales (pre-pago) o que el usuario va a pagar por los contenidos (post-pago). Tales identificadores de pago podrían ser el identificador del cupón asociado con los contenidos digitales pero también pueden ser usados otros identificadores, tales como una cuenta del usuario, número de tarjeta de crédito (posiblemente protegida criptográficamente), o identificador de transacción de pago. Esta información de pago se puede obtener entonces a partir del agente de DRM como una parte del mecanismo de cargo de la funcionalidad de DRM.

También se puede incluir alguna información asociada con el dispositivo de uso, que incluye una versión/código identificador o número del dispositivo de uso en la información de uso. Tal información del dispositivo de uso incluye una clave de dispositivo asociada, o una clave derivada de allí. Esta información se puede usar para verificar más tarde que el uso de los contenidos digitales encargados realmente ha sido realizado con un dispositivo de uso aprobado.

El cupón que se recibe antes de descargar o difundir de forma continua los contenidos digitales típicamente incluye una descripción del SDP (Protocolo de Descripción de Sesiones), u otro protocolo de configuración de difusión de forma continua, por ejemplo RTSP (Protocolo de Flujo de Datos en Tiempo Real), SMIL (Lenguaje de Integración Multimedia Sincronizado), etc. Tal descripción del SDP es una descripción textual para describir la sesión que proporciona los contenidos e identifica, entre otros, el URI que especifica la dirección de los contenidos digitales, la información de la dirección del cliente (la dirección de correo electrónico, la Identidad Internacional de Abonado Móvil (IMSI), el Número Internacional de la Red Digital de Servicios Integrados de la Estación Móvil (MSISDN) o el número de teléfono), la información de conexión, la información del ancho de banda y (posiblemente protegida) la(s) clave(s) de cifrado. Esta descripción del SDP generalmente especifica por qué ha pagado el usuario realmente y se puede usar más tarde para comparar con lo que realmente se ha recibido/usado. Por ejemplo, el SDP podría especificar la calidad pagada, por ejemplo el ancho de banda o la velocidad de las muestras, de los contenidos digitales. Si la calidad real también se almacena en el campo de calidad de uso 172-2 de la información de uso, es posible verificar más tarde si el

ancho de banda real correspondió a por el que el usuario ha pagado. De esta manera, la descripción del SDP, una parte de la misma o una función de generación de claves de la descripción o parte de la misma, se incluye preferentemente en la información de uso.

Las entradas de registro también pueden comprender otra información que concierne al uso de los contenidos digitales, tal como especificar cómo ha usado el cliente los derechos asociados con los contenidos digitales y cuántos y qué usos de los contenidos restan de acuerdo con las reglas de uso.

En algunas aplicaciones podría ser posible para el usuario del módulo o sistema cliente especificar alguna de la información que va a ser incluida en el registro. Por ejemplo, el usuario podría introducir el número de la tarjeta de crédito o el identificador o número de cuenta que va a ser cargada por el uso de los contenidos digitales. Adicionalmente, si el usuario ha recibido uno o más cupones que se pueden usar para cargar el uso de los contenidos encargados, el sistema del cliente podría listar cualquiera de tales cupones de cargo disponibles. El usuario entonces puede seleccionar uno o varios cupones para el pago de los contenidos y sus identificadores correspondientes se introducen entonces como información de uso en el registro.

También podría ser posible para el sistema cliente, a través de un interfaz de usuario, presentar un resumen o descripción de la información de uso registrada, o parte de la misma, para el usuario. Adicionalmente, el sistema cliente se podría implementar para visualizar una petición en el interfaz de usuario. Tal petición entonces incita al usuario a confirmar la información de uso registrada: Consecuencias similares como las que fueron tratadas anteriormente en conexión con la autentificación del registro se podrían emplear si el usuario no confirma la información de uso registrada.

La información de uso puede incluir todos o alguno de los elementos tratados anteriormente, o alguna otra información asociada con el uso de los contenidos.

Como se mencionó anteriormente, la información de uso preferentemente se autentifica, permitiendo la identificación del cliente o usuario, especialmente cuando el registro está almacenado externamente. En una implementación típica, se puede añadir una etiqueta de autentificación 174 a la información de uso, como se ilustra en la Fig. 6. Esta etiqueta de autentificación 174 puede ser por ejemplo una firma digital o un código de autentificación del mensaje, calculado por la clave específica del cliente tratada en conexión con la Fig. 5. En lugar de, o como un complemento a, usar una etiqueta de autentificación dedicada 174, la información de uso entera se puede autentificar y/o cifrar usando un cifrado y clave de firma, que tanto protegen criptográficamente como autentifican (en caso solamente de cifrado, la autentificación está implícita) la información de uso. Si la etiqueta se almacena localmente en el sistema cliente, se podría relajar un poco la necesidad de una etiqueta de autentificación o alguna otra forma de información de identificación.

El agente de registro dispuesto en el sistema cliente se podría implementar para generar la información de uso individualmente para cada uso de los contenidos digitales que se realiza por el cliente. En tal situación, cada uso se monitoriza y la información del mismo se registra y se puede recuperar más tarde para resolver los desacuerdos del usuario y el proveedor de contenidos. No obstante, en lugar de monitorizar y registrar cada uso, el agente de registro se puede configurar para monitorizar y registrar la información de uso para usos seleccionados aleatoriamente. El registro también se podría realizar intermitentemente para los usos, por ejemplo cada segundo uso. La cuestión más importante aquí es que la monitorización y el registro del uso de los contenidos digitales debería disuadir al usuario de repudiar el uso de los contenidos. Registrando la información intermitentemente o aleatoriamente, el usuario no es consciente de qué uso se registra y por lo tanto se disuade de repudiar las reglas de uso. Si no se registra cada uso, preferentemente no se debería permitir al usuario conocer qué uso se registra realmente y cuál no. Además, la estrategia usada para registrar la información de uso, por ejemplo qué uso realmente debería ser registrado y/o cuándo debería ser registrado, se puede especificar en la licencia o cupón asociado con los contenidos digitales recibidos.

No obstante, si la información de uso registrada se usa como una base para el cargo, la información de uso que concierne a cada uso preferentemente se genera, autentifica y proporciona a la entidad de cargo.

La información de uso que se origina a partir de los clientes puede proporcionar por su puesto una fuente de información de alto valor sobre el uso real de los contenidos digitales. Tal información puede tener un alto valor potencial para los proveedores de contenidos, cuando se deciden los modelos de negocio, el precio de los contenidos digitales, etc. Dado que la información de uso de varios clientes se puede almacenar junto con uno o varios registros en una parte de confianza, el proveedor de contenidos puede acceder entonces a los registros y usar la información almacenada allí dentro como una fuente de información estadística en la labor del proveedor. En tal caso, la información usada para la recogida de las estadísticas primero se “despersonaliza” preferentemente para proteger la privacidad de los usuarios.

Si se proporcionan los contenidos digitales como datos de difusión de forma continua, el proveedor de contenidos está en línea, comunicando con el dispositivo de presentación del cliente durante la presentación. En esta presentación “sobre la marcha”, el transporte de los contenidos típicamente se hace con un protocolo poco fiable, tal como UDP (Protocolo de Datagrama de Usuario) [7]. Los datos de difusión de forma continua incluyen los contenidos digitales que se presentan en tiempo real según se reciben sobre una red. Los datos también pueden haber sido

almacenados, al menos temporalmente, antes de que tenga lugar la presentación real, lo cual es bien conocido por una persona experta en la técnica. La monitorización de presentaciones y el registro de la información de las mismas se hacen en este caso preferentemente durante la presentación real. De esta manera, durante la presentación de los contenidos digitales, el agente de registro en el sistema cliente genera intermitentemente información que concierne a la presentación en curso. Por ejemplo, el agente de registro se podría implementar para generar la información de uso cada 30 segundos, cada segundo, minuto o algún otro intervalo de tiempo, periódicamente o no. La información de uso generada se almacena entonces en un registro de usuario, como se trató anteriormente. No obstante, la información de uso también se puede enviar preferentemente, típicamente después de ser autentificada, al proveedor de contenidos para la confirmación de la recepción y la presentación de los datos de difusión de forma continua. El proveedor de contenidos se puede equipar con una funcionalidad de DRM que recibe esta información de uso del cliente y solamente continúa difundiendo de forma continua los datos si la información de uso se recibe dentro de un periodo de tiempo predeterminado. De esta manera, el proveedor de contenidos podría terminar el flujo de difusión de forma continua de los contenidos digitales si no se envía la información desde el cliente durante el periodo de tiempo predeterminado.

En algunas aplicaciones de difusión de forma continua, el proveedor de contenidos intermitentemente envía informes de transmisión al cliente. Estos informes pueden incluir información de los contenidos digitales entregados hasta ahora. Tal información puede ser la cantidad de paquetes de datos enviados al cliente y/o la cantidad de los contenidos entregados. Cuando el cliente recibe estos informes de transmisión, el usuario podría responder enviando un informe de recepción, por ejemplo confirmando, aceptando o rechazando aquello que se incluye en la información que realmente se ha culminado, por ejemplo el número especificado de datos de paquetes que ha sido recibido realmente con la correcta calidad de contenidos. El agente de registro entonces se puede implementar para incluir la información de uso generada en los informes de recepción. Si no se recibe la información de uso por el proveedor de contenidos junto con los informes de recepción, el flujo de difusión de forma continua de los contenidos digitales se podría terminar, como anteriormente.

En lugar de, o como un complemento a, terminar el flujo de datos de difusión de forma continua, el agente de registro podría incluir una notificación en la información de uso de que el usuario rechaza la transmisión de, o no ha enviado, la información de uso junto con los informes de recepción al proveedor de contenidos.

Además, los protocolos usados específicamente para la difusión de forma continua de los datos digitales, tal como el Protocolo de Transporte en Tiempo Real (RTP) y el Protocolo de Transporte Seguro en Tiempo Real (SRTP), típicamente tienen un mecanismo de informe, en el que el receptor de los datos de difusión de forma continua, es decir el cliente, envía intermitentemente o periódicamente un informe de recepción del protocolo RTP que acompaña al transmisor de los datos, es decir el proveedor de contenidos [8, 9]. La información de uso generada por el agente de registro entonces se puede incluir y enviar junto con los informes de recepción al proveedor de contenidos. Además, el SRTP proporciona una trama general para proteger criptográficamente los informes. Este cifrado SRTP también se podría usar para proteger la información de uso según se envía sobre la red. En el SRTP también es obligatorio autentificar los informes de realimentación, y esta autentificación se podría extender por ejemplo mediante firmas digitales para propósitos de registro.

Para aumentar la seguridad de la funcionalidad de registro en el sistema cliente, el agente de registro se podría implementar en un dispositivo a prueba de sabotajes, ver Fig. 7. Tal dispositivo hace mucho más difícil para un atacante acceder y modificar el agente de registro y por ello modificar la información de uso generada. También, el registro de uso se puede almacenar en un dispositivo a prueba de sabotajes, evitando por ello el fácil acceso, modificación y eliminación por el usuario del mismo. El dispositivo a prueba de sabotajes preferentemente es portátil y dispuesto de manera extraíble en el módulo o sistema cliente. Tal dispositivo entonces se puede mover entre y usar en conexión con distintos módulos cliente. En tal caso, el módulo cliente preferentemente incluye los medios para recibir y almacenar una licencia asociada con los contenidos digitales recibidos. Además, un adicionador para adjuntar el registro de uso a la licencia se dispone preferentemente en el módulo cliente. Este adicionador adjunta el registro a la licencia de manera que cuando el módulo a prueba de sabotajes se mueve a otro módulo cliente, tanto la licencia como el registro acompañan al dispositivo al nuevo módulo cliente. No obstante, el adicionador preferentemente debería dejar la licencia intercambiada salvo que adjunte el registro al mismo.

