(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACIÓN EN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la Propiedad Intelectual
Oficina internacional

(43) Fecha de publicación internacional
3 de octubre de 2013 (03.10.2013)

WIPO | PCT

(10) Número de Publicación Internacional
WO 2013/144384 A1

(51) Clasificación Internacional de Patentes:
G06Q 20/12 (2012.01) *H04L 9/14* (2006.01)

(21) Número de la solicitud internacional:
PCT/ES2012/070208

(22) Fecha de presentación internacional:
27 de marzo de 2012 (27.03.2012)

(25) Idioma de presentación: español

(26) Idioma de publicación: español

(72) Inventor; e

(71) Solicitante : **CARRILLO DE LA FUENTE, Miguel Angel** [ES/ES]; Avenida De Entrevias, Num 66 Piso 4º B, E-28053 Madrid (ES).

(81) Estados designados *(a menos que se indique otra cosa, para toda clase de protección nacional admisible)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Estados designados *(a menos que se indique otra cosa, para toda clase de protección regional admisible)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europea (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publicada:

— *con informe de búsqueda internacional (Art. 21(3))*

[Continúa en la página siguiente]

(54) **Title**: PROTECTION METHOD AND SYSTEM FOR DISTRIBUTING DIGITAL FILES WHETHER NEW, SECOND-HAND, FOR RENTAL, EXCHANGE OR TRANSFER

(54) **Título** : MÉTODOS PROTECCIÓN Y SISTEMA DISTRIBUCIÓN DE FICHEROS DIGITALES DE PRIMERA/SEGUNDA MANO, ALQUILER, INTERCAMBIO Y CESIÓN

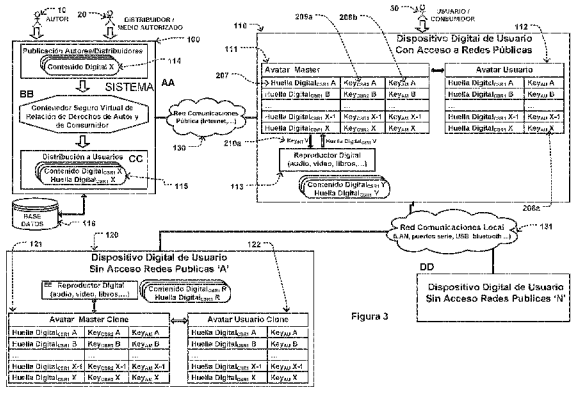


Figura 3

10 Author
20 Distributor / authorised medium
30 User /consumer
110 Digital user device with access to public networks
111 Avatar Master
112 Avatar User
116 Database
120/DD Digital user device without access to public networks 'A'
121 Avatar Master clone
122 Avatar User clone
130 Public communication network (Internet, etc.)
131 Local communication network (LAN, serial ports, USB, Bluetooth, etc.)
114 Digital content
AA System
BB Virtual secure container for relating the rights of the author and consumer
CC Distribution to users
Publicación Autores/Distribuidores... Author/distributor publication
Huella digital... Digital fingerprint

(57) **Abstract**: The invention relates to methods for generating a virtual recursive secure container and for generating a virtual secure container for relating rights together with a system for distributing digital content by an author in compliance with the legal framework for intellectual property when distributed electronically, whether via the internet or any other digital medium and offers consumers their rights as purchasers of the digital content. The digital content can be of different types, such as electronic books, digital video files, digital music files, computer applications, computer programs or any digital work which, in order to be used and/or enjoyed, requires a digital device (for example: portable personal computers, MP3 music players, MP4 players, video players, mobile devices, iTablets, eBooks, etc.). The scenarios for distributing digital content to a digital user device enabled by the invention are new, second-hand, rental, exchange and temporary transfer / gift. Distributions in second-hand/exchange/transfer mode are only possible if the user has acquired the digital content via the invention, in either the new, second-hand, exchange or gift modes. The software components of the invention, 'Avatar Master' and 'Avatar User', which reside in the digital devices of the user, create the virtual framework for relating the rights of the author and consumer, wherein Avatar Master ensures that copyright is not violated and Avatar User maintains the rights of the consumer when digital content is purchased. Since each avatar has one of the keys for deciphering the data of the digital content distributed by the system, the virtual link is created for relating the rights of the author and consumer. The combination of the method for generating a virtual recursive

[Continúa en la página siguiente]

WO 2013/144384 A1

— *con reivindicaciones modificadas (Art. 19(1))*

secure container which establishes virtual links for relating to a digital file, together with the unique distribution of at least one of the encryption keys that results from the method for generating the virtual recursive secure container to a series of avatars forms a virtual secure relation container. The invention only distributes digital content in a virtual secure container for relating the rights of the author and consumer which an author or authorised medium has published beforehand in the system, granting its authorisation as author / authorised medium of the digital content for distribution via the modes enabled by the system.

(57) Resumen: Métodos de generación de un contenedor seguro recursivo virtual y de generación de un contenedor seguro virtual de relación de derechos junto con un sistema para la distribución de contenidos digitales de autor respetando el marco legal de la propiedad intelectual cuando se distribuye electrónicamente, bien a través de Internet o de cualquier otro medio digital y ofrece a los consumidores sus derechos como comprador del contenido digital. El contenido digital puede ser de diferentes naturalezas, tales como un libro electrónico, un archivo digital de video, un archivo digital de música, una aplicación informática, un programa de computadora o cualquier trabajo digital que para su uso y/o disfrute sea necesario un dispositivo digital (por ejemplo: ordenador personal y portátil, reproductores música mp3, mp4, reproductores de video, dispositivos móviles, iTablets, eBooks, etc.). Los escenarios de distribución de un contenido digital a un dispositivo digital de usuario que permite la invención son primera mano, segunda mano, alquiler, intercambio y cesión temporal/ regalo. Las distribuciones en modalidad de segunda mano/intercambio/cesión sólo son posibles si el usuario ha adquirido el contenido digital a través de la invención, bien por la modalidad de primera mano/segunda mano/intercambio/regalo. Los componentes lógicos de la invención, 'Avatar Master' y 'Avatar Usuario', que residen en los dispositivos digitales del usuario crean el marco virtual de relación de derechos de autor y de consumidor, donde el avatar master custodia que no se infringen los derechos de autor y el avatar usuario mantiene los derechos del consumidor cuando compra un contenido digital. Al disponer cada avatar una de las claves para poder descifrar los datos del contenido digital distribuido por el sistema se crea el nexo virtual de relación de derechos de autor y de consumidor. La combinación del método de generación de un contenedor seguro recursivo virtual que establece nexos virtuales de relación a un fichero digital, junto con la distribución de manera única de al menos de una de las claves de cifrado resultado del método de generación contenedor seguro recursivo virtual a un conjunto de avatares forma un contenedor seguro virtual de relación. La invención sólo distribuye contenidos digitales en un contenedor seguro virtual de relación de derechos de autor y de consumidor que previamente un autor o un medio autorizado lo ha publicado en el sistema y da su autorización como autor/medio autorizado del contenido digital para su distribución mediante las modalidades que permite el sistema.

Descripción

Título de la invención: MÉTODOS PROTECCIÓN Y SISTEMA DISTRIBUCIÓN DE FICHEROS DIGITALES DE PRIMERA/ SEGUNDA MANO, ALQUILER, INTERCAMBIO Y CESIÓN

Sector técnico

[1] La invención se refiere a la protección y distribución de contenidos digitales de autor respetando el marco legal de la propiedad intelectual cuando se distribuye electrónicamente, bien a través de Internet o de cualquier otro medio digital y ofrece a los consumidores sus derechos como comprador del contenido digital.

[2] El contenido digital puede ser de diferentes naturalezas, tales como un libro electrónico, un archivo digital de video, un archivo digital de música, una aplicación informática, un programa de computadora o cualquier trabajo digital que para su uso y/ o disfrute sea necesario un dispositivo digital.

[3] Los términos 'contenido digital' o 'trabajo digital' o 'fichero digital' se utilizan aquí de manera sinónima, y para los tres términos, se refiere a cualquier tipo de elemento que tiene un contenido que para su uso y/o disfrute sea necesario un dispositivo digital.

[4] Los escenarios de distribución que proporciona la invención son:

- Distribución en modalidad de 'Primera Mano', cuando un usuario adquiere el trabajo digital a través de la invención directamente de la publicación del autor o desde un medio autorizado.
- Distribución en modalidad de 'Segunda Mano', cuando un usuario vende el trabajo digital a otro usuario, por lo tanto, ya no puede volver a hacer uso del contenido digital.
- Distribución en modalidad de 'Alquiler', cuando un medio autorizado realiza un alquiler de un contenido digital a un usuario.
- Distribución en modalidad de 'Intercambio', cuando dos usuarios se intercambian un contenido digital, en esta modalidad dos usuarios realizan un intercambio de contenidos digitales diferentes.
- Distribución en modalidad de 'Cesión', cuando un usuario realiza una cesión temporal del contenido digital a otro usuario y no existe ninguna transacción económica entre el usuario que cede el contenido digital y el usuario que recibe temporalmente el uso del contenido digital. Durante el periodo de la cesión temporal, el usuario que transfiere temporalmente el contenido digital ya no podrá hacer uso del contenido digital, mientras que el usuario que recibe la cesión temporal podrá hacer uso del trabajo digital. Esta modalidad de distribución también incluye la modalidad de 'regalar' un contenido digital a otro

usuario en donde no se pone un límite a la temporalidad de la cesión del contenido digital.

[5] La invención proporciona a cada contenido digital la capacidad de disponer copias con su propia huella digital que lo diferenciará del resto de copias del fichero digital original, como del resto de contenidos digitales protegidos y distribuidos.

[6] Cada copia del trabajo digital tiene su propia huella digital, y cuando se distribuye a un usuario va protegido en un contenedor seguro virtual de relación de derechos de autor y de consumidor, para de esta manera siempre garantizar los derechos del autor y asegurar que sólo puede hacer uso de la copia del trabajo digital el usuario que ha adquirido el contenido digital a través de la invención.

Técnica anterior

[7] El contenido digital, ha ganado popularidad sobre el contenido analógico principalmente por dos cuestiones, la primera es por las ventajas técnicas asociadas con su producción, reproducción y manipulación, y la segunda porque hay, a veces, mejor calidad percibida que su contraparte analógica. Desde el nacimiento de los ordenadores personales, los archivos de contenido digital se han convertido en un medio fácil de copiar un número ilimitado de veces sin sufrir degradación alguna en la calidad de las copias realizadas. Normalmente, los contenidos analógicos pierden calidad con cada generación copiada, y frecuentemente durante su uso normal.

[8] Desde la aparición del medio de comunicación de Internet, las vías de difusión, promoción y distribución de todo tipo de productos y contenidos se han multiplicado de forma exponencial. Internet, permite una conexión instantánea con todos los rincones del mundo, facilitando la comunicación con personas situadas a veces a miles de kilómetros del sujeto emisor, sin que por ello exista limitación alguna en la transmisión del contenido o de los mensajes. Entre los contenidos que pueden comunicarse a través de Internet, está toda modalidad de expresión artística empaquetado en un contenido digital.

[9] Internet permite compartir nuestras creaciones artísticas, nuestros intereses y gustos culturales con cualquier sujeto conectado a un ordenador en cualquier lugar del mundo, y junto con la popularización de las herramientas para compartir archivos han simplificado la distribución de los contenidos digitales con derechos de autor.

[10] El sector de la música, películas, libros digitales entre otros, están siendo los primeros en vivir esta revolución en la difusión y distribución de contenidos digitales. Ante un mercado con tan atractivo horizonte, es inevitable que a su vez existan múltiples discusiones y disputas sobre las fórmulas más adecuadas de utilización de Internet en cuanto a la difusión de los contenidos digitales de autor.

[11] En un sector a veces algo convulsionado, es preciso mantener un objetivo claro con

independencia de los modelos de negocio e intereses económicos que se defiendan. Este objetivo debería girar siempre en torno a la defensa de los derechos derivados de la creación de los contenidos digitales y en especial del creador único del contenido digital, el autor, y sin por otro lado descuidar los derechos e intereses de los consumidores, el usuario.

[12] Se han definido un amplio conjunto de tecnologías para resolver la protección de los derechos de propiedad intelectual, los cuales han sido designados como 'Gestión de los Derechos de Propiedad Intelectual' (IPRM), 'Gestión de los Derechos de Propiedad Digital' (DPRM), 'Gestión de la Propiedad Intelectual' (IPM), 'Gestión de Derechos' (RM), y 'Gestión de Copyright Electrónico' (CM), referidos aquí colectivamente como 'Gestión de Derechos Digitales' (DRM).

[13] DRM es un término genérico que se refiere a las tecnologías de control de acceso utilizado por editoriales y dueños de los derechos de autor para limitar el uso de medios o dispositivos digitales. También se puede referir a las restricciones asociadas a instancias específicas de obras digitales o dispositivos.

[14] Para la gestión de los derechos digitales, por ejemplo, se debe tener en cuenta: autenticación, autorización, contabilidad, pago y liquidación financiera, especificación de los derechos, verificación de los derechos, protección de los derechos y protección de los documentos. Las patentes de los Estados Unidos 5.530.235, 5.634.012, 5.715.403 y 5.629.980 describen conceptos DRM que se refieren a estos asuntos.

[15] La disponibilidad de múltiples copias perfectas de material protegido es percibida por la industria de los medios como un problema para su viabilidad y su coste, particularmente dentro de la industria de la música, del cine y de los videojuegos. Quienes publican material digital tienen típicos modelos de negocios que recaen en la habilidad de obtener una tarifa por cada copia hecha del trabajo digital, y algunas veces por cada ejecución de dicho trabajo.

[16] DRM fue creado o diseñado por quienes publican un contenido digital con medidas para permitirles el control de la duplicación y distribución de su contenido digital. El objetivo principal consiste en asignar un conjunto de derechos digitales al contenido digital y su posterior gestión. Los diferentes mecanismos de DRM, diseñados por distintas empresas, en general todos tienen en común algunas características:

[17] - Pueden detectar quién accede a cada trabajo digital, cuándo y bajo qué condiciones.

[18] - Autorizan o deniegan el acceso al contenido digital, de acuerdo a condiciones que pueden ser cambiadas unilateralmente por el proveedor del trabajo digital.

[19] - Cuando autorizan el acceso, lo hacen bajo condiciones restrictivas que son fijadas unilateralmente por el proveedor del contenido digital, independientemente de los derechos que la ley otorgue al autor o al consumidor.

[20] Se ha empleado dos esquemas DRM básicos, contenedores seguros y sistemas de

confianza. Un 'contenedor seguro' (o simplemente un contenido digital encriptado) ofrece una forma de mantener encriptado el contenido del trabajo digital hasta que se cumple un conjunto de condiciones de autorización y se cumplen algunos términos del copyright (por ejemplo, pago por uso). Después de verificar varias condiciones y términos con el proveedor de contenidos digitales, el contenido digital es entregado al usuario en forma clara.

[21] Productos comerciales como CRYPTOLOPES™ y DIGIBOXES™ implementan el esquema del contendor seguro. El método del contenedor seguro proporciona una solución para proteger un contenido digital durante la entrega por canales inseguros, pero no proporciona ningún mecanismo para evitar que los usuarios legítimos obtengan el contenido digital en claro y después lo usen y redistribuyan en violación de la propiedad intelectual de los propietarios de los contenidos digitales.

[22] En el método del 'sistema de confianza', todo el sistema es responsable de evitar el uso no autorizado y la distribución del documento. Construir un sistema de confianza implica por lo general introducir nuevo hardware tal como un procesador seguro, almacenamiento seguro y dispositivos de presentación seguros. Esto también requiere que se certifique que todas las aplicaciones de software que se ejecutan en 'sistemas de confianza' son de confianza. Aunque la construcción de un sistema de confianza a prueba de manipulación es un reto real para las tecnologías existentes, las tendencias actuales del mercado sugieren que los sistemas sean abiertos y de confianza.

[23] La mayoría de los esfuerzos se han orientado sobre los derechos de propiedad en lo referente a los creadores o autores, pero dejando de lado los derechos de los consumidores. Cuando un usuario compra un objeto, servicio u obra, el usuario adquiere ciertos derechos asociados. Sin embargo, muchas veces estos derechos no son tan obvios ni explícitos, más aún, las nuevas tecnologías han permitido el olvido de algunos de los derechos de los consumidores.

[24] Habría que responder a la cuestión de qué es lo que adquiere un usuario cuando compra una modalidad de expresión artística empaquetado en un contenido digital. Durante muchos años, por ejemplo, la música se vendía y se distribuía usando discos de vinilo. Estos discos de vinilo, con el cuidado necesario, pueden durar muchos años (más que la vida promedio de un ser humano, por ejemplo). Por lo tanto, al comprar un disco de vinilo un consumidor está comprando el derecho de escucharlo por toda su vida. Al mismo tiempo, tiene el derecho a regalarlo, o a venderlo nuevamente.

[25] En la década de los 1980s la tecnología cambió y el cassette se convirtió en la forma más común para vender y distribuir. Lamentablemente, los cassettes no tienen una vida infinita o tan larga como la de los discos de vinilo, pero sí es lo suficientemente larga como para que un usuario no percibiera la disminución en la longevidad de los derechos como consumidor.

[26] Después del cassette, vinieron los discos ópticos (DVDs (Digital Versatile Disc), CDs (Compact Disk), etc.), mejor sonido pero los mismos problemas, y la vida de los discos ópticos es aún más corta que la del cassette. Pero el paso más importante en ese momento, fue hacia los contenidos digitales que no envejecen. La secuencia de 0s y 1s puede ser almacenada para siempre sin pérdida de calidad.

[27] Con la llegada de los contenidos digitales se produce un nuevo debate, ¿qué adquiere un consumidor cuando compra un contenido digital? ¿la secuencia de 1s y 0s? ¿o sólo el usuario es dueño del objeto físico que contiene esta secuencia?.

[28] Si el consumidor compra la secuencia de 1s y 0s entonces el usuario debería tener todo su derecho de usar cualquier dispositivo para reproducirla, almacenar la secuencia en un dispositivo digital y moverla al dispositivo digital que más le guste. Más aún, en nuestros días, sería muy sencillo regalar un contenido digital, simplemente sería pasar la secuencia de 1s y 0s, y posteriormente se borraría el contenido digital de todos los dispositivos digitales en los que hubiese una copia, por lo tanto, se podría estar en presencia de una extensión o ampliación de los derechos como consumidores.

[29] Lamentablemente no es el caso, las compañías a cargo de la venta y distribución de contenidos digitales de autor despliegan esfuerzos para evitar mantener los derechos como consumidores cuando se compra un contenido digital. Muchos sistemas actuales limitan el traslado de la secuencia de 1s y 0s a otros dispositivos. Existen limitaciones para almacenar, copiar o regalar música.

[30] No obstante, también se ha trabajado para proporcionar derechos a los consumidores, las patentes PCT/US2010/062658 y PCT/US2011/044964 describen una plataforma conocida comercialmente como ReDigi™, que venden contenidos digitales (archivos de música) de 'segunda mano'. La plataforma en cuestión permite al usuario deshacerse de temas que ya no escucha, para así obtener a cambio descuentos aplicables en la compra de nuevas canciones. La patente PCT/US2005/043142 permite un mercado de contenidos digitales usados entre terminales móviles y un almacenamiento electrónico seguro.

[31] UltraViolet™ (UV) propone una plataforma DRM basada 100% en la nube. UV como plataforma DRM puede proteger cualquier medio, desde películas hasta música, pasando por libros electrónicos o series de televisión. UV puede autorizar a través de una interfaz web hasta 12 dispositivos de reproducción. Así mismo, hasta 6 usuarios pueden estar viendo un mismo contenido de forma simultánea. También, en esos servidores centralizados de UV quedan almacenados los datos del usuario: dónde y cuándo ha reproducido un contenido así como con quién lo ha compartido. Un hándicap en esta plataforma DRM es la compatibilidad. Todo el contenido licenciado bajo UV únicamente puede estar disponible en dispositivos que lo soporten. Estos dispositivos incluyen desde televisores, tablets, discos duros, móviles y portátiles. Por

otra parte, la mayoría de ellos requieren estar conectados a la nube de alguna manera para gestionar el acceso a las licencias.

[32] La IEEE Project P1817 - Standard for Consumer-ownable Digital Personal Property, trabajan en estándares que describe los métodos, algoritmos, protocolos y mecanismos de gestión que participan en la protección criptográfica de las obras con derechos de autor de la redistribución pública y en la preservación de la autonomía de los consumidores y la privacidad. La IEEE, está estudiando una nueva propuesta que podría suponer una alternativa al DRM, la DPP (Digital Personal Property). La Digital Personal Property es un sistema que permite copiar libremente pero que precisa de una clave de acceso a los contenidos. La clave no se puede copiar, pero sí se puede transferir a quien se quiera. La tecnología DPP funciona en que el contenido digital protegido consta de dos elementos, una carpeta con el archivo en cuestión y una clave a la que acceder a través de un enlace. La carpeta con los archivos se puede copiar y compartir sin restricciones, pero para poder disfrutar de su contenido digital hay que transferir la clave, que no puede ser copiada, sólo movida.

[33] La principal barrera a eliminar para que se pueda mantener los derechos como consumidores es asegurar que cuando un usuario vende, intercambia o regala un contenido digital, dicho contenido digital sea verdaderamente eliminado/borrado de todos los dispositivos digitales del usuario que realiza la venta, intercambio o regalo, o aunque hubiese una copia del contenido digital, no fuera posible hacer uso del mismo.

[34] Los objetivos de la invención son proporcionar una distribución segura durante la entrega del contenido digital, una protección de los derechos de propiedad intelectual de uso idéntica a cuando el contenido digital se distribuye en un formato físico (papel impreso (por ejemplo, libros,...), discos ópticos (DVDs, CDs, etc.) y permitir los modelos de distribución de contenidos digitales de primera mano, segunda mano, alquiler, intercambio y cesión temporal/regalo a través de la invención.

[35] Todo contenido digital que distribuye la invención se realiza bajo un contenedor seguro virtual de relación de derechos de autor y de consumidor que combina un método de generación de un contenedor seguro recursivo virtual con el uso de dos componentes lógicos de la invención: 'Avatar Master' y el 'Avatar Usuario'. Los avatares crean el marco virtual de relación de derechos de autor y de consumidor. El Avatar Master asegura los derechos de autor mientras que el Avatar Usuario mantiene los derechos del consumidor que compra un contenido digital.