La Fig. 7 ilustra una realización de un módulo cliente 10 que incorpora una unidad de comunicación de entrada/salida (I/O) 510, un dispositivo de presentación 300 y un dispositivo a prueba de sabotajes 400. La unidad I/O 110 típicamente implementa una pila de protocolos de comunicación de red, de esta manera permite la descarga o difusión de forma continua de los contenidos digitales desde un proveedor de contenidos. Como para las realizaciones anteriores, el dispositivo de presentación 300 comprende un procesador de medios 340, pantalla 342 y/o altavoz 344 para presentar los contenidos digitales y, preferentemente, un agente de DRM 330. Un agente de DRM 430 también se dispone preferentemente en el dispositivo a prueba de sabotajes 400. En tal caso, el agente de registro 150 se puede implementar en el agente de DRM 430 asociado con el dispositivo a prueba de sabotajes 400. Una unidad de autentificación 160 para autentificar la información de uso a partir del agente de registro 150 se proporciona en el módulo cliente 10, preferentemente en el dispositivo a prueba de sabotajes 400 o en su agente de DRM 430.

La realización del módulo cliente 10 en la Fig. 7, podría ser una unidad móvil, por ejemplo un teléfono móvil. Esta ofrece una ventaja comparada con si el agente de registro de la invención se dispone en un ordenador. Esta ventaja se manifiesta en una seguridad potencialmente aumentada contra piratería, debido a que las plataformas de los

sistemas operativos del ordenador, por ejemplo Windows y Linux, son mucho mejor conocidas por el público que las plataformas correspondientes de las unidades móviles, las cuales por ello llegan a ser más difíciles de atacar y modificar. Por lo tanto, un agente de registro de acuerdo con la presente invención es muy adecuado para la implementación en una unidad móvil.

Una solución particularmente atractiva es cuando el agente de registro se implementa en un dispositivo a prueba de sabotajes emitido por una parte de confianza tanto por el cliente como el proveedor de contenidos. Esta parte de confianza por ejemplo podría ser el operador de red, que tiene un acuerdo contractual con el proveedor de contenidos para proporcionar a sus abonados con módulos cliente. Tal dispositivo a prueba de sabotajes proporcionado por el operador podría ser un módulo de identidad, incluyendo los módulos de identidad de abonado (SIM) de red. Este SIM de red puede ser una tarjeta inteligente leída por un lector de tarjetas conectado al módulo cliente. Otra solución es usar tarjetas SIM estándar usadas en las unidades móviles del GSM (Sistema Global para Comunicaciones Móviles) y cualquier otra SIM de red conocida en la técnica, incluyendo también SIM de UMTS (Servicio Universal de Telecomunicaciones Móviles) (USIM), ISIM (Módulo de Identidad de Servicios Multimedia de Internet) WIM (Módulo de Identidad Inalámbrico), y más generalmente módulos UICC (Tarjeta Universal de Circuitos Integrados). No obstante, también se pueden proporcionar otras tarjetas que tienen funcionalidades similares como las tarjetas SIM estándar, por ejemplo las tarjetas inteligentes usadas para transacciones bancarias, con un agente de registro de acuerdo con la presente invención. Por ejemplo, el módulo de identidad a prueba de sabotajes podría ser una tarjeta inteligente asociada con un receptor multimedia digital para TV por satélite o un módulo de identidad a prueba de sabotajes para un centro general de entretenimiento de hogar digital.

La Fig. 8 ilustra un dispositivo a prueba de sabotajes 400 en forma de un módulo de identidad de abonado de red que incorpora un agente de registro 150 de la invención, El SIM 400 de la Fig. 8 también se proporciona con un módulo de Acuerdo de Clave y Autentificación (AKA) 460, que comprende algoritmos, por ejemplo los algoritmos AKA A3/A8 de GSM, para operar en los datos enviados/recibidos por la unidad móvil, autentificando por ello el cliente en la red. Estos algoritmos AKA típicamente usan una clave específica SIM 466, por ejemplo la clave de suscripción asociada con la suscripción usuario-operador, una clave asociada con un agente de DRM 430 implementada en el SIM, o una clave derivada de estas claves. También es posible usar criptografía asimétrica para los propósitos de autentificación. El SIM 400 también podría comprender un autentificador de la información de uso 160 para realizar la operación de seguridad (autentificación) de la invención. Alternativamente, o como complemento, sería posible configurar los algoritmos del módulo AKA 460 para autentificar y/o proteger criptográficamente la información de uso generada por el agente de registro 150 en la unidad móvil. El SIM 400 también se proporciona con una unidad de entrada/salida convencional 410 que analiza los comandos enviados al SIM 400 y maneja la comunicación con las funciones internas. Para más información sobre los módulos SIM, se hace referencia a [10, 11].

El agente de registro 150 se puede implementar en el SIM 400 en el programa informático, los componentes físicos o una combinación de los mismos. El módulo del cliente, o el SIM 400, se puede proporcionar con el agente de registro 150 en o durante la fabricación. En lugar de usar un módulo cliente o el SIM 400 prefabricado con un agente de registro 150, el agente de registro 150 se puede descargar sobre la red desde un nodo de red asociado por ejemplo con el operador de red o el proveedor de contenidos, y se puede implementar en el módulo cliente o el SIM 400. Esta solución de descarga es especialmente ventajosa para implementar el agente de registro 150 en el SIM 400. Como el interfaz de la unidad móvil-SIM típicamente se asocia con los comandos tratados para enviar datos más o menos arbitrarios al SIM 400 para usar allí dentro, por ejemplo el comando “ENVELOPE” para las tarjetas SIM de GSM, el código para implementar el agente de registro 150 en el SIM 400, por ejemplo como una aplicación general de subprograma de Java, se podría enviar usando tales comandos. El subprograma puede estar dando varios grados de autorización para acceder a archivos residentes relativos a GSM/UMTS, una posibilidad que es para darle “acceso GSM/UMTS” completo”. La aplicación del agente de registro enviada por el comando se implementa en un entorno de aplicaciones 490 proporcionado por un juego de herramientas de aplicaciones asociado con el SIM 400. Para un SIM de GSM se proporciona el entorno de aplicaciones por un Juego de Herramientas de Aplicaciones del SIM (SAT), mientras que el análogo del USIM se proporciona por el SAT de UMTS (USAT). De esta manera, el juego de herramientas de aplicaciones del SIM permite al fabricante, operador o proveedor de contenidos o bien “codificar” (fabricante), o descargar (operador o proveedor de contenidos, a través del operador de red), sobre el aire, una aplicación de agente de registro en el SIM 400. Si el agente de registro 150 se descarga al entorno de aplicaciones del SIM 490, es preferible autentificar la aplicación (agente de registro) como viene del operador de derechos. De esta manera, esto da protección contra la descarga de “virus” o agentes de registro incorrectos desde un servidor malicioso. La aplicación de registro descargada también se puede cifrar, por ejemplo con una clave asociada a la SIM, de manera que los contenidos de la misma no están disponibles fuera del SIM. La información adicional del SAT y USAT se encuentran en la referencia [12-14] y [15], respectivamente.

Si se usa un dispositivo a prueba de sabotajes o tarjeta SIM, se pueden usar otras distintas de las tarjetas SIM para comunicación móvil, sus correspondientes comandos de descarga y entorno de aplicación para implementar una aplicación del agente de registro allí dentro.

Usando una solución implementada del entorno de aplicaciones para el agente de registro 150, o una solución de implementación similar, es posible actualizar las funciones del agente de registro 150. Esta actualización puede concernir por ejemplo una nueva ubicación de almacenamiento del registro de uso 170, 175, nueva información incluida en las entradas de registro, etc. Tales actualizaciones entonces simplemente se descargan usando los comandos de

descarga, por ejemplo el comando ENVELOPE, asociado con el módulo cliente e implementado en el módulo cliente. Esta es una solución ventajosa si el agente de registro 150 está roto o “pirateado”, de manera que sus claves secretas y/o código lleguen a ser conocidas públicamente, por ejemplo en Internet. Entonces, en lugar de cambiar todo el agente de registro que contiene los módulos cliente o los dispositivos a prueba de sabotajes, incluyendo las tarjetas SIM de red 400, el agente de registro 150 simplemente se puede actualizar descargando e implementando nuevas actualizaciones, por ejemplo nuevas claves.

Como se ilustra en la Fig. 8, no solamente se puede implementar el agente de registro 150 sino también el agente de DRM 430 en el entorno de aplicaciones 490. Esto significa que también se pueden actualizar otras aplicaciones y funciones de DRM a través de descargas.

Con referencia a la Fig. 3, el operador de red 20 puede incluir aplicaciones del agente de registro 24 que van a ser descargadas a sus clientes de suscripción 10. Tales aplicaciones 24 también podrían incluir la actualización del agente de registro las cuales se transmiten por medio de la unidad de comunicación de I/O 22 sobre la red 40 al módulo cliente 10 para la implementación allí dentro.

Volviendo de nuevo a la Fig. 8, el agente de registro 150 en el entorno de aplicaciones genera la información de uso y la información de uso generada se autentifica preferentemente usando por ejemplo el autentificador 160 o el módulo AKA 460 con la clave asociada al SIM 466. La información de uso autentificada entonces se almacena en un registro de uso 170, 175. Este registro se podría almacenar, como se trató anteriormente, externamente (número de referencia 170 en la Fig. 8) en una parte de confianza, en el SIM 400 (número de referencia 175 en la Fig. 8) y/o en el módulo cliente cooperando con el SIM 400. En el SIM 400 de la Fig. 8, el registro 175 se puede disponer en el entorno de aplicaciones 490, por ejemplo en el agente de registro 150 o de DRM 490, o en algún otro lugar en el SIM 400.

Como se trató brevemente anteriormente, la información de uso de la invención se puede almacenar en un entorno seguro como una parte de la operación de seguridad, en lugar de ser autentificada. Si está disponible suficiente capacidad de memoria, una solución adecuada es almacenar el registro 175 en un módulo de identidad de abonado 400, como se ilustró en la Fig. 8. Para activar para un cliente el entorno SIM primero tiene que introducir un código pin. Este código es un código personal asociado con el cliente real que tiene una suscripción con el operador de red. Una vez activado, se puede almacenar la información de uso generada en el registro 175 en el SIM 400. Almacenando la información de uso generada en el registro implementado en el SIM 175 es posible asociar la información de uso con el individuo que posee el SIM 400, es decir que tiene una suscripción manifestada en un SIM con el operador de red. No obstante, si la información de uso registrada posteriormente va a ser transmitida a una parte de confianza, por ejemplo para ser base de cargo o evidencia de usos, la información de uso primero se autentifica, por ejemplo usando el autentificador 160 o módulo AKA 460 del SIM 400, antes de la transmisión.

El SIM 400 también se podría usar como una base para un mecanismo de cargo que se puede usar para el pago de los contenidos digitales en el sistema de DRM. En tal caso, la información de uso desde el agente de registro 150 se autentifica por medio de por ejemplo, la clave 466 asociada con la suscripción con el operador de red. El autentificador 160 o módulo AKA 460 puede firmar la información de uso, proteger criptográficamente y/o autentificar el mensaje, permitiendo la identificación de qué SIM 400 (abonado) origina la información de uso. La información de uso autentificada entonces se transfiere al operador de red o a una entidad de facturación dedicada (servidor de cargo) que gestiona el cargo real de los contenidos digitales. En tal caso, la información de uso especifica la cantidad que va a ser cargada desde el cliente, o alguna información, por ejemplo un identificador de los contenidos digitales usados y el tiempo total de uso, que permite a la entidad de facturación calcular la cantidad total a cargar. Esta cantidad entonces se carga desde una cuenta asociada con el cliente, desde la suscripción del cliente (factura de teléfono móvil), o por algún otro medio.

La Fig. 9 ilustra una parte de un sistema cliente 10 que incorpora un módulo de identidad de abonado 400. Similar a la Fig. 4, este sistema cliente 10 incluye un dispositivo de presentación autónomo 300 con el procesador de medios 340 y la pantalla 342 para presentar los contenidos digitales encargados. El dispositivo de presentación 300 además incluye un agente de DRM 220 que incorpora un agente de registro 150 y el autentificador de la información de uso 160 de acuerdo con la invención. En la Fig. 9, solamente se ilustra el SIM 400 del dispositivo de recepción. No obstante, durante el funcionamiento este SIM 400 está cooperando con/dispuesto en el dispositivo de recepción con una unidad de comunicación de I/O para permitir el encargo y la recepción de los contenidos digitales.

El sistema cliente de la Fig. 9 (y la Fig. 4) tiene una funcionalidad de DRM distribuida, con un agente de DRM 430 asociado con el SIM 400 (dispositivo de recepción) y un agente de DRM asociado 330 con el dispositivo de presentación 300. Durante el funcionamiento, el dispositivo de recepción típicamente encarga unos contenidos digitales y recibe un cupón desde un operador de red. Una copia del cupón se transmite a un proveedor de contenidos, el cual descarga o difunde de forma continua los contenidos digitales al dispositivo de recepción. Estos contenidos digitales entonces se envían, posible después del descifrado, al dispositivo de presentación, en el que la presentación real tiene lugar. El agente de registro 150 en el agente de DRM 330 entonces genera la información de uso sobre la presentación de los contenidos. Esta información de uso se autentifica preferentemente por el autentificador 160 y se transmite a través de una unidad de entrada/salida (I/O) 310 al SIM 400, donde una unidad de I/O 410 recibe la información y la envía a un registro, por ejemplo un registro externo 170 para el almacenamiento. Alternativamente, o además, la información de uso se almacena en un registro 175 del SIM 400. Si el módulo AKA 460 tiene algoritmos para realizar la

autentificación y posible cifrado de la información de uso generada, el autentificador 160 del agente de DRM 330 se podría omitir. En tal caso, tras la recepción de la información de uso desde el dispositivo de presentación 300, la unidad de I/O 410 típicamente envía la información al módulo AKA 460. Como se mencionó anteriormente, el módulo AKA 460 autentifica la información de uso preferentemente usando una clave de suscripción 466 asociada con el SIM 400, antes de que la información se envíe al registro.

Con tal adaptación podría ser aconsejable configurar de manera resistente a sabotajes el SIM 400 y el dispositivo de presentación 300 con la información de la clave específica del dispositivo de presentación para permitir la comunicación segura entre los dos agentes de DRM 330 y 430. La información de la clave del dispositivo puede ser una clave secreta compartida, o una pareja de claves asimétricas, que permiten la autentificación y/o protección de la información, incluyendo la información de uso, comunicada entre los agentes de DRM 330, 430. La clave del dispositivo, y, se almacena normalmente de manera resistente a sabotajes 365 en el dispositivo de representación 300. La infraestructura del operador de red y/o la parte de certificación de confianza se puede usar para transferir de manera segura la información de la clave del dispositivo correspondiente para el almacenamiento 465 en el SIM 400, como se describirá en más detalle debajo.

En el ejemplo particular de la Fig. 9, el cual se refiere a una clave del dispositivo simétrica, tanto el SIM 400 como el dispositivo de presentación 300 se configuran con la clave específica del dispositivo de presentación de secreto compartido, y, o una representación del mismo. La clave del dispositivo compartida se implementa en los agentes de DRM 330, 430 de las entidades implicadas. Esta es una solución perfectamente válida, por ejemplo cuando el agente de DRM 330 del dispositivo de presentación 300 se implementa como un circuito de componentes físicos. No obstante, puede ser beneficioso implementar de manera resistente a sabotajes la clave del dispositivo, y, fuera del agente de DRM 330 en el dispositivo de presentación 300, especialmente cuando el agente de DRM 330 es una aplicación basada en programas informáticos. En tal caso, la clave del dispositivo, y, (o su representación) se almacena preferentemente dentro de un entorno a prueba de sabotajess, tal como un circuito de seguridad dedicado, en el dispositivo de presentación 300.

Durante el funcionamiento, el agente de registro 150 en el agente de DRM 330 compila la información de uso según el dispositivo de presentación 300 consume los contenidos digitales, y envía la información al agente de DRM 430 del SIM 400, usando preferentemente la comunicación basada en la clave del dispositivo seguro y/o autentificado. Por ejemplo, es beneficioso usar la clave del dispositivo para proteger la integridad de la información de uso compilada. El agente de DRM 430 autentifica y/o descifra la información de uso en base a la información de la clave del dispositivo correspondiente y almacena la información en el registro 175 y/o envía la información de uso al módulo AKA 460 para la autentificación del mismo. A partir de entonces, la información autentificada se puede enviar a una parte externa de confianza para el registro 170, si se desea.

En un protocolo de comunicación más elaborado, el agente de DRM 430 y el agente de DRM 330 intercambian señales de control para controlar el proceso de presentación. Por ejemplo, el agente de DRM 330 en el dispositivo de presentación 300 genera intermitentemente una señal de reconocimiento ACK que indica que el proceso de usar los contenidos digitales recibidos se desarrolla sin perturbaciones. La señal de ACK preferentemente se acompaña por la información de uso desde el agente de registro 150, por ejemplo relacionado con la cantidad de tiempo de presentación, cantidad de datos exitosamente presentados, calidad de la presentación, retardos de tiempo, desbordamientos de almacenamientos temporales, y otros datos que conciernen al proceso de presentación. El agente de DRM 430 incluye la funcionalidad para procesar esta información de señal y para enviar una denominada señal de proceder al envío FPS al agente de DRM 330 en respuesta a la misma. La señal FPS se requiere para que el proceso de presentación continúe, mientras que una señal FPS perdida provoca que el proceso de presentación se pare o siga de acuerdo con las limitaciones predeterminadas, por ejemplo la QoS (Calidad de Servicio) limitada. La señal FPS puede incluir información, tal como un DAC (Código de Acceso de Dispositivo) extraído desde el cupón correspondiente por el agente de DRM 430 o información obtenida analizando los datos de registro recibidos desde el agente de registro 150, que se puede usar para controlar el proceso de presentación. El agente de DRM 330 se configura de esta manera para recibir la señal FPS y para controlar el proceso de presentación en dependencia 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 uso desde el agente de registro 150 sirve como una base para el cargo. Si el agente de DRM 430 no recibe tal información de uso, el agente de DRM 430 no es capaz de controlar el proceso de presentación continuado por medio de la señal FPS.

El agente de DRM 430 también puede ser capaz de extraer las reglas de uso asociadas con los contenidos digitales a partir del cupón y enviar estas reglas al dispositivo de presentación 300 para la aplicación por su agente de DRM 330. Alternativamente, no obstante, las reglas de uso se envían directamente, preferentemente junto con los contenidos digitales cifrados, al dispositivo de presentación 300 y el agente de DRM 330 de allí dentro.

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

De aquí en adelante, sigue una breve descripción de cómo se puede establecer una comunicación basada en la clave del dispositivo entre los agentes de DRM distribuidos de un sistema cliente.

Durante al fabricación, el dispositivo de presentación se configura de manera resistente a sabotajes con una clave específica del dispositivo de uso y. Señalar que no es seguro escribir simplemente “y” en el exterior del dispositivo de presentación, ya que se podría copiar y se podrían crear fácilmente dispositivos no seguros, clonados. En su lugar, la información de identificación, tal como el resultado de aplicar alguna función criptográfica h a la clave y se puede adjuntar a una “etiqueta” en el dispositivo de presentación cuando se vende, o transferir desde el dispositivo de presentación al dispositivo de recepción asociado del sistema cliente cuando se interconecta, haciendo disponible de esta manera una representación criptográfica de la clave del dispositivo disponible a un usuario/al dispositivo de presentación. Cuando el cliente desea activar el dispositivo, envía la representación criptográfica (abierta) h(y), o información de identificación similar, al operador (u otra parte de certificación de confianza) quien comprueba que h(y) está asignada a un dispositivo válido, recupera la clave del dispositivo o la información de la clave adecuada, tal como y', derivada de la clave del dispositivo, y finalmente actualiza la aplicación de DRM en el dispositivo de recepción (o SIM del dispositivo de recepción) con la clave de dispositivo y o la información de la clave derivada de allí.

Se supone que el operador u otra parte de certificación de confianza (en algunos modelos de negocio, la parte de confianza puede ser el fabricante del dispositivo) tiene alguna clave que le permite invertir la función h o de otro modo es capaz de recuperar la información de la clave del dispositivo adecuada, por ejemplo usando tablas de búsqueda, típicamente conocidas solamente por el Operador. Por ejemplo, puede ser el caso de que la clave del dispositivo en sí misma nunca debería estar disponible fuera del dispositivo de presentación, incluso explícitamente no conocida por la parte de confianza. En este caso, la parte de confianza es capaz de recuperar la información de la clave, tal como y', que se basa en la clave real del dispositivo y y quizás los datos de entrada adicionales.

También se supone que la información de la clave del dispositivo se transfiere de manera segura desde la parte de certificación al SIM en el dispositivo de recepción en base a alguna clave específica SLIM. Una vez configurada adecuadamente en el agente de DRM del SIM, la información de la clave del dispositivo, es decir la clave del dispositivo o alguna otra clave derivada de la clave del dispositivo, se podría usar para establecer la comunicación (segura y/o autentificada) con el agente de DRM en el dispositivo de presentación. Aparentemente, si una clave derivada de la clave real del dispositivo y se transfiere a y se implemente en el SIM, el dispositivo de presentación tiene que implementar alguna función que en base a la clave del dispositivo genera la misma clave derivada como en el SIM.

Aunque la presente invención en lo anterior principalmente ha sido tratada con referencia a realizaciones de un proveedor de contenidos que proporciona los contenidos digitales a un sistema cliente sobre una red, también se prevé emplear la funcionalidad de registro de la invención en otros sistemas de distribución de servicios y contenidos. Por ejemplo, un proveedor de servicios puede proporcionar un servicio a un sistema cliente del usuario. Cuando el usuario usa posteriormente el servicio, se genera la información de registro sobre el uso, preferentemente autentificado y almacenado. Un ejemplo típico es el pago por utilizar una plaza de estacionamiento, por ejemplo en un estacionamiento de coches de varios pisos. Un proveedor de servicios entonces puede proporcionar servicios para el pago de la tarifa del estacionamiento usando una unidad móvil o teléfono (sistema cliente), controlando un portón o puerta que permite la entrada a y salida del estacionamiento de coches, etc. La información de uso generada entonces podría incluir un identificador del estacionamiento de coches y/o plaza de estacionamiento y la hora de entrada y salida (y/o el tiempo total en el que se utiliza el servicio de estacionamiento). La información de uso generada se podría usar entonces para adeudar al usuario asociado con el sistema cliente.