Divulgación de la invención

Problema técnico

[36] En la actualidad, un consumidor tiene la posibilidad de vender, intercambiar o dejar prestado: un libro, un DVD/CD de música, etc. a otra persona, cediendo todos los

derechos a la nueva persona poseedora del artículo físico. Las bibliotecas realizan préstamos de libros a los usuarios permitiendo la difusión del conocimiento y de la cultura de manera universal respectando los derechos de autor, y en las tiendas autorizadas se permiten el alquiler de películas, dos usuarios deciden por mutuo acuerdo intercambiarse un libro.

[37] La invención proporciona una protección de los derechos de propiedad intelectual de uso idénticos a cuando el contenido digital se distribuye en un formato físico y proporciona los modelos de distribución electrónica de contenidos digitales (primera mano, segunda mano, alquiler, intercambio y cesión temporal/regalo) respetando en todo momento los derechos de autor, tal y como actualmente se dispone cuando el contenido digital se ha distribuido en un formato físico.

Solución a problema

[38] De acuerdo con la invención, los objetivos descritos de la invención se consiguen mediante la utilización de técnicas de criptografía. Las técnicas de criptografía que se usan en la invención son técnicas de cifrado simétrico, técnicas de cifrado asimétrico, técnicas de resumen criptográfico y la firma digital.

[39] Las dos 'claves' o 'claves de cifrado', ambos términos se utilizan aquí de manera sinónimas, implicadas en el proceso de cifrado/descifrado pueden ser o no iguales dependiendo del sistema de cifrado utilizado.

[40] **Técnicas de Cifrado Simétrico**

[41] Las técnicas de cifrado simétrico permiten cifrar y descifrar mensajes mediante la misma clave.

[42] AES (Advanced Encryption Standard) es uno de los algoritmos más utilizados, ya que se convirtió en estándar en 2002. Utiliza un tamaño de bloque de 128 bits y claves de 128, 192 o 256 bits. AES es rápido tanto por software como por hardware, es relativamente sencillo de implementar y requiere poca memoria en el proceso.

[43] **Técnicas de Cifrado Asimétrico**

[44] Las técnicas de cifrado asimétrico (algoritmos de clave pública y privada) son algoritmos que utilizan dos claves diferentes para cifrar y descifrar mensajes. Una de las claves se publica (clave pública) y la otra se mantiene privada (clave privada).

[45] RSA es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente. El algoritmo fue patentado por el MIT en 1983 en Estados Unidos con el número 4.405.829 y la patente expiró en el 2000.

[46] **Técnicas de Resumen Criptográfico**

[47] Las técnicas de resumen criptográfico permiten asignar a un contenido digital de una huella digital de encriptado, es decir, un resumen criptográfico con el objetivo de disponer de una identificación única del contenido digital. Un hash que permite crear

una huella digital, teóricamente única, de un archivo. Una colisión entre hashes supondría la posibilidad de la existencia de dos documentos con la misma huella. Entre las técnicas de resumen criptográfico están MD5 y SHA-512.

[48] **Firma Digital**

[49] Las firmas digitales se utilizan comúnmente para la distribución de software, transacciones financieras y en otras áreas donde es importante detectar la falsificación y la manipulación. La firma digital es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma digital.

[50] La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente. Funciona en una sola dirección, es decir, no es posible, a partir del valor resumen, calcular los datos originales.

[51] **Uso de cada Técnica Criptográfica en la Invención**

[52] Las técnicas de cifrado simétrico y las técnicas de cifrado asimétrico se utilizan en la invención para cifrar/descifrar los contenidos digitales y las claves de cifrado en un contenedor seguro recursivo virtual. Además, las técnicas de cifrado asimétrico se usan en la invención para proporcionar un entorno de confianza entre los componentes lógicos de la invención. Toda comunicación entre los componentes lógicos se realiza de manera segura y de confianza con la finalidad de asegurar todos los derechos de autor de un contenido digital.

[53] Las técnicas de resumen criptográfico proporcionan a cada contenido digital con un contenedor seguro iterativo una huella digital. Esta huella digital es lo que le diferencia del resto de contenidos digitales con un contenedor seguro virtual de relación de derechos de autor y de consumidor distribuidos por la invención.

[54] La huella digital permite que un contenido digital con un contenedor seguro virtual de relación de derechos de autor y de consumidor pueda ser distribuido en las modalidades de segunda mano, alquiler, intercambio y cesión temporal/regalo, ya que al disponer el contenido digital un identificador único, las claves de cifrado para generar el contenedor seguro recursivo virtual podrán ir transfiriéndose a los avatares (master y de usuario) y de esta manera sólo podrá hacer uso del contenido digital con un contenedor seguro virtual de relación de derechos de autor y de consumidor los avatares que en esos instantes dispongan las claves de cifrado de relación de derechos.

[55] Además, las firmas digitales se utilizan en la invención para validar y verificar que todos los componentes lógicos que se ejecutan son de confianza. Todos los componentes lógicos deben ser de confianza, que no han sufrido ninguna modificación por terceros, y de esta manera asegurar que en ningún componente lógico se viola la protección de los derechos de autor de un contenido digital con un contenedor seguro

virtual de relación de derechos de autor y de consumidor.

Efectos ventajosos de la invención

[56] La invención aporta a la distribución electrónica de contenidos digitales los mismos modelos de distribución del pasado y del presente de la distribución de formatos físicos, y crea un entorno en dónde los usuarios de contenidos digitales distribuidos electrónicamente a través de la invención dispongan de las mismas opciones de compartir/vender/ intercambiar/regalar que cuando adquieren el contenido digital en un formato físico y a los autores de contenidos digitales la protección de sus derechos de propiedad intelectual.

[57] Difusión del conocimiento y de la cultura a través de los medios digitales de manera universal respectando en todo momento los derechos de autor al permitir la cesión temporal/regalo, intercambio y alquiler de contenidos digitales con un contenedor seguro virtual de relación de derechos de autor y de consumidor.

[58] Genera un marco 'win2win' entre autores y consumidores en el contexto de los contenidos digitales con un contenedor seguro virtual de relación de derechos de autor y de consumidor al proporcionar a los consumidores los mismos derechos que cuando adquiere dicho contenido digital a través de un medio físico y protege a la vez todos los derechos de la propiedad intelectual de los autores.

[59] La industria de los medios de contenidos digitales de autor da la oportunidad de expandir y fortalecer los derechos de los consumidores. Permitiendo que los consumidores cuando compran un contenido digital como música, películas, libros electrónicos, etcétera puedan disponer de los mismos derechos de consumidor que cuando lo adquieren en formato físico, dando la posibilidad a los consumidores de crear un álbum 'especial' de contenidos digitales y regalárselo a otra persona dentro de los márgenes de los derechos de consumidor y respetando en todo momento los derechos de autor.

[60] Brinda la oportunidad a un autor novel de disponer de un espacio donde publicar sus expresiones artísticas empaquetados en un contenido digital con un contenedor seguro virtual de relación de derechos de autor y de consumidor, y poder obtener recursos económicos a partir de sus creaciones artísticas.

[61] Motiva la creatividad del autor, al disponer de la garantía que su actividad artística estará protegida contra copias ilegales, ya que el contenido digital se distribuye con un contenedor seguro virtual de relación de derechos de autor y de consumidor.

[62] Promueve a los consumidores a comprar contenidos digitales de autor con un contenedor seguro virtual de relación de derechos de autor y de consumidor ya que se mantienen sus derechos de consumidor de poder venderlo, intercambiarlo o regalarlo una vez que ya no quiera seguir disfrutando del contenido digital de autor.

Descripción breve de las figuras

[63] Para un mejor entendimiento de la invención se puede seguir a través de las referencias indicadas en los dibujos, y en los cuales:

[64] La Figura 1 describe los componentes lógicos del método de generación del contenedor seguro recursivo virtual de acuerdo a la invención.

[65] La Figura 2 describe el diagrama de flujo de la lógica del método de generación de contenedor seguro recursivo virtual de acuerdo a la invención.

[66] La Figura 3 describe los componentes lógicos/físicos de un Sistema de protección y distribución electrónica de contenidos digitales de autor de primera mano, segunda mano, intercambio, alquiler y cesión temporal/regalo de acuerdo a la invención.

[67] La Figura 4 es un diagrama de secuencia de los mensajes y las activaciones de los componentes lógicos de acuerdo a la invención en la distribución de primera mano.

[68] La Figura 5 es un diagrama de secuencia de los mensajes y las activaciones de los componentes lógicos de acuerdo a la invención en la distribución de segunda mano y alquiler.

[69] La Figura 6 es un diagrama de secuencia de los mensajes y las activaciones de los componentes lógicos de acuerdo a la invención en la distribución de intercambio.

[70] La Figura 7 es un diagrama de secuencia de los mensajes y las activaciones de los componentes lógicos de acuerdo a la invención en la distribución de cesión temporal/ regalo, devoluciones de cesión temporal y de alquiler.

[71] La Figura 8 es un diagrama de secuencia de los mensajes y las activaciones de los componentes lógicos de acuerdo a la invención para describir las acciones que se realizan cuando un usuario hace uso de un contenido digital con un contenedor seguro virtual de relación de derechos de autor y de consumidor.

[72] La Figura 9 es un diagrama de secuencia de los mensajes y las activaciones de los componentes lógicos de acuerdo a la invención para describir las acciones que se realizan para la sincronización de los avatares con sus respectivos avatares clones en los dispositivos digitales con/sin acceso a una red pública del usuario.

Modo de realizar la invención

[73] **Actores que Interaccionan con la Invención**

[74] Un actor es algo con comportamiento, como una persona (identificada por un rol), un sistema informatizado u organización que interactúa con la invención.

[75] Los actores principales que interactúan con el Sistema 100 son:

- Un autor 10 que crea un contenido digital 114 y lo publica en el Sistema 100 para su protección y distribución. Normalmente, el autor 10 es quien crea el contenido digital, no obstante, el término 'autor' como se utiliza aquí, es como el propietario del contenido digital.

- El distribuidor 20, es el editor o cualquier medio autorizado a distribuir trabajos digitales de autor.
- El usuario 30, es quien consume un contenido digital que ha sido publicado por un autor 10 o un distribuidor 20. El contenido digital que un usuario adquiere a través de la invención es un Contenido $Digital_{CSR1}$ 115.

[76] **Estructura Interna del Fichero Digital de un Contenido Digital**

[77] Un contenido digital se almacena en un fichero digital, en la estructura interna del fichero digital se puede distinguir la cabecera 114a y los datos 114b del fichero digital.

[78] En la cabecera 114a se almacena los metadatos del fichero digital. Los metadatos (metadata) son campos de texto que van incrustados en casi todos los tipos de ficheros que añaden información adicional como la fecha de creación, resolución, tamaño, fecha de modificación, autor, etcétera por ejemplo, el sistema operativo para cada archivo almacenado se guardan los siguientes metadatos: fecha y hora de creación, fecha y hora de modificación, última vez que fue accedido, etcétera.