La Fig. 10 resume esquemáticamente el método de monitorización de uso de acuerdo con la presente invención. En el paso S1 el módulo o sistema cliente, por ejemplo presenta, guarda, envía, copia, ejecuta, elimina y/o modifica, los contenidos digitales recibidos desde un proveedor de contenidos sobre una red. El paso S2 registra la información de uso que concierne al uso de los contenidos digitales individualmente para cada uso que va a ser monitorizado. Una operación de seguridad que permite la identificación de la cual (el cliente, individuo o cuenta) origina la información se realiza en el paso S3. El método entonces finaliza. La Fig. 11 ilustra el paso de registro S2 de la Fig. 10 en más detalle. En el paso S4, un agente de registro dispuesto en el sistema cliente genera la información respecto al uso. Esta generación de la información de uso se realiza preferentemente de manera resistente a sabotajes, por ejemplo implementando el agente de registro en un entorno a prueba de sabotajess, reduciendo el riesgo de que el usuario manipule o borre la información de uso generada. El método sigue al paso S3. El paso de realización de la seguridad de la Fig. 10 se ilustra en más detalle en la Fig. 12. En el paso opcional S5, la información de uso se protege criptográficamente, por ejemplo mediante una clave simétrica o una clave pública, en la que la clave de descifrado privada asociada se mantiene de manera segura en una ubicación de confianza. El paso S6 realiza al menos una parte de un autentificación de la información de uso. Tal autentificación usa una clave de firma, clave protegida o alguna otra información criptográfica asociada con el cliente para autentificar la información de uso según se asocia con el cliente. El método entonces se finaliza. Los pasos opcionales adicionales del método de monitorización de la invención se ilustran en la Fig. 13. En el paso S7, la información de uso se envía desde el sistema cliente a una parte de confianza, por ejemplo un operador de red, un servidor de cargo o una entidad de facturación. La información de uso enviada se almacena entonces como una entrada de registro en el registro en el paso S8. La información de uso registrada se puede usar entonces como base para el cargo de los contenidos digitales, como evidencia del uso realizado realmente si surge una discusión más tarde entre el cliente y el proveedor de contenidos, para propósitos de no repudiación y/o como base para las estadísticas de los usos del cliente de los contenidos digitales. El método se completa entonces.

Un método de DRM de acuerdo con la presente invención se ilustra esquemáticamente en el diagrama de flujo de la Fig. 14. El paso S10 proporciona los contenidos digitales desde un servidor de contenidos a un sistema cliente

sobre una red. En el sistema cliente los contenidos digitales recibidos se usan y un agente de registro de acuerdo con la invención genera la información que concierne al uso individualmente para cada uno de un conjunto de usos del cliente. Además, la operación de seguridad (autentificación) se realiza sobre la información de uso que permite la identificación del cliente que ha usado los contenidos digitales. La información de uso de origen identificable y generada entonces se recibe y almacena como una entrada de registro en un registro en el paso S 11. El método de DRM entonces se finaliza.

Las realizaciones descritas anteriormente se dan meramente como ejemplos, y debería ser entendido que la presente invención no se limita a las mismas. Modificaciones, cambios y mejoras adicionales, que mantienen los principios básicos subyacentes revelados o reivindicados aquí dentro están dentro del alcance de la invención como se define por las reivindicaciones adjuntas.

REFERENCIAS

[1] A.J. Menezes, P.C. van Oorschot y S.C. Vanstone, “Manual de Criptografía Aplicada”, CRC Press.

[2] L. Kaati, “Técnicas Criptográficas y Cifrados para la Gestión de Derechos Digitales”, Tesis de Maestría en Ciencias de Ordenadores. Departamento de Análisis Numérico y Ciencias de Ordenadores, Real Instituto de Tecnología, Universidad de Stockholm, 2001.

[3] Solicitud de patente sueca Nº 0101295-4 presentada en Abril de 2001.

[4] ISO/IEC 13888-1 Tecnologías de la Información, técnicas de Seguridad, no repudiación, Parte 1: General, 1997.

[5] ISO/IEC 13888-2 Tecnologías de la Información, técnicas de Seguridad, no repudiación, Parte 2: Mecanismos que usan técnicas simétricas, 1998.

[6] ISO/IEC 13888-3 Tecnologías de la Información, técnicas de Seguridad, no repudiación, Parte 3: Mecanismos que usan técnicas asimétricas, 1997.

[7] J. Postel, “Protocolo de Datagrama de Usuario”, RFC 768, IETF, agosto de 1980.

[8] V. Jacobson, S.L. Cashier, R. Frederick y H. Schulzrinne, “RTP: Un Protocolo de Transporte para Aplicaciones en Tiempo Real”, RFC 1889, IETF, noviembre de 2001.

[9] M. Baugher, R. Blom, E. Carrara, D. McGrew, M. Näslund, K. Norrman y D. Oran “El Protocolo de Transporte Seguro en Tiempo Real”, draft-ietf-avt-srtp-05.txt, IETF, junio de 2002.

[10] “Módulos de Identidad de Abonado (SIM), Características Funcionales”, ETSI TS 100 922, GSM 02.17, Especificación Técnica del sistema de Telecomunicaciones Celulares Digitales, versión 3.2.0, febrero de 1992.

[11] “Especificación del interfaz del Módulo de Identidad de Abonado – Equipo Móvil (SIM - ME)” 3GPP TS 11.11, ETSI TS 100 977, Especificación Técnica del Proyecto de Cooperación de 3ª Generación, Especificación Técnica de los Terminales de Grupo, versión 8.5.0, 1999.

[12] “API de GSM para juego de herramientas del SIM, Etapa 2”, 3GPP TS 03.19, ETSI TS 101 476, Especificación Técnica del Proyecto de Cooperación de 3ª Generación, Especificación Técnica de los Terminales de Grupo, versión 8.4.0, 1999.

[13] “Especificación del Juego de Herramientas de Aplicaciones del SIM para el interfaz del Módulo de Identidad de Abonado – Equipo Móvil (SIM – ME)”, 3GPP TS 11.14, ETSI TS 101 267, Especificación Técnica del Proyecto de Cooperación de 3ª Generación, Especificación Técnica de los Terminales de Grupo, versión 8.10.0, 1999.

[14] “Mecanismo de Seguridad para el Juego de Herramientas de Aplicaciones del SIM, Etapa 2”, 3GPP TS 03.48, ETSI TS 101 181, Especificación Técnica del Proyecto de Cooperación de 3ª Generación, Especificación Técnica de los Terminales de Grupo, versión 8.8.0, 1999.

[15] “Juego de Herramientas de Aplicaciones del SIM (USAT)”, 3GPP TS 31.111, ETSI TS 131 111, Especificación Técnica del Proyecto de Cooperación de 3ª Generación, Especificación Técnica de los Terminales de Grupo, versión 4.4.0, Publicación 4.

REIVINDICACIONES

1. Un método de monitorizar el uso del cliente de los contenidos digitales descargados o difundidos de forma continua proporcionados por un proveedor de contenidos (30) a un sistema cliente (10) sobre una red (40), dicho método que consta de los pasos de:

- registrar (S2) el uso generando información de uso que concierne al uso de dichos contenidos digitales, recibiendo datos de entrada desde distintos medios externos dependientes de la información de uso que van a ser generada;

- realizar (S3) una operación de seguridad para permitir la identificación de al menos una de una cuenta y un cliente para vincular dicha información de uso a la cuenta y/o cliente identificado, y

monitorizar el uso del cliente de los contenidos digitales descargados o difundidos de forma continua usando la información de uso generada, y en donde el cliente se identifica mediante dicha operación de seguridad, en donde dicha información de uso se mantiene en un registro (175) en dicho sistema cliente (10), y dicho paso de realizar una operación de seguridad comprende el paso de almacenar dicho registro (175) en un entorno a prueba de sabotajess asociado con dicho sistema cliente (10), y en donde dicha información de uso comprende una representación (172-1) de dichos contenidos digitales usados por el cliente; la información de la calidad de uso (172-2); y la información temporal (172-N) relacionada con el uso de dichos contenidos digitales.

2. El método de acuerdo con la reivindicación 1, en donde dicho paso de realizar una operación de seguridad comprende el paso de realizar al menos parte de una autentificación de dicha información de uso.

3. El método de acuerdo con la reivindicación 2, en donde dicho paso de realizar al menos parte de la autentificación comprende al menos uno de: - firmar dicha información de uso por una clave de firma (166; 466); - cifrar dicha información de uso por una clave de cifrado (166; 466); y – adjuntar una etiqueta de autentificación (174), calculada por una clave de autentificación, a dicha información de uso.

4. El método de acuerdo con la reivindicación 1, en donde dicha información de la calidad (172-2) comprende al menos uno de:

- el ancho de banda de dichos contenidos digitales usados;

- la velocidad de las muestras de dichos contenidos digitales;

- la compresión de los datos de dichos contenidos digitales;

- la resolución de dichos contenidos digitales usados;

- la información temporal (172-N) relacionada con el uso de dichos contenidos digitales; y

- la información de cualquier interrupción durante el uso de dichos contenidos digitales.

5. El método de acuerdo con la reivindicación 1, en donde dicha información de uso comprende al menos una de:

- la forma de uso;

- la identificación de un dispositivo de uso de los contenidos (300);

- la información sobre el pago de dichos contenidos digitales;

- la información temporal relacionada con la transmisión de dichos contenidos digitales desde dicho proveedor de contenidos (30) a dicho sistema cliente; y

- la información temporal relacionada con la recepción de dichos contenidos digitales por dicho sistema cliente (10).

6. El método de acuerdo con la reivindicación 1, en donde dicho paso de generación comprende el paso de:

- generar de manera resistente a sabotajes dicha información de uso; y en el que el método comprende el paso adicional de:

- almacenar dicha información de uso como una entrada de registro (172) en un registro a prueba de sabotajess del usuario (170; 175; 175-1; 175-2).

7. El método de acuerdo con la reivindicación 1, que además comprende el paso de enviar dicha información de uso desde dicho sistema cliente (10) a una parte externa de confianza para almacenar allí dentro como la entrada de registro (172) en un registro de uso (170).

8. El método de acuerdo con la reivindicación 1, en donde dichos contenidos digitales se proporcionan como datos de difusión de forma continua y dichos datos digitales se usan por dicho sistema cliente (10), dicho paso de registrar la información de uso comprende el paso de para cada uso del cliente de los datos de difusión de forma continua en curso, registrando intermitentemente la información de uso durante dicho uso del cliente.

9. El método de acuerdo con la reivindicación 8, que además comprende el paso de enviar intermitentemente dicha información de uso registrada intermitentemente a dicho proveedor de contenidos (30) para la confirmación de la recepción y la presentación de los datos.

10. El método de acuerdo con la reivindicación 9, en donde dicha información de uso se incluye en los informes de recepción asociados con el mecanismo de informe del protocolo de difusión de forma continua usado para difundir de forma continua dichos datos.

11. El sistema cliente (10) capaz de usar los contenidos digitales descargados o difundidos de forma continua proporcionados por un proveedor de contenidos (30) sobre una red (40) a un sistema cliente, dicho sistema cliente (10) que comprende:

un agente de registro (150) que comprende un generador (152) para generar la información de uso que concierne al uso de dichos contenidos digitales, recibiendo los datos de entrada desde distintos medios externos dependientes de la información de uso que va a ser generada;

los medios para realizar (160; 460) una operación de seguridad para permitir la identificación de al menos una de una cuenta y un cliente para vincular dicha información de uso a la cuenta y/o cliente identificado, y en donde el agente de registro además se adapta para monitorizar el uso del cliente de los contenidos digitales descargados o difundidos de forma continua usando la información de uso generada, y

en donde el cliente se identifica por dicha operación de seguridad, en donde dicha información de uso se mantiene en un registro (175) en dicho sistema cliente (10), y dicha operación de seguridad que realizan los medios se configura para almacenar dicho registro (175) en un entorno a prueba de sabotajess asociado con dicho sistema cliente (10) y en donde dicha información de uso comprende una representación (172-1) de dichos contenidos digitales usados por el cliente; la información de la calidad de uso (172-2); y la información temporal (172-N) relacionada con el uso de dichos contenidos digitales.

12. El sistema cliente de acuerdo con la reivindicación 11, en donde dichos medios que realizan la operación de seguridad (160; 460) se configuran para realizar al menos parte de una autentificación de dicha información de uso.

13. El sistema cliente de acuerdo con la reivindicación 12, en donde dichos medios que realizan la operación de seguridad (160; 460) comprenden al menos uno de:

- los medios (160, 460) para firmar dicha información de uso por una clave de firma (166; 466);

- los medios (160; 460) para cifrar dicha información de uso por una clave de cifrado (166; 466); y

- los medios (160; 460) para calcular una etiqueta de autentificación (172) mediante una clave de autentificación y adjuntar dicha etiqueta de autentificación (172) a dicha información de uso.