[79] Los datos 114b del fichero digital son el conjunto de bits que definen el contenido digital y vienen a continuación de la cabecera 114a.

[80] **Método de Generación Contenedor Seguro Recursivo Virtual**

[81] El método de generación de un contenedor seguro recursivo virtual 200 establece nexos virtuales de relación a un fichero digital 114 mediante la generación de contenedores seguros iterativos tanto al fichero digital 114 como a las claves de cifrado 203, 210. Los cifrados que se pueden ir realizando en cada iteración son mediante técnicas de cifrado simétrico o mediante técnicas de cifrados asimétricos. Cuando se realiza un cifrado en una iteración se puede realizar sobre el resultado obtenido de un cifrado anterior si previamente ya se hizo un cifrado.

[82] El término 'contenedor seguro', tal y como se usa aquí, es para referirse a un contenido digital o clave de cifrado encriptado totalmente o parcialmente, y el término 'recursivo', tal y como se usa aquí, es cuando iterar se usa como un término genérico, como sinónimo de repetición, la recursividad es un ejemplo de iteración.

[83] El método de generación de un contenedor seguro recursivo virtual de la invención tiene como datos de entrada: Un fichero digital 114, las claves externas 203 y el modelo contenedor seguro recursivo 204.

[84] Y como salida del método se obtiene:

- Un fichero digital 115, que podrá tener un conjunto de cifrados simétricos/asimétricos de manera iterativa: en la cabecera del fichero digital y/o en los datos del fichero digital y/o en todo el fichero digital de datos. El orden en que se realizan los cifrados simétricos/asimétricos parcial o totalmente en el fichero digital no es condicionante ni limitante.
- Una huella $digital_{CSR1}$ 207, la huella digital identifica de manera unívoca al

fichero digital 115. La huella digital$_{CSR1}$ 207 se obtiene de aplicar una técnica de resumen criptográfico al fichero digital 115.

- Una lista de claves sin contenedor seguro iterativo 208.
- Una lista de claves con un contenedor seguro iterativo 209.

[85] Las claves externas 203, son un conjunto de claves de cifrado que se pueden usar en un cifrado simétrico/asimétrico en una determinada iteración. Las claves externas 203 se representan por una lista de una estructura de datos compuesta de dos campos, el primer campo representa el identificador de la clave externa y el segundo campo su valor. A modo de ejemplo, las claves externas 203 se modelan con la siguiente lista de la estructura de datos [{Id_KeyExt_A, Valor_A},{Id_KeyExt_B, Valor_B}, ...,{Id_KeyExt_N, Valor_N}].

[86] El modelo contenedor seguro recursivo 204 define la secuencia de cifrados simétricos/asimétricos a realizar. El cifrado se puede realizar en uno de los siguientes objetos de datos: En la cabecera 114a del fichero digital, en los datos 114b del fichero digital, en todo el fichero digital 114 y en una clave de cifrado 203, 210.

[87] El modelo de contenedor seguro recursivo 204 indica para cada iteración definida el objeto de datos, la técnica de cifrado simétrico/asimétrico a realizar en el objeto de datos y la clave de cifrado a utilizar en el cifrado (puede ser una clave externa 203, o ser generada de manera aleatoria 210).

[88] El modelo contenedor seguro recursivo 204 se representa por una lista de una estructura de datos compuesta de dos elementos, el primer elemento define la técnica del cifrado simétrico/asimétrico y el objeto de datos en el que realizar el cifrado:

- Para indicar que se realice con técnicas de cifrado simétrico un cifrado en la cabecera del fichero digital se usa el token FILE$_{CSR_HEAD}$, si es para los datos del fichero digital se usa token FILE$_{CSR_DATA}$ y si es para todo el fichero digital se usa el token FILE$_{CSR_FULL}$.
- Para indicar que se realice con técnicas de cifrado asimétrico un cifrado en la cabecera del fichero digital, se usa el token FILE$_{CASR_HEAD}$, si es para los datos del fichero digital se usa token FILE$_{CASR_DATA}$ y si es para todo el fichero digital se usa el token FILE$_{CASR_FULL}$.
- Para indicar que se realice con técnicas de cifrado simétrico un cifrado en una clave de cifrado se usa el token TEXT$_{CSR}$.
- Para indicar que se realice con técnicas de cifrado asimétrico un cifrado en una clave de cifrado se usa el token TEXT$_{CASR}$.

[89] El segundo elemento indica la clave de cifrado a utilizar para generar el contenedor seguro en la iteración, esta clave de cifrado puede ser externa o bien ser generada de manera aleatoria. Para una clave de cifrado externa se indica el identificador de la clave de cifrado de la clave externa 203.

[90] Mientras que, para una clave de cifrado generada de manera aleatoria 210:

- Si es una clave de cifrado simétrico se usa el token newKeyInternal y se indica un identificador único para identificarla {Identificador clave}.
- Si es una clave de cifrado asimétrico se usa el token $newKeyInternal_{PUB}$ o bien el token $newKeyInternal_{PRI}$. Además, se indican los identificadores únicos para identificar la clave pública y clave privada {Identificador clave pública, Identificador clave privada}. Si se usa el token $newKeyInternal_{PUB}$ el cifrado asimétrico se realiza con la clave pública, mientras que si se indica el token $newKeyInternal_{PRI}$ el cifrado asimétrico se realiza con la clave privada.

[91] El número de iteraciones a realizar viene determinado por el modelo de contenedor seguro recursivo 204, y podrá tener de 2 a N iteraciones (siendo N un número entero) según el grado de nexos virtuales de relación a establecer.

[92] A modo de ejemplo, un modelo contenedor seguro recursivo 204 que cree los siguientes nexos virtuales de relación:

- Generar un contenedor seguro iterativo de dos iteraciones para los datos del fichero digital, la primera iteración con cifrado asimétrico con la clave externa KeyExt_A y la segunda iteración con cifrado simétrico con una clave generada internamente con identificador KeyInternal_A2.
- Generar un contenedor seguro iterativo de dos iteraciones para la clave externa KeyExt_A, la primera iteración con cifrado asimétrico con la clave externa KeyExt_B y la segunda iteración con un cifrado simétrico con la clave generada internamente con identificador KeyInternal_A4.
- Generar un contenedor seguro iterativo de tres iteraciones para la clave interna KeyInternal_A2, la primera iteración con cifrado simétrico con la clave externa KeyExt_C, la segunda iteración con cifrado simétrico con una clave generada internamente (KeyInternal_A6) y la tercera iteración con cifrado asimétrico con la clave externa KeyExt_B.

[93] Por lo tanto, según el ejemplo anterior, los datos de entrada son:

- Fichero digital 114.
- Claves Externas 203, con una estructura de datos [{KeyExt_A, Valor_A},{KeyExt_B, Valor_B},{KeyExt_C, Valor_C}].
- Modelo del contenedor seguro recursivo 204, con una estructura de datos: [{Iteración 1: $FILE_{CASR\_DATA}$ * [KeyExt_A]},{Iteración 2: $FILE_{CSR\_DATA}$ * [newKeyInternal{KeyInternal_A2}]},{Iteración 3: $TEXT_{CASR}$(KeyExt_A) * [KeyExt_B]},{Iteración 4: $TEXT_{CSR}$(KeyExt_A) * [newKeyInternal{KeyInternal_A4}]},{Iteración 5: $TEXT_{CSR}$(KeyInternal_A2) * [KeyExt_C]},{Iteración 6: $TEXT_{CSR}$(KeyInternal_A2) * [newKeyInternal{KeyInternal_A6}]},{Iteración 7: $TEXT_{CASR}$

(KeyInternal_A2) * [KeyExt_B] }].

[94] En la Figura 1, se describen los componentes lógicos del método de generación de contenedor seguro recursivo virtual. El componente lógico principal es el Controlador Lógico Generador Contenedor Seguro Recursivo Virtual 202, este componente lógico a partir de los datos de entrada ejecuta la lógica descrita en la Figura 2, para crear nexos virtuales de relación según el modelo de contenedor seguro recursivo indicado como dato de entrada.

[95] La primera fase del método consiste en el Analizador Datos de Entrada 202b que valida que son correctos los datos de entrada. Los datos de entrada obligatorios son el contenido digital 114 y el modelo contenedor seguro recursivo 204, mientras que las claves externas 203 es opcional, y solo es necesario si el modelo contenedor seguro recursivo 204 se definen referencias a claves de cifrado externas.

[96] El Analizador de los Datos de Entrada 202b realiza las siguientes validaciones y comprobaciones:

- El fichero digital 114 es correcto y el formato del archivo es válido.
- Las claves externas 203 y el modelo contenedor seguro recursivo 204 son correctos tanto a nivel sintáctico como semánticamente.
- Integridad referencial de las claves indicadas en el modelo contenedor seguro recursivo 204. Todas las claves externas indicadas en el modelo contenedor seguro recursivo deben tener su correspondiente referencia y un valor en el dato de entrada claves externas 203. Además valida que todos los contenedores seguros iterativos a realizar sobre una clave generada aleatoriamente indicada en el modelo de contenedor seguro recursivo 204 se genera en una iteración previa.

[97] En el caso que exista cualquier error en los datos de entrada o no se pueda resolver la referencia a una clave externa indicada en el modelo de contenedor seguro recursivo se termina con error indicando la causa que ha provocado la finalización del método.

[98] Los objetos de datos, es un conjunto de bits con entidad propia que gestiona/ procesa/transforma el método de generación de contenedor seguro recursivo virtual. Los objetos de datos son: todo el fichero digital 114, o parcialmente el fichero digital (cabecera 114a, datos 114b) y las claves de cifrado (tanto las claves externas 203, como las claves generadas aleatoriamente 210).

[99] La siguiente fase del método es el componente lógico Controlador de Objetos de Datos 202c que realiza las siguientes funcionalidades:

- Crear la Estructura de Objetos de Datos 202a inicial, analiza el modelo contenedor seguro recursivo 204 y asigna a cada objeto de datos un identificador único.
- Define a nivel lógico las acciones a realizar en cada iteración a partir de lo

definido en el modelo contenedor seguro recursivo 204.

- Determina y prepara los objetos de datos a procesar en la iteración en curso. Para decidir los objetos de datos necesarios, analiza la iteración en el modelo contenedor seguro recursivo 204. Para preparar el objeto de datos lo busca de la Estructura de Objetos de Datos 202a de la iteración anterior.

[100] La Estructura de Objetos de Datos 202a es una estructura de datos dinámica que mantiene la evolución de transformación de cada objeto de datos en cada iteración. A los objetos de datos se le van aplicando de manera iterativa cifrados simétricos/asimétricos con la clave de cifrado que indica la iteración. Además, esta estructura de datos se utiliza para recuperar la transformación del objeto de datos de la iteración anterior cuando en la iteración en curso se indica realizar un cifrado simétrico/ asimétrico en el objeto de datos.

[101] La siguiente fase del método es determinar la clave de cifrado a utilizar en la iteración en curso para realizar el cifrado simétrico/asimétrico 202d:

- Si la clave se genera de manera aleatoria, se solicita al componente lógico Generador Clave Simétrica/Asimétrica 201 una clave de cifrado 210 (simétrica o asimétrica según la técnica de cifrado que se vaya a realizar).
- Si la clave de cifrado es externa, se obtiene el valor de la clave de cifrado indicada en las claves externas 203 a partir del identificador de la clave de cifrado externa que indica el modelo contenedor seguro recursivo 204.