14. El sistema cliente de acuerdo con la reivindicación 11, en donde dicho generador (152) comprende:

- los medios (152) para generar de manera resistente a sabotajes dicha información de uso; y el agente de registro comprende medios adicionales para almacenar (154; 156) dicha información de uso como una entrada de registro (172) en un registro de uso (170; 175).

15. El sistema cliente de acuerdo con la reivindicación 11, en donde dicho agente de registro (175) comprende además los medios (156) para enviar dicha información de uso a una parte externa de confianza para el almacenamiento allí dentro como una entrada de registro (172) en un registro de uso (170).

16. El sistema cliente de acuerdo con la reivindicación 11, que además comprende:

- un dispositivo de uso (300) adaptado para usar dichos contenidos digitales proporcionados; y

- un primer agente de gestión de derechos digitales (DRM) (130; 330), al menos parcialmente implementado en dicho dispositivo de uso (300), que tiene la funcionalidad para permitir el uso de dichos contenidos digitales.

17. El sistema cliente de acuerdo con la reivindicación 16, que además comprende:

- un segundo agente de DRM (230; 430) implementado en dicho sistema cliente (10), que tiene la funcionalidad para permitir la recepción de dichos contenidos digitales desde dicho proveedor de contenidos (30); y

los medios (210; 310; 410) para la comunicación entre dicho primer agente de DRM (330) y dicho segundo agente de DRM (230; 430), dicho primer agente de DRM (330) que comprende medios para transferir una primera señal

de control asociada con dicha información de uso a dicho segundo agente de DRM (230; 430) y dicho segundo agente de DRM (230; 430) comprende los medios para procesar los datos de la señal asociados con dicha señal de control para generar una segunda señal de control, y los medios para enviar dicha segunda señal de control a dicho primer agente de DRM (330) para controlar el proceso de uso de los contenidos digitales.

18. El sistema cliente de acuerdo con la reivindicación 14, que además comprende un módulo a prueba de sabotajess, en el que se implementa dicho agente de registro (150).

19. El sistema cliente de acuerdo con la reivindicación 18, en donde dicho módulo a prueba de sabotajess es un módulo de identidad de abonado (400).

20. El sistema cliente de acuerdo con la reivindicación 19, en donde dicho agente de registro (150) se implementa al menos parcialmente como una aplicación en un entorno de aplicaciones (490) proporcionado por un juego de herramientas de aplicaciones asociado con dicho módulo de identidad de abonado (400).

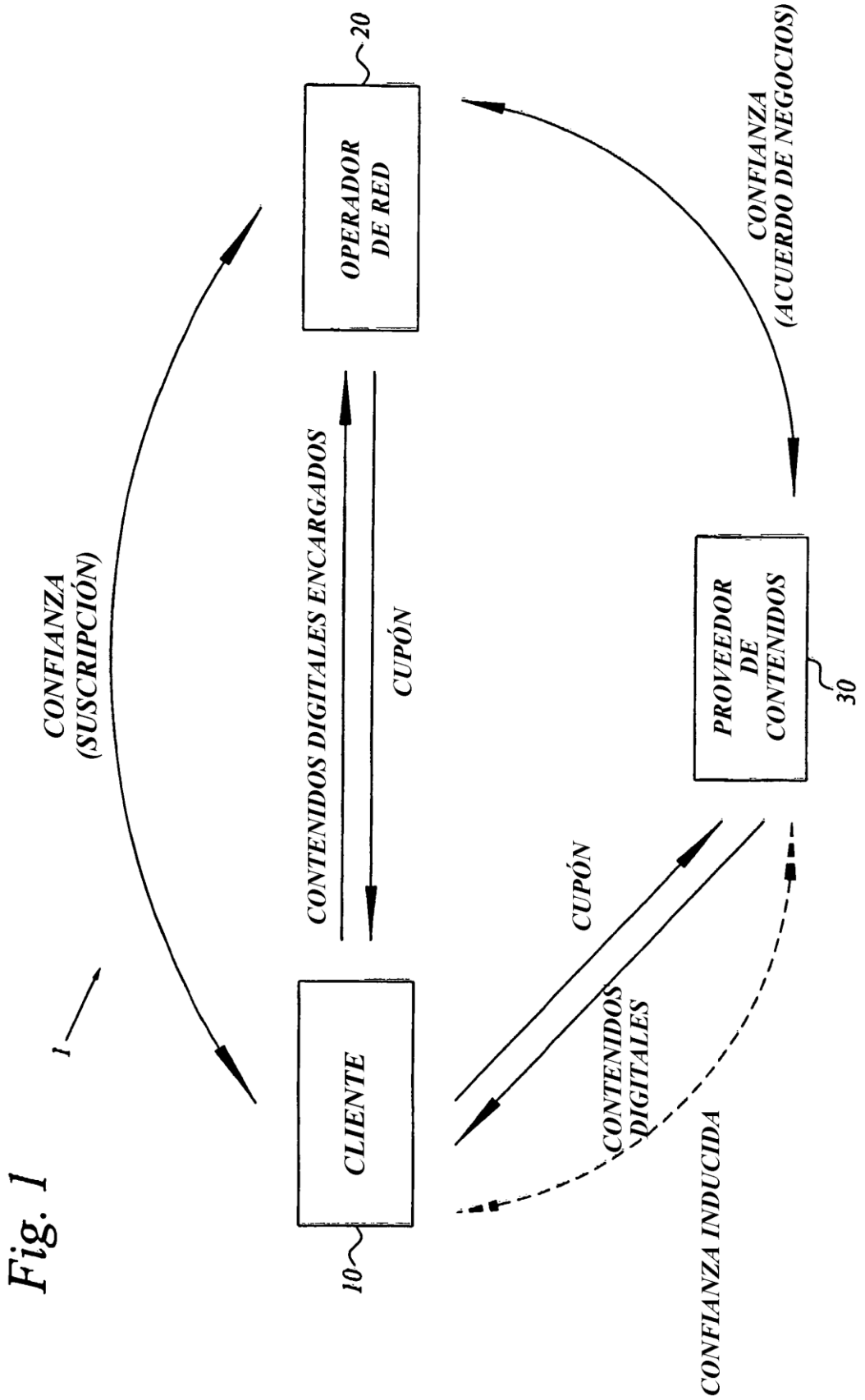
21. El sistema cliente de acuerdo con la reivindicación 20, en donde dicha aplicación del agente de registro se descarga en dicho módulo de identidad de abonado (400) sobre dicha red (40) a partir de un proveedor de servicios de red (20; 30) asociado con dicho módulo de identidad de abonado (400).

22. El sistema cliente de acuerdo con la reivindicación 11, en donde dichos contenidos digitales se proporcionan como datos difundidos de forma continua y dicho sistema cliente (10) comprende medios (300) para usar dichos datos difundidos de forma continua, y dicho agente de registro (150) se configura, para cada uso del cliente de los datos difundidos de forma continua en curso, para generar intermitentemente la información de uso durante dicho uso del cliente.

23. El sistema cliente de acuerdo con la reivindicación 22, que además comprende los medios (156) para enviar intermitentemente dicha información de uso generada intermitentemente a dicho proveedor de contenidos (30) para confirmar la recepción y uso de los datos.

24. El sistema cliente de acuerdo con la reivindicación 23, en donde dicha información de uso se incluye en los informes de recepción asociados con el mecanismo de informe del protocolo de difusión de forma continua usado para difundir de forma continua dichos datos.

Fig. 1


1
CONFIANZA (SUSCRIPCIÓN)
OPERADOR DE RED
20
CONFIANZA (ACUERDO DE NEGOCIOS)
CONTENIDOS DIGITALES ENCARGADOS
CUPÓN
PROVEEDOR DE CONTENIDOS
30
CUPÓN
CONTENIDOS DIGITALES
CLIENTE
10
CONFIANZA INDUCIDA

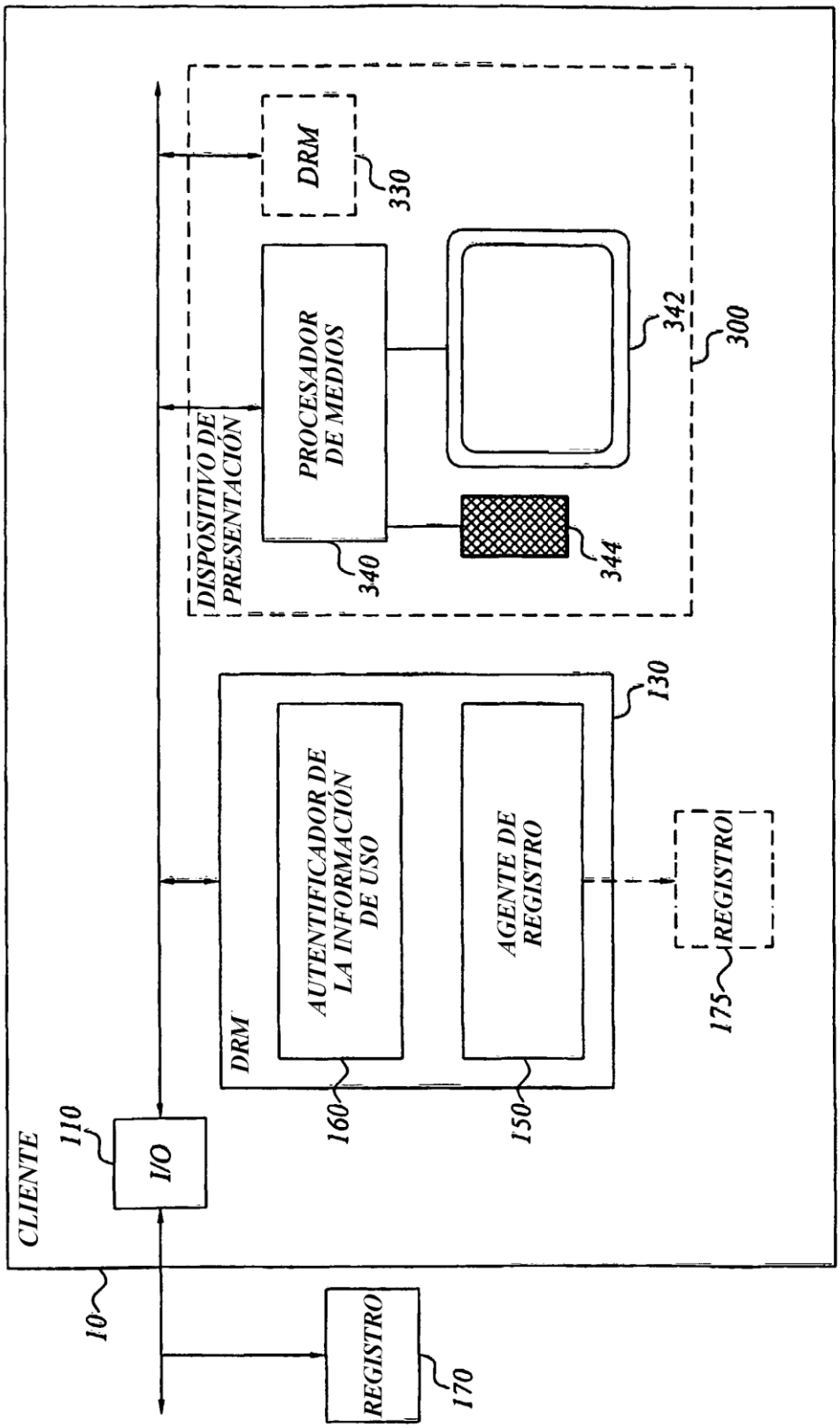

CLIENTE
110
I/O
10
REGISTRO
170
DRM
130
AUTENTIFICADOR DE LA INFORMACIÓN DE USO
160
AGENTE DE REGISTRO
150
175
REGISTRO
DISPOSITIVO DE PRESENTACIÓN
PROCESADOR DE MEDIOS
340
342
344
300
DRM
330

Fig. 2

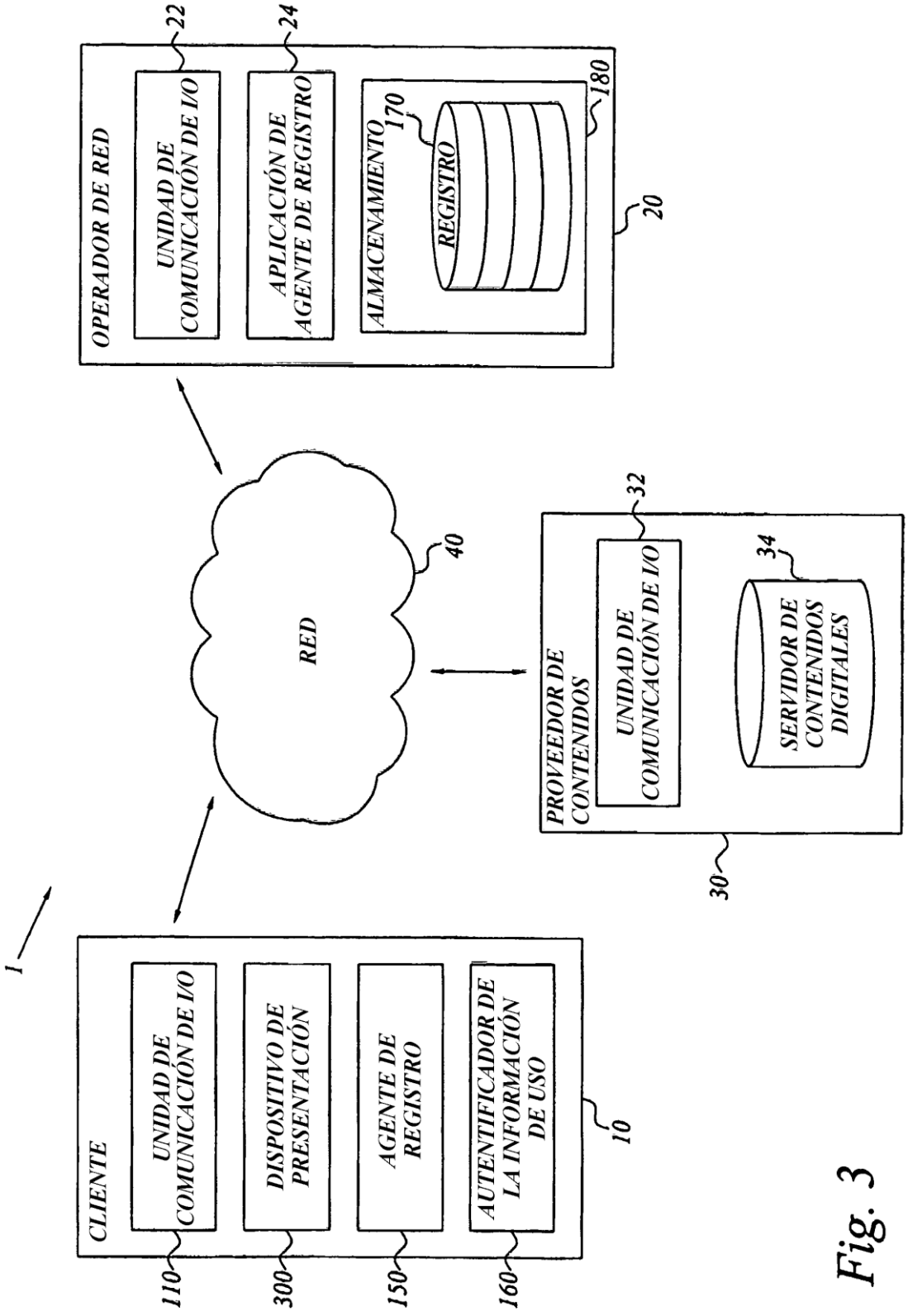

1
CLIENTE
UNIDAD DE COMUNICACIÓN DE I/O
DISPOSITIVO DE PRESENTACIÓN
AGENTE DE REGISTRO
AUTENTIFICADOR DE LA INFORMACIÓN DE USO
10
110
300
150
160
RED
40
OPERADOR DE RED
UNIDAD DE COMUNICACIÓN DE I/O
APLICACIÓN DE AGENTE DE REGISTRO
ALMACENAMIENTO
REGISTRO
170
180
20
22
24
PROVEEDOR DE CONTENIDOS
UNIDAD DE COMUNICACIÓN DE I/O
SERVIDOR DE CONTENIDOS DIGITALES
30
32
34

Fig. 3

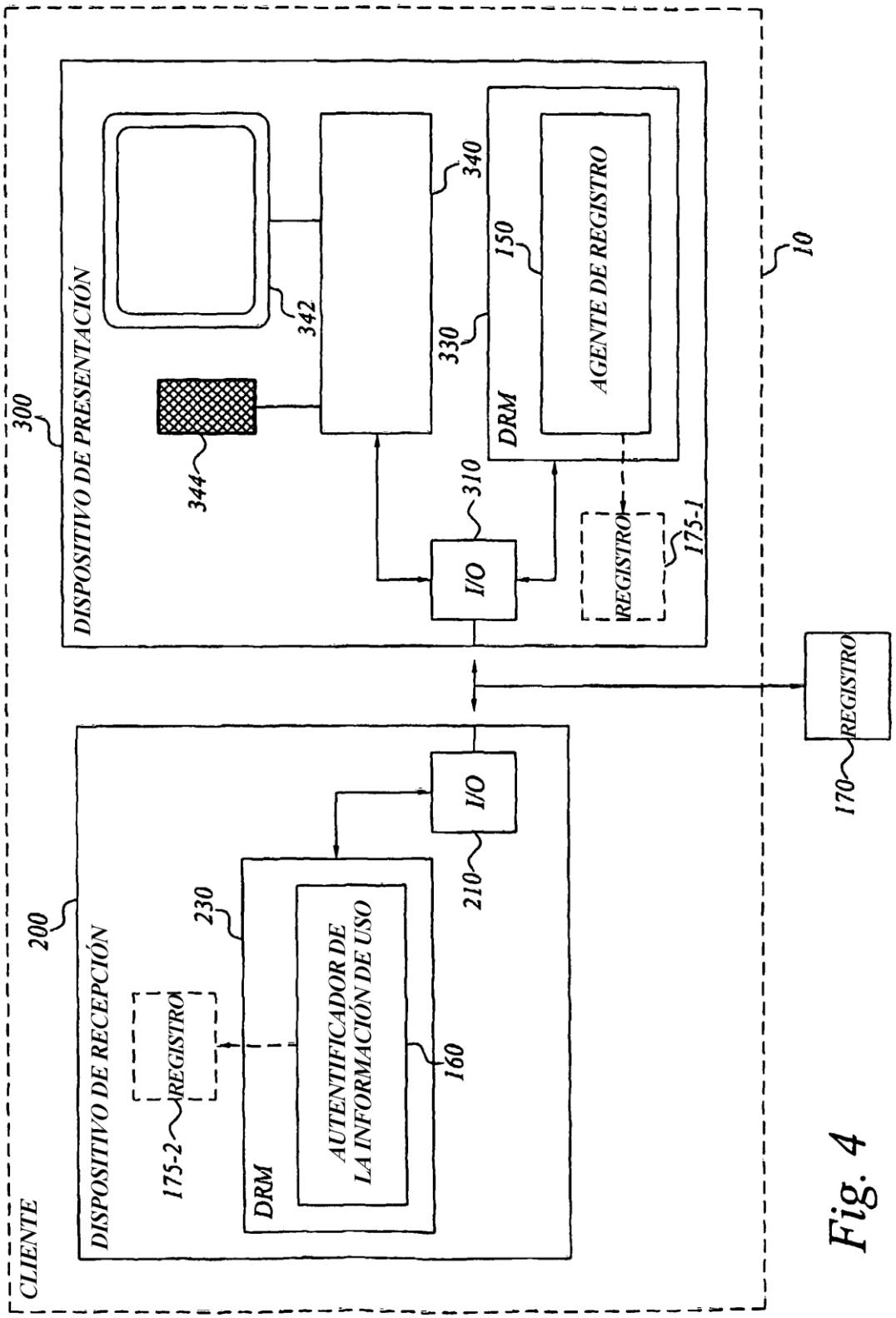

CLIENTE
10
DISPOSITIVO DE RECEPCIÓN
200
175-2
REGISTRO
230
DRM
AUTENTIFICADOR DE LA INFORMACIÓN DE USO
160
I/O
210
DISPOSITIVO DE PRESENTACIÓN
300
344
342
340
330
DRM
150
AGENTE DE REGISTRO
I/O
310
REGISTRO
175-1
REGISTRO
170