[102] La siguiente fase del método es determinar en qué objeto de datos se debe aplicar la técnica de cifrado indicada en la iteración en curso con la clave de cifrado determinada en la fase anterior:

- Si es el token $FILE_{CSR\_HEAD}$ 202e se le indica al componente lógico Cifrado Simétrico Contenido 205a que realice con técnicas de cifrado simétrico un cifrado en la cabecera 114a del fichero digital.
- Si es el token $FILE_{CSR\_DATA}$ 202f se le indica al componente lógico Cifrado Simétrico Contenido 205b que realice con técnicas de cifrado simétrico un cifrado en los datos 114b del fichero digital.
- Si es el token $FILE_{CSR\_FULL}$ 202g se le indica al componente lógico Cifrado Simétrico Contenido 205c que realice con técnicas de cifrado simétrico un cifrado en todo el fichero digital 114.
- Si es el token $TEXT_{CSR}$ 202h se le indica al componente lógico Cifrado Simétrico Texto 206a que realice con técnicas de cifrado simétrico un cifrado en una clave de cifrado.
- Si es el token $FILE_{CASR\_HEAD}$ 202i se le indica al componente lógico Cifrado Asimétrico Contenido 205d que realice con técnicas de cifrado asimétrico un cifrado sobre la cabecera 114a del fichero digital.

- Si es el token $FILE_{CASR\_DATA}$ 202j se le indica al componente lógico Cifrado Asimétrico Contenido 205e que realice con técnicas de cifrado asimétrico un cifrado en los datos 114b del fichero digital.
- Si es el token $FILE_{CASR\_FULL}$ 202k se le indica al componente lógico Cifrado Asimétrico Contenido 205f que realice con técnicas de cifrado asimétrico un cifrado en todo el fichero digital 114.
- Si es el token $TEXT_{CASR}$ 202m se le indica al componente lógico Cifrado Asimétrico Texto 206b que realice con técnicas de cifrado asimétrico un cifrado en una clave de cifrado.

[103] Una vez que se ha realizado el cifrado con técnicas de cifrado simétrico o asimétrico sobre un objeto de datos, se ejecuta Actualizar Objetos de Datos 202n, en este punto se actualiza la Estructura de Objetos de Datos 202a de la iteración en curso con el estado de transformación de todos los objetos de datos. En el caso que haya sido necesario crear una clave simétrica, se añade una nueva entrada en la Estructura de Objeto de Datos 202a, o dos entradas en el caso de una clave asimétrica (pública/privada).

[104] La siguiente fase es determinar si ha finalizado 202o de procesar el modelo contenedor seguro recursivo 204, si ha finalizado se genera la huella digital con el Generador Resumen Criptográfico 211. Si debe realizar otra iteración, vuelve al Controlador Objeto de Datos 202c para comenzar con la siguiente iteración indicada en el modelo contenedor seguro recursivo 204.

[105] **El Modelo de Contenedor Seguro Recursivo Preferido para la Invención**

[106] El modelo de contenedor seguro recursivo 204 preferido para la invención se define de la manera más sencilla que permite todos los modelos de distribución de la invención y es el que se usa para describir los casos de usos más representativos de la invención, pudiendo usarse otros modelos de contenedor seguro recursivo y se adaptarían los casos de usos al nuevo modelo de contenedor seguro recursivo. El modelo de contenedor seguro recursivo preferido para la invención:

- Iteración 1: $FILE_{CSR\_DATA}$ * [newKeyInternal{KeyInternal_A1}] (nota: La clave KeyInternal_A1, se utiliza aquí, como key_{INT} 210a).
- Iteración 2: $TEXT_{CSR}$(KeyInternal_A1) * [newKeyInternal{KeyInternal_A2}] (nota: La clave KeyInternal_A2, se utiliza aquí, como key_{AU} 208a).
- Iteración 3: $TEXT_{CSR}$(KeyInternal_A1) * [newKeyInternal{KeyInternal_A3}] (nota: La clave KeyInternal_A3, se utiliza aquí, como key_{AM} 208b).

[107] El modelo de contenedor seguro recursivo de realización preferido, genera un contenedor seguro iterativo de una iteración sobre los datos 114b del fichero digital con la clave simétrica de cifrado key_{INT} 210a, y en key_{INT} 210a genera un contenedor seguro iterativo de dos iteraciones con las claves key_{AU} 208a y key_{AM} 208b.

[108] De acuerdo al modelo de contenedor seguro recursivo preferido, a la salida tras

aplicar el método de generación de contenedor seguro recursivo virtual:

- Contenido $Digital_{CSR1}$ 115, este término se usa aquí, para identificar al fichero digital 114 con un contenedor seguro iterativo de una iteración en sus datos 114b con la clave simétrica de cifrado key_{INT} 210a generada aleatoriamente.
- Huella $Digital_{CSR1}$ 207, este término se usa aquí, para identificar la huella digital del Contenido $Digital_{CSR1}$ 115.
- key_{CSR2} 209a, este término se usa aquí, para identificar la clave key_{INT} 210a con un contenedor seguro iterativo de dos iteraciones.
- key_{AU} 208a, este término se usa aquí, para identificar la clave simétrica de cifrado generada aleatoriamente utilizada para generar el contenedor seguro iterativo en la primera iteración de la clave key_{INT} 210a, obteniéndose como resultado la clave key_{CSR1}.
- key_{AM} 208b, este término se usa aquí, para identificar la clave simétrica de cifrado generada aleatoriamente usada para generar el contenedor seguro iterativo en la segunda iteración de la clave key_{INT} 210a, obteniéndose como resultado la clave key_{CSR2} 209a.

[109] **Método descifrado del Contenedor Seguro Recursivo Virtual**

[110] El método de descifrado del contenedor seguro recursivo virtual consiste en aplicar descifrados simétricos/asimétricos de manera inversa a como se han realizado los cifrados simétricos/asimétricos aplicados para ir generando los contenedores seguros iterativos, es decir, ir procesando el modelo de contenedor seguro recursivo 204 de manera inversa (desde el final al inicio) realizando un descifrado simétrico o asimétrico según aplique (en el caso de cifrado asimétrico, si se cifró con la clave pública se usa la clave privada, y si se cifró con la clave privada se utiliza la clave pública).

[111] A modo de ejemplo, para descifrar los datos 114b del Contenido $Digital_{CSR1}$ 115 y obtener los datos 114b del contenido digital 114 de acuerdo al modelo de contenedor seguro recursivo 204 preferido, se hacen los siguientes pasos:

- Primero, descifrar simétricamente key_{CSR2} 209a, con la clave key_{AM} 208b (se obtiene el objeto de datos temporal key_{CSR1}).
- Segundo, descifrar simétricamente key_{CSR1} con la clave key_{AU} 208a (se obtiene el objeto de datos key_{INT} 210a).
- Tercero, descifrar simétricamente los datos 114b del Contenido $Digital_{CSR1}$ 115 con la clave key_{INT} 210a.

[112] **Contenedor Seguro Virtual de Relación de Derechos: de Autor y de Consumidor**

[113] La palabra 'virtual' se suele usar para referirse a algo que existe sólo aparentemente y no es real físicamente. Para establecer una relación de derechos de autor y de usuario debe existir al menos un nexo virtual de asociación en el Contenido $Digital_{CSR1}$ 115.

[114] Los nexos virtuales de asociación se crean con el método de generación de contenedor seguro recursivo virtual, cada nuevo cifrado iterativo que se realiza establece un nuevo nexo virtual de asociación. Los nexos virtuales de relación se pueden establecer sobre cualquier objeto de dato que maneja el método de generación de contenedor seguro recursivo virtual.

[115] Los componentes lógicos de la invención Avatar Master 111 y el Avatar Usuario 112 crean el marco virtual de relación de derechos de autor y de consumidor, donde el avatar master custodia que no se infringen los derechos de autor y el avatar usuario mantiene los derechos del consumidor cuando compra un contenido digital. El avatar master almacena de manera segura la clave key_{AM} 208b y el avatar usuario guarda de forma segura la clave key_{AU} 208a. Al disponer cada avatar de al menos de una de las $Claves_{CSRI}$ 208, 209 para poder descifrar los datos del $Contenido\ Digital_{CSRI}$ 115 se establece el nexo virtual de relación de derechos de autor y de consumidor.

[116] El término 'avatar', se usa aquí, para indicar la representación virtual de una entidad en donde se traslada el rol de la entidad al avatar. Cuando la relación de derechos se crea entre del autor y del consumidor, el rol de autor se traslada al componente lógico de la invención Avatar Master 111 y el rol de consumidor al Avatar Usuario 112.

[117] El término '$Claves_{CSRI}$' se usa aquí, para referir a la lista de claves con un contenedor seguro iterativo 209 y la lista de claves sin contenedor seguro iterativo 208 que se obtienen en la salida del método de generación de contenedor seguro recursivo virtual.

[118] La combinación del método de generación de contenedor seguro recursivo virtual que establecen los nexos virtuales de relación a un fichero digital 114 con las claves de cifrado 203, 210 junto con la distribución de manera única de al menos de una de las $Claves_{CSRI}$ 208, 209 relacionadas con la $Huella\ Digital_{CSRI}$ 207 del Contenido Digital $_{CSRI}$ 115 a cada uno de los avatares forma el contenedor seguro virtual de relación de derechos.

[119] **Contenedor Seguro Virtual de Relación de Derechos: de Autor, de Consumidor y otras Entidades**

[120] Un contendor seguro virtual de relación de derechos no está limitado exclusivamente a un autor 10 y a un consumidor 30, sino que puede extenderse con más nexos virtuales de relación que representen los derechos de otras entidades, por ejemplo, un distribuidor, un órgano regulador, etcétera.

[121] Para establecer nuevos nexos virtuales de relación se incrementa el número de iteraciones de cifrado simétrico/asimétrico en el método de contenedor seguro recursivo virtual y se distribuye de manera única de al menos una de las $Claves_{CSRI}$ 208, 209 asociada con la $Huella\ Digital_{CSRI}$ 207 del $Contenido\ Digital_{CSRI}$ 115 a un nuevo avatar que representa a la nueva entidad. Además, en el avatar máster se redefine la lógica para consultar a los nuevos avatares y obtener la clave de cifrado que custodia cada

avatar de otra entidad.

[122] **Avatar con varios Roles**

[123] Un avatar puede implementar internamente varios roles y representar a la vez a varias entidades. Cuando una avatar disponga de un conjunto de roles, recibirá por cada rol implementado de manera única de al menos una de las claves de cifrado del nexo virtual de relación de derechos ($Claves_{CSR1}$ 208, 209). El avatar con varios roles escucha por varios puertos de comunicaciones y cada puerto está asociado a un rol.

[124] **Arquitectura Lógica y Física de la Invención**

[125] La arquitectura lógica tiene como objetivo determinar el diseño de más alto nivel de la invención, y define de manera abstracta los componentes lógicos principales que llevan a cabo alguna tarea de computación, sus interfaces y la comunicación entre ellos. Toda arquitectura debe ser impleméntable en una arquitectura física, que consiste en determinar en qué hardware/dispositivo digital tendrá asignada cada funcionalidad.