Fig. 4

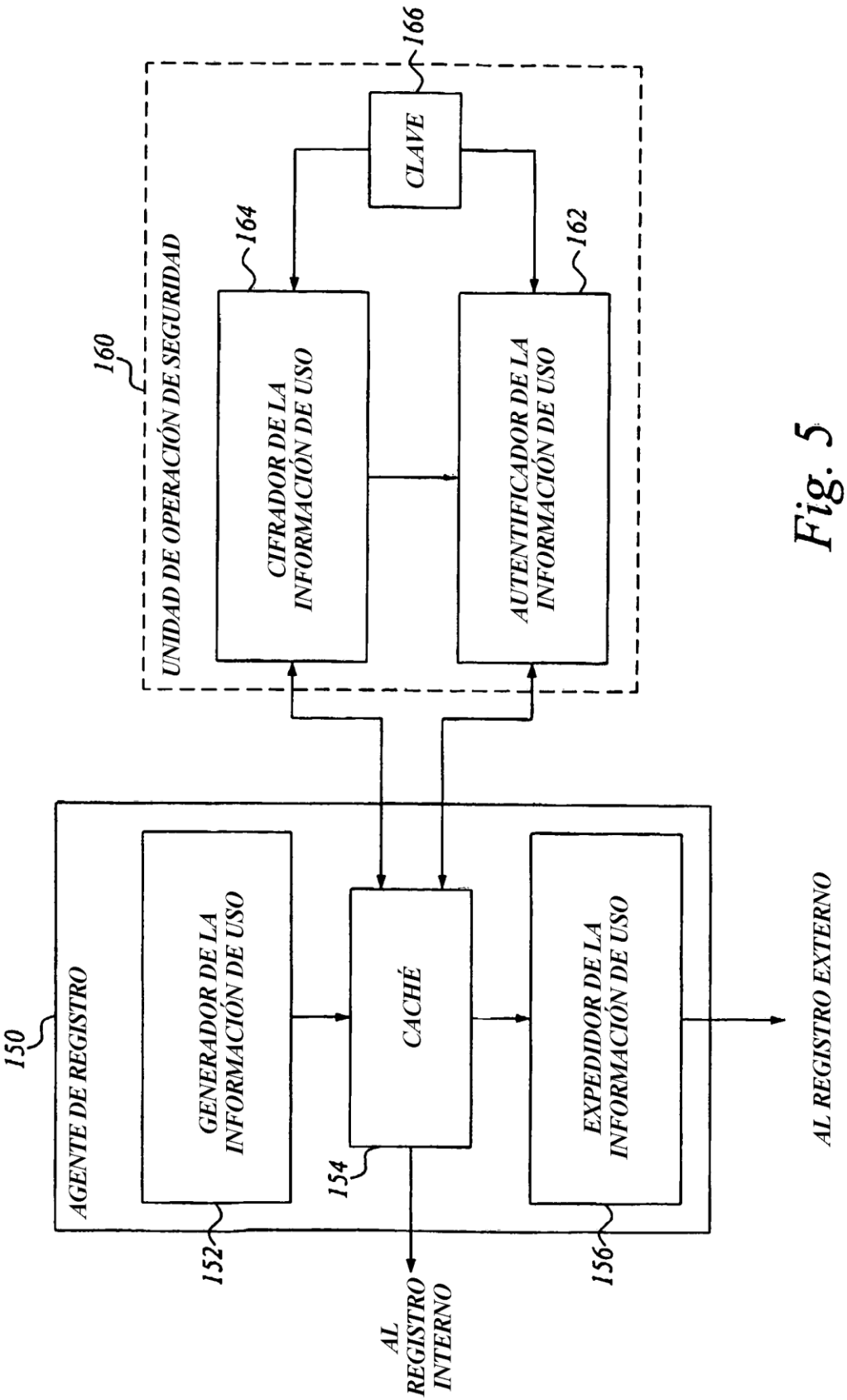
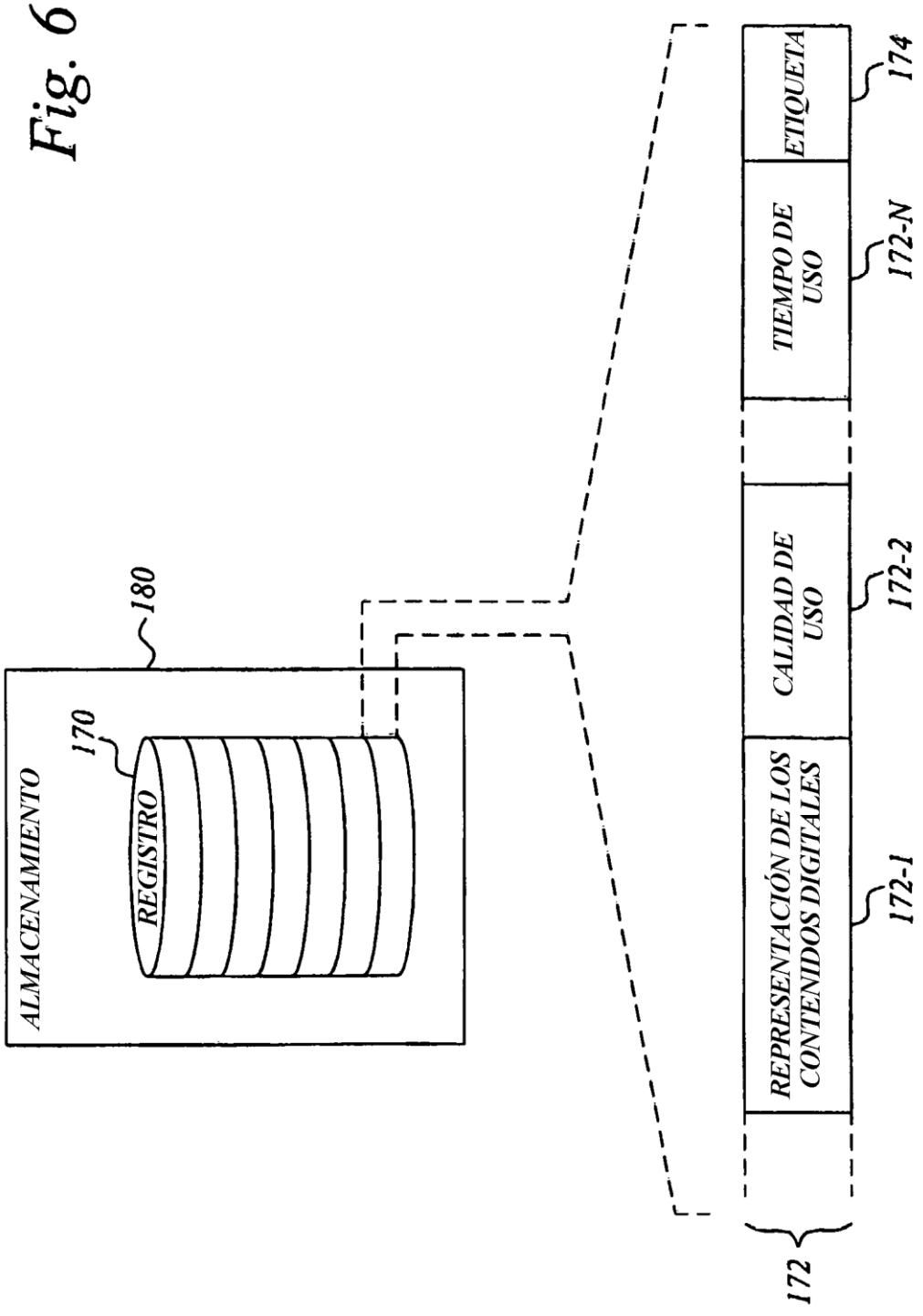

166
CLAVE
164
162
160
UNIDAD DE OPERACIÓN DE SEGURIDAD
CIFRADOR DE LA INFORMACIÓN DE USO
AUTENTIFICADOR DE LA INFORMACIÓN DE USO
150
AGENTE DE REGISTRO
GENERADOR DE LA INFORMACIÓN DE USO
CACHÉ
EXPEDIDOR DE LA INFORMACIÓN DE USO
AL REGISTRO EXTERNO
154
152
156
AL REGISTRO INTERNO

Fig. 5

Fig. 6


180
ALMACENAMIENTO
170
REGISTRO
172
REPRESENTACIÓN DE LOS CONTENIDOS DIGITALES
172-1
CALIDAD DE USO
172-2
TIEMPO DE USO
172-N
ETIQUETA
174

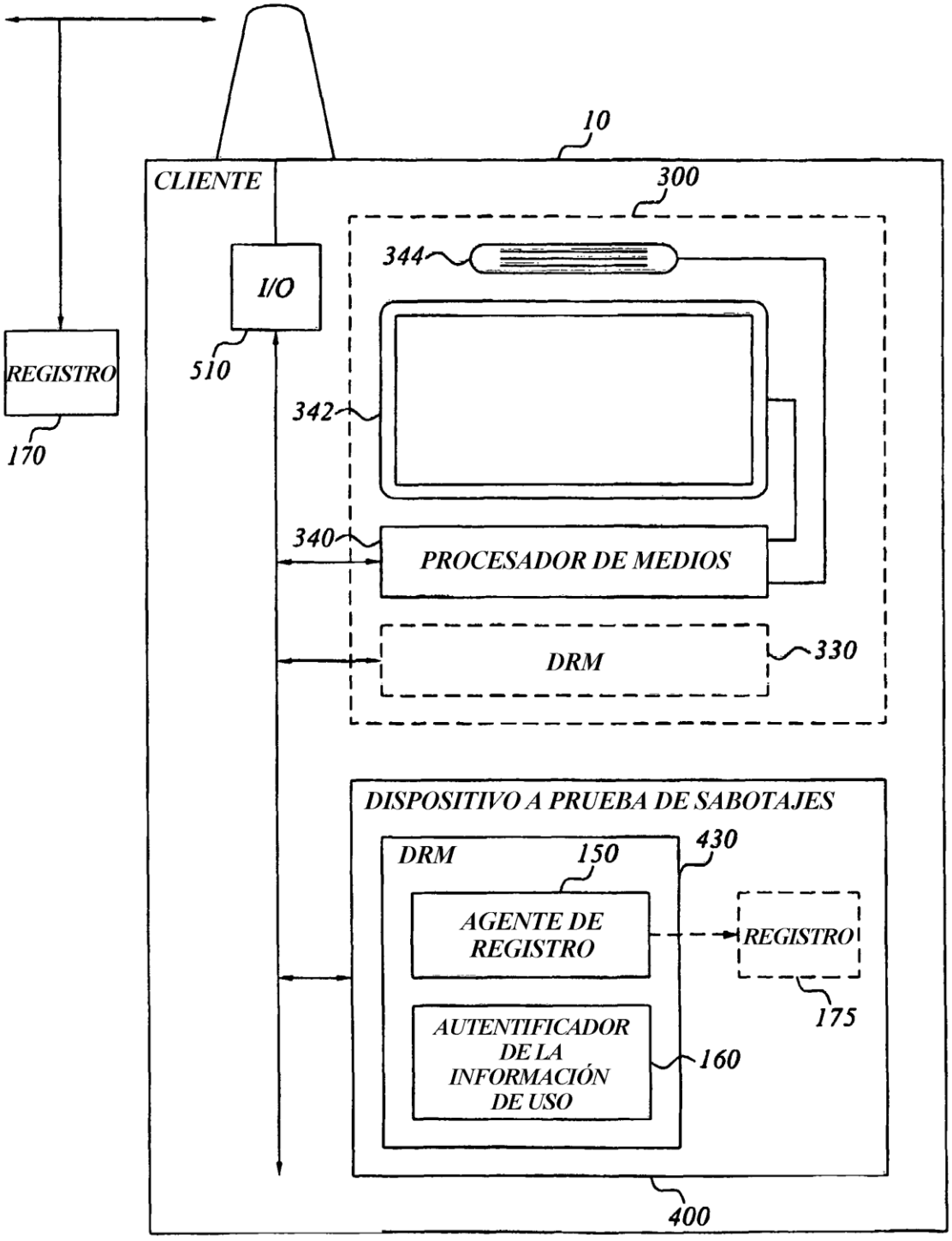

10
CLIENTE
300
344
I/O
510
REGISTRO
170
342
340
PROCESADOR DE MEDIOS
DRM
330
DISPOSITIVO A PRUEBA DE SABOTAJES
DRM
150
430
AGENTE DE REGISTRO
REGISTRO
175
AUTENTIFICADOR DE LA INFORMACIÓN DE USO
160
400

Fig. 7

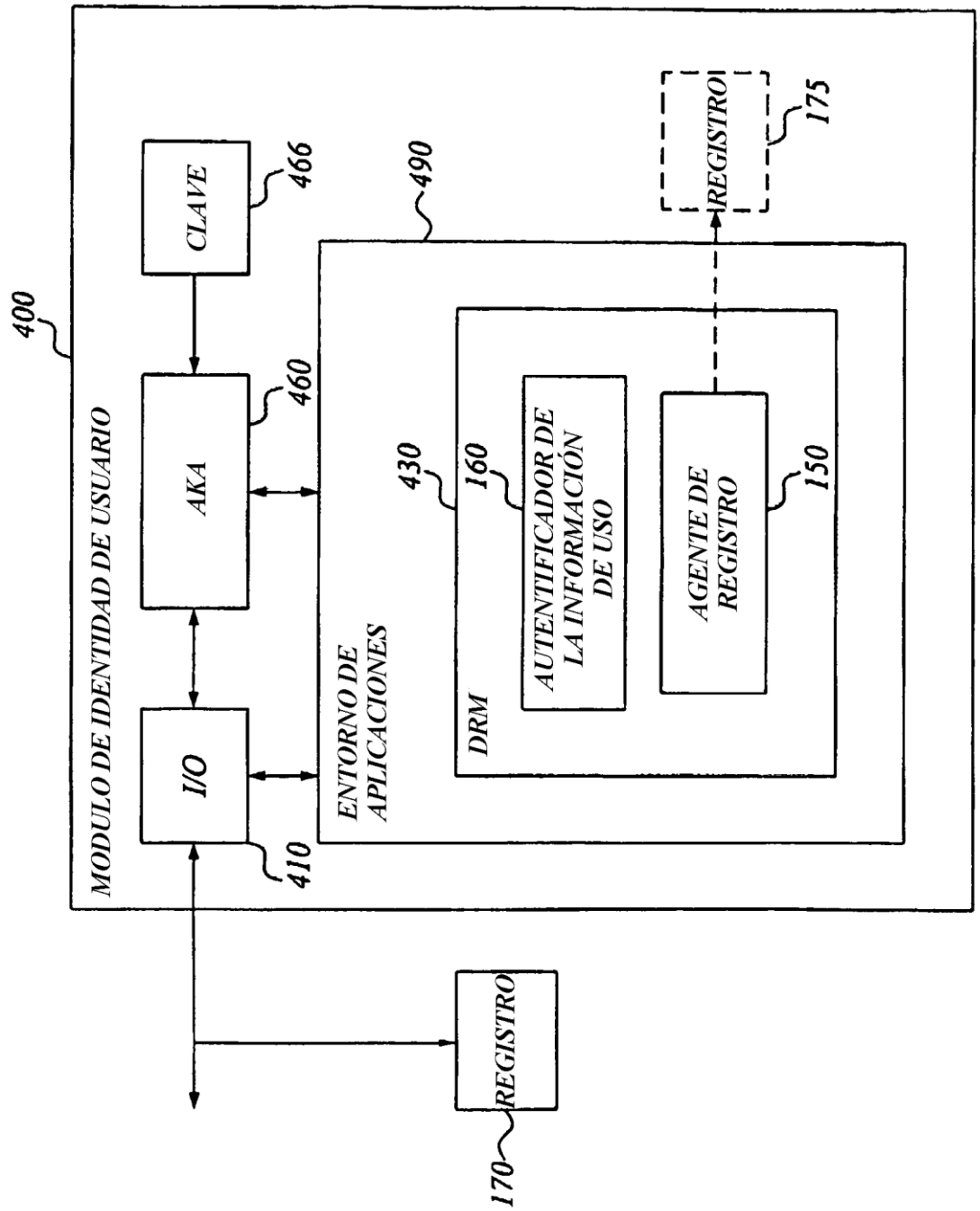

400
MODULO DE IDENTIDAD DE USUARIO
CLAVE
466
AKA
460
I/O
410
490
ENTORNO DE APLICACIONES
430
DRM
160
AUTENTIFICADOR DE LA INFORMACIÓN DE USO
AGENTE DE REGISTRO
150
REGISTRO
175
REGISTRO
170

Fig. 8

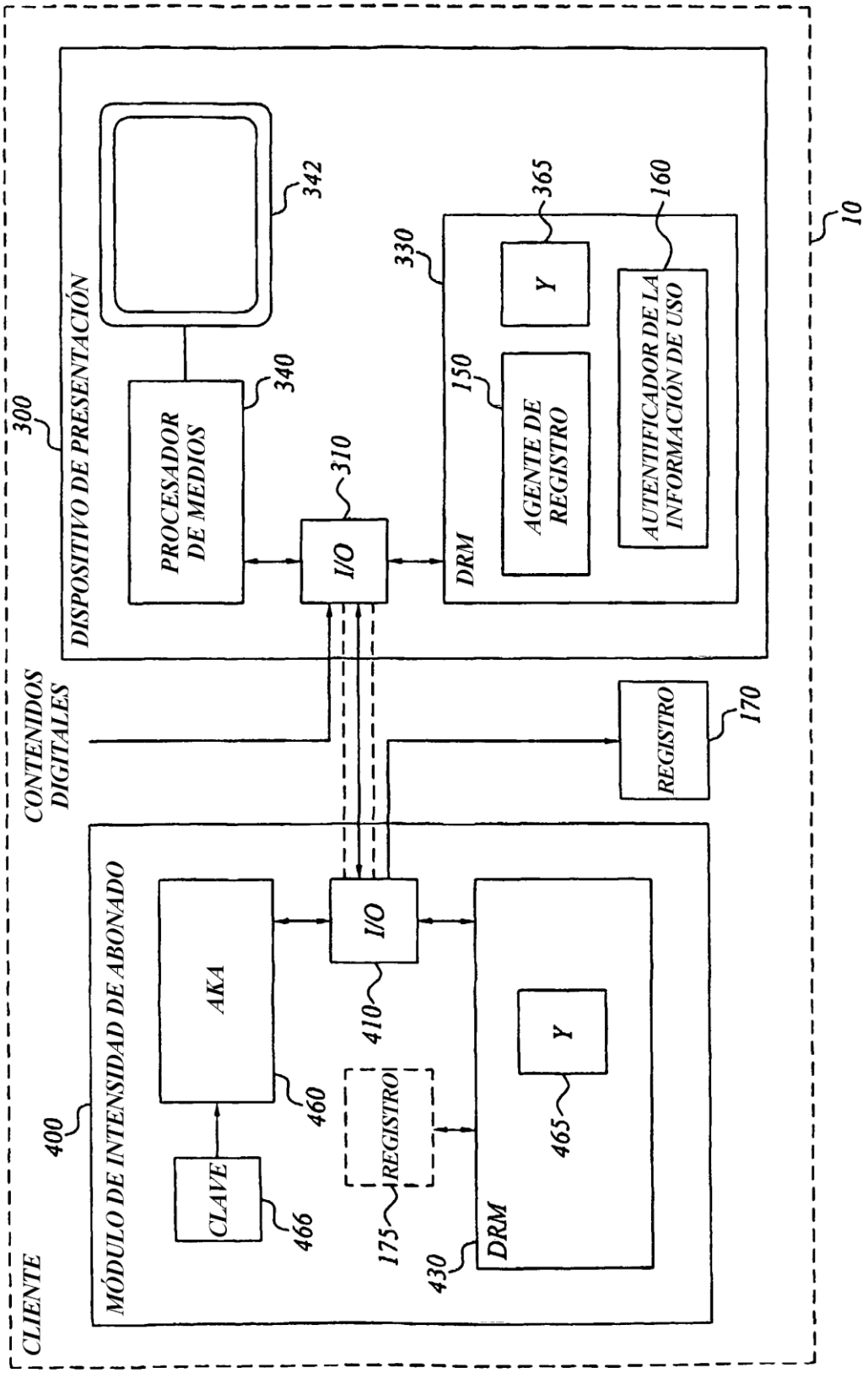

CLIENTE
10
DISPOSITIVO DE PRESENTACIÓN
300
342
PROCESADOR DE MEDIOS
340
I/O
310
330
DRM
AGENTE DE REGISTRO
150
Y
365
AUTENTIFICADOR DE LA INFORMACIÓN DE USO
160
CONTENIDOS DIGITALES
REGISTRO
170
MÓDULO DE INTENSIDAD DE ABONADO
400
AKA
460
CLAVE
466
I/O
410
REGISTRO
175
DRM
430
Y
465

Fig. 9

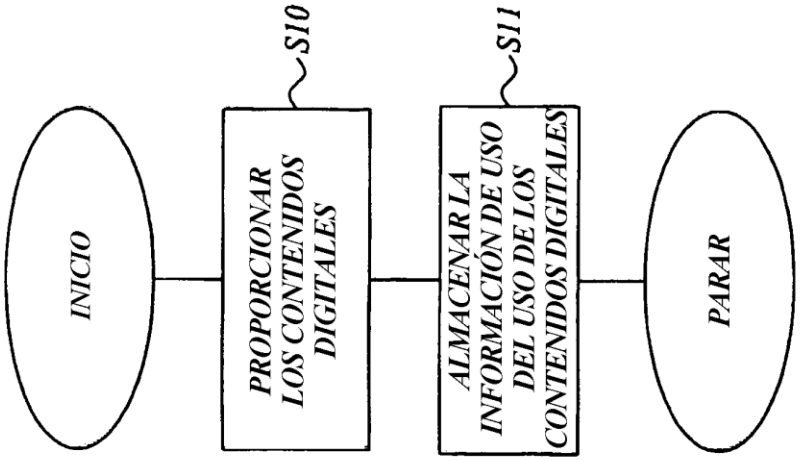

INICIO
S10
PROPORCIONAR LOS CONTENIDOS DIGITALES
S11
ALMACENAR LA INFORMACIÓN DE USO DEL USO DE LOS CONTENIDOS DIGITALES
PARAR

Fig. 14

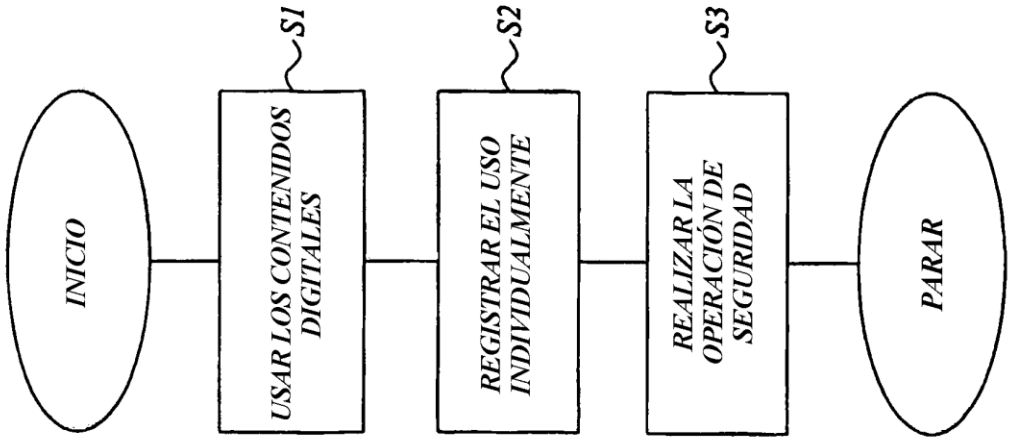

INICIO
S1
USAR LOS CONTENIDOS DIGITALES
S2
REGISTRAR EL USO INDIVIDUALMENTE
S3
REALIZAR LA OPERACIÓN DE SEGURIDAD
PARAR

Fig. 10

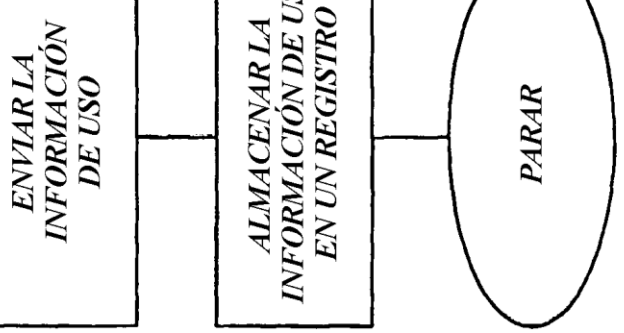


Fig. 13

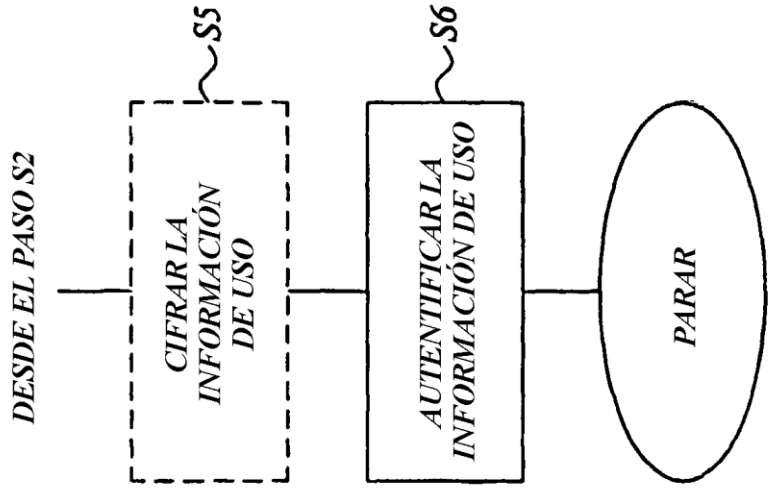


Fig. 12

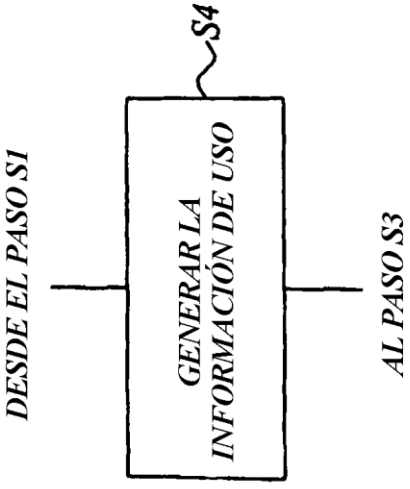


Fig. 11