[126] En la Figura 3, se muestra la arquitectura lógica y física de la invención. Los componentes lógicos de la invención son los siguientes:

[127] El Sistema 100, componente lógico que realiza la transformación de un contenido digital 114 a un Contenido $Digital_{CSR1}$ 115 con un contenedor seguro virtual de relación de derechos de autor y de consumidor, permite las diferentes modalidades de distribución y genera todo el marco funcional de gestión en el lado del servidor.

[128] El Avatar Master 111, es el componente lógico que custodia que no se infringen los derechos de autor. Almacena de modo seguro la asociación entre la $Huella\ Digital_{CSR1}$ 207 de un Contenido $Digital_{CSR1}$ 115, la clave key_{CSR2} 209a que es la transformación de key_{INT} 210a con un contenedor seguro iterativo de dos iteraciones y la clave key_{AM} 208b usada para generar el contenedor seguro iterativo de key_{INT} 210a en la segunda iteración, y físicamente se ejecuta en un Dispositivo Digital de Usuario con Acceso a Redes Públicas 110 y/o en el Sistema 100.

[129] El Avatar Usuario 112, es el componente lógico que mantiene los derechos del consumidor cuando compra un contenido digital. Almacena de modo seguro la asociación entre la $Huella\ Digital_{CSR1}$ 207 de un Contenido $Digital_{CSR1}$ 115 y la clave key_{AU} 208a usada para generar el contenedor seguro iterativo de key_{INT} 210a en la primera iteración, y se ejecuta físicamente en un Dispositivo Digital de Usuario con Acceso a Redes Públicas 110 y/o en el Sistema 100.

[130] El Avatar Master Clone 121, es el componente lógico que custodia que no se infringen los derechos de autor. Almacena de modo seguro la asociación entre la $Huella\ Digital_{CSR1}$ 207 de un Contenido $Digital_{CSR1}$ 115 la clave de cifrado key_{CSR2} 209a y la clave de cifrado key_{AM} 208b. Físicamente se ejecuta en un Dispositivo Digital de Usuario sin Acceso a Redes Públicas 120.

[131] El Avatar Usuario Clone 122, es el componente lógico que mantiene los derechos del

consumidor cuando compra un contenido digital. Almacena de modo seguro la asociación entre la Huella $Digital_{CSR1}$ 207 de un Contenido $Digital_{CSR1}$ 115 y la clave de cifrado key_{AU} 208a . Físicamente se ejecuta en un Dispositivo Digital de Usuario sin Acceso a Redes Públicas 120.

[132] El Reproductor Digital 113, es el componente lógico que reproduce/visualiza/ejecuta el Contenido $Digital_{CSR1}$ 115, para llevar dicha tarea dialoga con el Avatar Master 111 para obtener la clave key_{INT} 210a de descifrado de los datos 114b del Contenido Digital $_{CSR1}$ 115, y se podrá ejecutar en un Dispositivo Digital de Usuario con Acceso a Redes Públicas 110 o un Dispositivo Digital de Usuario sin Acceso a Redes Públicas 120.

[133] Además, en la Figura 3, se muestran los componentes físicos en los que algunos componentes lógicos de la invención se ejecutan:

[134] Un conjunto de servidores donde se ejecuta el sistema y de bases de datos 116.

[135] Un Dispositivo Digital de Usuario con Acceso a Redes Públicas 110, es cualquier dispositivo electrónico que tiene la capacidad de conectarse a una red pública 130, por ejemplo, una computadora, un portátil, un teléfono móvil, un iTablet, etcétera y en dicho dispositivo se ejecutarán componentes lógicos de la invención.

[136] Un Dispositivo Digital de Usuario sin Acceso a Redes Públicas 120, es cualquier dispositivo electrónico que no dispone la capacidad de conectarse a una red pública pero si puede conectarse a un Dispositivo Digital de Usuario con Acceso a Redes Públicas 110 para transferir datos entre ellos, por ejemplo, un reproductor de mp3, etcétera y en dicho dispositivo se ejecutarán componentes lógicos de la invención.

[137] **Dispositivo Digitales**

[138] El Dispositivo Digital 110 y 120 es el hardware necesario para que los componentes lógicos de la invención que no se ejecutan en el Sistema 100 puedan reproducir/visualizar/ejecutar el Contenido $Digital_{CSR1}$ 115.

[139] Dispositivo Digital de Usuario con Acceso a Redes Públicas 110 se ejecutaran los siguientes componentes lógicos de la invención: Avatar Master 111, Avatar Usuario 112, Reproductor Digital 113 y está un repositorio de Contenidos $Digitales_{CSR1}$ 115 que un usuario ha adquirido a través del Sistema 100. Además, el Dispositivo Digital de Usuario con Acceso a Redes Públicas 110 puede tener acceso a una red de comunicaciones local 131, la comunicación entre los diferentes dispositivos se puede realizar a través de cualquier canal local, tal como una red de área local (LAN), puertos de comunicaciones serie, USB, bluetooth y análogos. Los canales de comunicaciones pueden utilizar tecnología inalámbrica, tal como radiofrecuencia o tecnología de infrarrojos. Mediante dicho acceso se podrá comunicar con un Dispositivo Digital de Usuario sin Acceso a Redes Públicas 120.

[140] Dispositivo Digital de Usuario sin Acceso a Redes Públicas 120 no dispone la capacidad de conectarse a una red pública pero si puede establecer una comunicación

con un Dispositivo Digital de Usuario con Acceso a Redes Públicas 110 para transferir datos entre ellos a través de una red de comunicaciones local 131. Se ejecutan componentes los lógicos de la invención: Avatar Master Clone 121, Avatar Usuario Clone 122, Reproductor Digital 113 y está un repositorio de Contenidos Digitales$_{CSR1}$ 115 que un usuario ha adquirido a través del Sistema 100.

[141] **Comunicación entre los Componentes Lógicos de la Invención**

[142] La comunicación entre los componentes lógicos se realiza siempre bajo canales seguros usando las técnicas de cifrado asimétrico y de cifrado simétrico. Las técnicas de cifrado asimétrico tienen clave pública y clave privada. El funcionamiento del cifrado asimétrico se basa en el mantenimiento en secreto de las claves privadas y en la certificación de las claves públicas.

[143] El algoritmo de cifrado RSA es reversible, además de permitir cifrar con la clave pública y descifrar con la privada, permite cifrar con la clave privada y descifrar con la pública. Así se puede utilizar tanto para obtener confidencialidad (cifrando con la clave pública del destinatario), como para firmar (cifrando con la clave privada del emisor).

[144] Las claves públicas pueden ser transmitidas por canales inseguros sin que ello represente una debilidad:

- Confidencialidad en comunicaciones con la clave pública del otro componente lógico (Comunicación entre A <-> B, A cifra un mensaje confidencial a B, CifradorAsimétrico(clave_pública_B, Mensaje)).
- Integridad y autenticación de cada componente lógico (clave privada) (Comunicación entre A <-> B, CifradorAsimétrico(clave_privada_A, Mensaje), el mensaje puede ser leído por cualquiera que posee la clave pública de A. El mensaje en claro sólo A pudo realizar ese cifrado, por lo que el mensaje es integro y auténtico).
- Confidencialidad, integridad y autenticación (Comunicación entre A <-> B, CifradorAsimétrico(clave_privada_A, CifradorAsímetrico(clave_pública_B, Mensaje)), el destinatario comprobará la autenticidad del mensaje y posteriormente podrá descifrar el mensaje).

[145] Una vez validada la identidad del componente lógico a través de su firma digital, se estable la comunicación con el otro componente lógico mediante un canal seguro para intercambiar datos.

[146] **Integridad de los Componentes Lógicos de la Invención**

[147] Además de establecer siempre canales seguros de comunicación entre los componentes lógicos, se valida al componente lógico que reside en los dispositivos digitales de usuario 120 que no han sufrido ninguna manipulación mediante la firma digital del componente lógico.

[148] Mediante el uso de técnicas de resumen criptográfico que son algoritmos ma-

temáticos que permite calcular un valor resumen del propio componente lógico a ser firmados digitalmente. Funciona en una sola dirección, es decir, no es posible, a partir del valor resumen, calcular los datos originales.

[149] **Diagramas de Secuencias de las Diferentes Modalidades de Distribución de la Invención**

[150] Los diagramas de secuencia que se describen a continuación muestran la interacción de los componentes lógicos en la invención a través del tiempo. El diagrama de secuencia contiene los actores, componentes lógicos de la invención y exponen la forma en que los componentes lógicos se comunican entre sí (a través de los mensajes intercambiados) al transcurrir el tiempo.

[151] Los diagramas de secuencia incluyen la dimensión temporal. La línea primordial es que las interacciones entre los componentes lógicos se realizan en una secuencia establecida y que la secuencia se toma su tiempo en ir del principio al fin.

[152] Los componentes lógicos/actores están representados en rectángulos con sus nombres, los mensajes están representados por líneas continuas con una punta de flecha, y el tiempo representando por una progresión vertical, que se inicia en la parte superior y avanza hacia la parte inferior. Un mensaje que esté más cerca de la parte superior ocurrirá antes que uno que esté más cerca de la parte inferior.

[153] Junto con la línea de vida de un componente lógico puede haber un rectángulo estrecho que se conoce como activación, el cual indica que el objeto realiza una operación interna o acción.

[154] Los diagramas de secuencia están simplificados con el objetivo de representar los mensajes más identificativos omitiéndose en algunas ocasiones mensajes de respuesta de confirmaciones, y la finalidad primordial es reflejar una de las posibles implementaciones de cada modalidad de distribución que proporciona la invención para un contenido digital protegido con un contenedor seguro virtual de relación de derechos de autor y de consumidor.

[155] **Distribución en Modalidad de 'Primera Mano'**

[156] La distribución de primera mano se realiza cuando un usuario adquiere un contenido digital protegido con un contenedor seguro virtual de relación de derechos de autor y de consumidor en la invención por la publicación del autor o de un medio autorizado.

[157] La Figura 4 describe el diagrama de secuencia de distribución en modalidad de primera mano. Este diagrama de secuencia describe una de las posibles secuencias de mensajes y activaciones de los componentes lógicos de la invención y expone como se resolvería la casuística de uso que se trata en este apartado.

[158] A continuación se describen los mensajes y activaciones de la Figura 4:

1. Mensaje 450: Un Usuario 30, accede al catalogo de Contenido $\text{Digital}_{\text{CSR1}}$ 115 publicados por un autor 10 o de un medio autorizado 20. Envía una solicitud

de compra del Contenido Digital$_{CSR1}$ 115 'X' al Sistema 100.

2. Mensaje 451: El Sistema 100, valida al Usuario 30 a través de su Avatar Usuario 112.
3. Mensaje 452: Avatar Usuario 112 envía un mensaje al Usuario 30 para que se valide y le informa del inicio de la compra del Contenido Digital$_{CSR1}$ 115 'X'.
4. Mensaje 453: Avatar Usuario 112 solicita al Usuario 30 que se autentique, una vez que el usuario se ha validado correctamente.
5. Mensaje 454: Avatar Usuario 112 confirma al Sistema 100 que el Usuario 30 se ha autenticado correctamente y el Avatar Usuario 112 se autentica con el sistema a través de su firma digital.
6. Mensaje 455: El Sistema 100, valida la integridad del Avatar Master 111.
7. Mensaje 456: El Avatar Master 111 se autentica con el Sistema 100 a través de su firma digital.
8. Mensaje 457: El Sistema 100, realiza la reserva de saldo con la plataforma de pagos 130. La plataforma de pago gestiona la cuenta monetaria del usuario, y en el caso que no tenga saldo suficiente dialogará con el usuario para solicitar una recarga de saldo.
9. Mensaje 458: La plataforma de pagos 130, retorna ok al Sistema 100, se autoriza la distribución del Contenido Digital$_{CSR1}$ 115 'X'.
10. Activación 459: El Sistema 100, genera la clave Key$_{INT}$ 210a 'X' y realiza el cifrado simétrico sobre los datos 114b del contenido digital 114 'X' y se genera Contenido Digital$_{CSR1}$ 115 'X'.
11. Activación 460: El Sistema 100, calcula la Huella Digital$_{CSR1}$ 207 'X' del Contenido Digital$_{CSR1}$ 115 'X'.
12. Activación 461: El Sistema 100, genera la clave de cifrado Key$_{AU}$ 208a 'X' y realiza cifrado simétrico a la clave Key$_{INT}$ 210a 'X' (primera iteración) (se obtiene Key$_{CSR1}$).
13. Activación 462: El Sistema 100, genera la clave de cifrado Key$_{AM}$ 208b 'X' y realiza cifrado simétrico a la clave Key$_{INT}$ 210a 'X' (segunda iteración) (se obtiene Key$_{CSR2}$ 209a).
14. Mensaje 463: El Sistema 100, envía al Avatar Master 111, la siguiente tripleta de datos: Huella Digital$_{CSR1}$ 207 'X' / Key$_{CSR2}$ 209a 'X' / Key$_{AM}$ 208b 'X' para que lo almacene de manera segura.
15. Mensaje 464: El Sistema 100, envía al repositorio 115a del Usuario 30 el Contenido Digital$_{CSR1}$ 115 'X' con un contenedor seguro iterativo de una iteración en los datos 114b con la clave de cifrado Key$_{INT}$ 210a 'X'.
16. Mensaje 465: El Sistema 100, envía al Avatar Usuario 112, el par de datos: Huella Digital$_{CSR1}$ 207 'X' / Key$_{AU}$ 208a 'X' y lo almacena de manera segura.

17. Con la distribución de las claves de cifrado Key_{CSR2} 209a 'X' / Key_{AU} 208a 'X' / Key_{AM} 208b 'X' a los avatares, el Sistema 100 distribuye el Contenido Digital 114 'X' al Usuario 30 transformado en Contenido $Digital_{CSR1}$ 115 'X' y protegido en un contenedor seguro virtual de relación de derechos de autor y de consumidor.
18. Mensaje 466: El Sistema 100, consolida el pago con la plataforma de pagos 130.
19. Mensaje 467: El Sistema 100, confirma la compra con éxito del Contenido $Digital_{CSR1}$ 115 'X'.

[159] **Distribución en Modalidad de 'Segunda Mano' / 'Alquiler'**

[160] La distribución de segunda mano se realiza cuando un usuario vende un Contenido $Digital_{CSR1}$ 115 adquirido en la invención a otro usuario a través de la invención. La distribución de alquiler se produce cuando un medio autorizado que cumple el marco legal para poder realizar alquileres de contenidos digitales de autor, alquila un Contenido $Digital_{CSR1}$ 115 a un usuario.

[161] La Figura 5 describe el diagrama de secuencia de distribución modalidad segunda mano / alquiler, y el objetivo de este diagrama de secuencia es detallar una de las posibles secuencias de mensajes y activaciones de los componentes lógicos de la invención para mostrar cómo se resolvería la casuística de uso de la distribución en modalidad de 'Segunda Mano' / 'Alquiler'.

[162] El diagrama de secuencia de alquiler es idéntico al de segunda mano, con la salvedad que actor que inicia el proceso es un medio autorizado para realizar el alquiler de contenidos digitales o bien un usuario que cumple el marco legal para poder realizar el alquiler, y lo que publica es el alquiler de un Contenido $Digital_{CSR1}$115.

[163] Para simplificar el diagrama de secuencia se tiene en cuenta que el usuario sólo ha dado de alta un único Avatar Master y Avatar Usuario. En el caso que el usuario dispusiera de más de un Avatar Master/Usuario, se repetiría los mensajes con cada Avatar Master/Usuario hasta que se borrasen todas las posibles copias y el sistema recibiese la correspondiente confirmación de cada Avatar Master para de esta manera poder comenzar el proceso de Segunda Mano o de Alquiler.

[164] También se ha simplificado el flujo de mensajes que se produciría entre los Avatar Master a los Avatares Clones en los diferentes dispositivos digitales sin acceso a una red pública, reflejándolo en la activación 561.

[165] A continuación se describen los mensajes y activaciones de la Figura 5:

1. Mensaje 550: El Usuario A 30a, adquirió a través del Sistema 100 el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'], y realiza una solicitud de publicar el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] en el mercado de segunda mano a través del Sistema 100.

2. Mensaje 551: El Sistema 100, valida al Usuario A 30a, a través de su Avatar Usuario A 112a.
3. Mensaje 552: Avatar Usuario A 112a le envía un mensaje al Usuario A 30a, para que se valide y le informa que se va a proceder a la venta de segunda mano el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'].
4. Mensaje 553: Avatar Usuario A 112a le solicita al Usuario A 30a que se autentique, una vez que el usuario se ha validado correctamente.
5. Mensaje 554: Avatar Usuario A 112a confirma al Sistema 100 que el usuario se ha autenticado correctamente y el Avatar Usuario A 112a se autentica con el Sistema 100 a través de su firma digital.
6. Mensaje 555: El Sistema 100, valida la integridad del Avatar Master A 111a, y le solicita toda la información de copias en Avatar Master Clone 121 realizadas para el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] y que no han sido borradas.
7. Activación 556: El Avatar Master A 111a obtiene el número de copias distribuidas en los diferentes Avatar Master Clone 121 del Usuario A 30a.
8. Mensaje 557: El Avatar Master A 111a se autentica con el Sistema 100 con su firma digital, y le informa del número de copias realizadas en Avatar Master Clone 121 y que aún no han sido eliminadas.
9. Mensaje 558: El Sistema 100, notifica al Usuario A 30a la puesta en venta del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'], informa del número de copias que tiene distribuidas en sus correspondientes Avatar Master Clone 121, solicita la confirmación del borrado por parte del Usuario A 30a.
10. Mensaje 559: El Usuario A 30a, acepta la publicación y que se proceda al borrado de todas las copias en los respectivos Avatar Master Clone 121.
11. Mensaje 560: El Sistema 100, notifica al Avatar Master A 111a que se proceda al borrado de todas las copias del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'].
12. Activación 561: El Avatar Master A 111a, comienza a realizar la operación de borrado solicitando al Usuario A 30a que conecte todos los dispositivos sin acceso a redes públicas para proceder con la sincronización con el Avatar Master Clone 121 y Avatar Usuario Clone 122 que están ejecutándose en dicho dispositivo. Valida previamente a todos los componentes lógicos con sus respectivas firmas digitales. Este proceso estará activo hasta que estén sincronizados todos los dispositivos digitales en los que el Avatar Master A 111a tiene registrada una sincronización del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'].
13. Mensaje 562: El Avatar Master A 111a ya se ha sincronizado con todos los

Avatar Master Clone 121 y Avatar Usuario Clone 122, y se han borrado todas las referencias del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'], procede al borrado de la referencias en el Avatar Usuario A 112a y la que tiene el mismo.

14. Mensaje 563: El Avatar Master A 111a borra el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] del repositorio de contenidos 115a del Usuario A 30a.
15. Mensaje 564: El Avatar Master A 111a, envía al Sistema 100, vía callback una notificación de que se han borrado todas las copias del Contenido Digital $_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] y que ya se puede publicar dicho contenido en la sección de segunda mano. Al recibir este mensaje el Sistema 100, se aseguran todos los derechos de autor, ya que se han borrado todas las claves del contenido digital que se desea vender en segunda mano.
16. Activación 565: El Sistema 100, publica en Segunda Mano, el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'], y queda registrado quién es el usuario que lo publica, junto con sus claves de cifrado asociadas Key_{CSR2} 209a 'X' / Key_{AM} 208b 'X' / Key_{AU} 208a 'X'.
17. Mensaje 566: El Sistema 100, notifica al Usuario A 30a la publicación del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] en segunda mano. (esta notificación puede ser vía mail, etc.).
18. Mensaje 567: Un Usuario B 30b, que está accediendo al catalogo de contenidos digitales publicados de segunda mano, decide comprar Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X']. Envía la solicitud de compra del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] al Sistema 100.
19. Mensaje 568: El Sistema 100, valida al Usuario B 30b a través de su Avatar Usuario B 112b.
20. Mensaje 569: Avatar Usuario B 112b le envía un mensaje al Usuario B 30b para que se valide y le informa que se va a proceder a la compra de segunda mano Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'].
21. Mensaje 570: Avatar Usuario B 112b le solicita al Usuario B 30b que se autentique, una vez que el usuario se ha validado correctamente.
22. Mensaje 571: Avatar Usuario B 112b confirma al Sistema 100 que el Usuario B 30b se ha autenticado correctamente y el Avatar Usuario B 112b se autentica con el sistema a través de su firma digital.
23. Mensaje 572: El Sistema 100, valida la integridad del Avatar Master B 111b.
24. Mensaje 573: El Avatar Master B 111b se autentica con el Sistema 100 a través de su firma digital.
25. Activación 574: El Sistema 100, comienza el inicio de la venta Segunda Mano

del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] desde Usuario A 30a al Usuario B 30b.

26. Mensaje 575: El Sistema 100, realiza la reserva de saldo con la plataforma de pagos 130. La plataforma de pago gestiona la cuenta monetaria del Usuario B 30b, y en el caso que no tenga saldo suficiente dialogará con el Usuario B 30b para solicitar un recarga de saldo.
27. Activación 576: La plataforma de pagos 130, realiza la reserva de saldo del Usuario B 30b.
28. Mensaje 577: La plataforma de pagos 130, retorna ok al Sistema 100, para que de esta manera se proceda la distribución del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] con un contenedor seguro virtual de relación de derechos de autor y de consumidor, y se distribuya las claves de cifrado usadas para generar la relación de derechos.
29. Mensaje 578: El Sistema 100, envía al Avatar Master B 111b, la siguiente tripleta de datos: Huella Digital$_{CSR1}$ 207 'X' / Key$_{CSR2}$ 209a 'X' / Key$_{AM}$ 208b 'X' para que lo almacene de manera segura.
30. Mensaje 579: El Sistema 100, envía al repositorio del Usuario B 30b de contenidos 115ba el Contenido Digital$_{CSR1}$ 115 'X' con un contenedor seguro iterativo de una iteración con clave Key$_{INT}$ 210a 'X'.
31. Mensaje 580: El Sistema 100, envía al Avatar Usuario B 112b, el par de datos: Huella Digital$_{CSR1}$ 207 'X' / Key$_{AU}$ 208a 'X' para que lo almacene de manera segura.
32. La distribución de las claves de cifrado Key$_{CSR2}$ 209a 'X' / Key$_{AU}$ 208a 'X' / Key$_{AM}$ 208b 'X' a los avatares del Usuario B 30b, Avatar Master B 111b y Avatar Usuario B 112b, el Sistema 100 distribuye el Contenido Digital 114 'X' al Usuario B 30b transformado en Contenido Digital$_{CSR1}$ 115 'X' y protegido en un contenedor seguro virtual de relación de derechos de autor y de consumidor.
33. Mensaje 581: El Sistema 100, consolida el pago con la plataforma de pagos 130 para el Usuario B 30b.
34. Mensaje 582: El Sistema 100, consolida el abono con la plataforma de pagos 130 para el Usuario A 30a.
35. Mensaje 583: El Sistema 100, confirma la compra con éxito del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] al Usuario B 30b.
36. Mensaje 584: El Sistema 100, confirma la venta en segunda mano con éxito del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] al Usuario A 30a.

[166] **Distribución en Modalidad de 'Intercambio'**

[167] La distribución de intercambio se produce cuando dos usuarios se intercambian un Contenido $Digital_{CSR1}$ 115, en esta modalidad ambos usuarios transfieren y reciben un Contenido $Digital_{CSR1}$ 115 del uno al otro y viceversa.

[168] Para simplificar el diagrama de secuencia se ha tenido en cuenta que cada usuario sólo dispone de alta un único Avatar Master y Avatar Usuario. En el caso que el usuario dispusiera de más de un Avatar Master/Usuario, se repetiría los mensajes con cada Avatar Master/Usuario hasta que se borrasen todas las posibles copias y el sistema recibiese la correspondiente confirmación de cada Avatar Master para de esta manera poder comenzar el proceso intercambio de Contenidos $Digitales_{CSR1}$ 115.

[169] También se ha simplificado todo el flujo de mensajes que se produciría entre los Avatar Master a los avatares clones en los diferentes dispositivos digitales sin acceso a una red pública, reflejándolo en las activaciones 668 y 680.

[170] La Figura 6 describe el diagrama de secuencia de distribución de intercambio, y el objetivo de este diagrama de secuencia es mostrar una de las posibles secuencias de mensajes y activaciones de los componentes lógicos de la invención para exponer como se resolvería la casuística de uso que se trata en este apartado.

[171] A continuación se describen los mensajes y activaciones de la Figura 6:

1. Mensaje 650: El Usuario A 30a, adquirió a través del Sistema 100 el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'], y realiza una solicitud de publicar el Contenido $Digital_{CSR1}$ 115 'X' [Huella $Digital_{CSR1}$ 207 'X'] para el intercambio con el Contenido $Digital_{CSR1}$ 115 'Y'[Huella $Digital_{CSR1}$ 207 'Y'] del Usuario B 30b.
2. Mensaje 651: El Sistema 100, valida al Usuario A 30a, a través de su Avatar Usuario A 112a.
3. Mensaje 652: Avatar Usuario A 112a le envía un mensaje al Usuario A 30a, para que se valide y le informa que se va a proceder el intercambio del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] por el Contenido $Digital_{CSR1}$ 115 'Y'[Huella $Digital_{CSR1}$ 207 'Y'] del Usuario B 30b.
4. Mensaje 653: Avatar Usuario A 112a le solicita al Usuario A 30a que se autentique, y Usuario A 30a se valida.
5. Mensaje 654: Avatar Usuario A 112a confirma al Sistema 100 que el usuario se ha autenticado correctamente y el Avatar Usuario A 112a se autentica con el sistema a través de su firma digital.
6. Activación 655: El Sistema 100, registra la solicitud del Usuario A 30a de intercambio del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] por el Contenido $Digital_{CSR1}$ 115 'Y'[Huella $Digital_{CSR1}$ 207 'Y'] del Usuario B 30b.
7. Mensaje 656: El Usuario B 30b, que adquirió a través del Sistema 100 el Contenido $Digital_{CSR1}$ 115 'Y'[Huella $Digital_{CSR1}$ 207 'Y'], y realiza una

solicitud de publicar el Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'] para el intercambio con el Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] del Usuario A 30a.

8. Mensaje 657: El Sistema 100, valida al Usuario B 30b, a través de su Avatar Usuario B 112b.
9. Mensaje 658: Avatar Usuario B 112b le envía un mensaje al Usuario B 30b, para que se valide y le informa que se va a proceder el intercambio del Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'] por el Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] del Usuario A 30a.
10. Mensaje 659: Avatar Usuario B 112b le solicita al Usuario B 30b que se autentique, el Usuario B 30b se valida correctamente.
11. Mensaje 660: Avatar Usuario B 112b confirma al Sistema 100 que el Usuario B 30b se ha autenticado correctamente y el Avatar Usuario B 112b se autentica con el sistema a través de su firma digital.
12. Activación 661: El Sistema 100, como ya dispone de la confirmación del intercambio desde el Usuario A 30a y del Usuario B 30b. Comienza la fase previa para poder realizar el intercambio del Usuario A 30a del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] por el Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'] del Usuario B 30b y viceversa.
13. Mensaje 662: El Sistema 100, valida la integridad del Avatar Master A 111a, solicita las copias realizadas en Avatar Master Clone 121 para el Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] y que no están borradas.
14. Activación 663: El Avatar Master A 111a obtiene el número de copias distribuidas en los diferentes Avatar Master Clone 121 del Usuario A 30a.
15. Mensaje 664: El Avatar Master A 111a se autentica con el Sistema 100 a través de su firma digital, y le informa del número de copias realizadas en Avatar Master Clone 121 y que aún no han sido eliminadas.
16. Mensaje 665: El Sistema 100, notifica al Usuario A 30a que se va a intercambiar el Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] por el Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'] del Usuario B 30b, y le informa del número de copias que tiene del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] en sus correspondientes Avatar Master Clone 121, y solicita la confirmación del borrado por parte del Usuario A 30a.
17. Mensaje 666: El Usuario A 30a, acepta el intercambio y que se proceda al borrado de las copias en los Avatar Master Clone 121 del usuario A 30a.
18. Mensaje 667: El Sistema 100, notifica al Avatar Master A 111a que se proceda al borrado de todas las copias del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'].

19. Activación 668: El Avatar Master A 111a, comienza a realizar la operación de borrado solicitando al Usuario A 30a que conecte todos los dispositivos sin acceso a redes públicas para proceder con la sincronización con el Avatar Master Clone 121 y Avatar Usuario Clone 122 que están ejecutándose en dicho dispositivo. Valida previamente a todos los componentes lógicos con sus respectivas firmas digitales. Este proceso estará activo hasta que estén sincronizados todos los dispositivos digitales en los que el Avatar Master A 111a tiene registrada una sincronización del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'].
20. Mensaje 669: El Avatar Master A 111a sincronizado con todos los Avatar Master Clone y Avatar Usuario Clone del Usuario A 30a, y borradas todas las referencias del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'], elimina la referencia en el Avatar Usuario A 112a y la suya propia.
21. Mensaje 670: El Avatar Master A 111a borra el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] del Repositorio de Contenidos A 115a del Usuario A 30a.
22. Mensaje 671: El Avatar Master A 111a, envía al Sistema 100, vía callback una notificación de eliminación de las copias del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] y el Usuario A 30a está listo para realizar el intercambio.
23. Activación 672: El Sistema 100, registra que el Usuario A 30a ya cumple las condiciones para realizar el intercambio del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] por el Contenido $Digital_{CSR1}$ 115 'Y'[Huella $Digital_{CSR1}$ 207 'Y'] del Usuario B 30b.
24. Mensaje 673: El Sistema 100, notifica al Usuario A 30a, que cumple las condiciones del intercambio. Se está a la espera para que el Usuario B 30b cumpla también las condiciones para poder realizar el intercambio.
25. Mensaje 674: El Sistema 100, valida la integridad del Avatar Master B 111b, y le solicita toda la información a realización de copias en Avatar Master Clone 121 realizadas para el Contenido $Digital_{CSR1}$ 115 'Y'[Huella $Digital_{CSR1}$ 207 'Y'] y que no han sido borradas.
26. Activación 675: El Avatar Master B 111b obtiene el número de copias distribuidas en los diferentes Avatar Master Clone 121 del Usuario B 30b.
27. Mensaje 676: El Avatar Master B 111b se autentica con el Sistema 100 a través de su firma digital, y le informa del número de copias realizadas en Avatar Master Clone 121 y que aún no han sido eliminadas.
28. Mensaje 677: El Sistema 100, notifica al Usuario B 30b que se va a intercambiar el Contenido $Digital_{CSR1}$ 115 'Y'[Huella $Digital_{CSR1}$ 207 'Y'] por el

Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] del Usuario A 30a, y le informa del número de copias que tiene del Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'] en sus correspondientes Avatar Master Clone 121, y solicita la confirmación del borrado por parte del Usuario B 30b.

29. Mensaje 678: El Usuario B 30b, acepta el intercambio y que se proceda al borrado de todas las copias en los respectivos Avatar Master Clone 121 del Usuario B 30b.

30. Mensaje 679: El Sistema 100, notifica al Avatar Master B 111b que se proceda al borrado de todas las copias del Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'].

31. Activación 680: El Avatar Master B 111b, comienza a realizar la operación de borrado solicitando al Usuario B 30b que conecte todos los dispositivos sin acceso a redes públicas para proceder con la sincronización con el Avatar Master Clone 121 y Avatar Usuario Clone 122 que están ejecutándose en dicho dispositivo. Valida previamente que todos los componentes lógicos con sus respectivas firmas digitales. Este proceso estará activo hasta que estén sincronizados todos los dispositivos digitales en los que el Avatar Master B 111b tiene registrada una sincronización del Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'].

32. Mensaje 681: El Avatar Master B 111b, sincronizado con todos los Avatar Master Clone y Avatar Usuario Clone del Usuario B 30b, y borradas todas las referencias del Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'], se eliminan la referencia en el Avatar Usuario B 112b y la suya propia.

33. Mensaje 682: El Avatar Master B 111b borra el Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'] del Repositorio de Contenidos B 115ba del Usuario B 30b.

34. Mensaje 683: El Avatar Master B 111b, envía al Sistema 100, vía callback una notificación de que se han borrado todas las copias del Contenido Digital $_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'] y que el Usuario B 30b está listo para realizar el intercambio.

35. Activación 684: El Sistema 100, registra que el Usuario B 30b ya cumple las condiciones para realizar el intercambio del Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'] por el Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] del Usuario A 30a.

36. Mensaje 685: El Sistema 100, notifica al Usuario B 30b, que ya cumple todas las condiciones para realizar el intercambio, y que el Usuario A 30a también las condiciones previas para poder realizar el intercambio.

37. Activación 686: El Sistema 100, como tanto el Usuario A 30a y el Usuario B

30b, cumplen todas las condiciones para realizar el intercambio del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] por el Contenido $Digital_{CSR1}$ 115 'Y'[Huella $Digital_{CSR1}$ 207 'Y'] del Usuario B 30b y viceversa. Inicia el proceso de intercambio.

38. Mensaje 687: El Sistema 100, envía al Avatar Master B 111b, la siguiente tripleta de datos: Huella $Digital_{CSR1}$ 207 'X' / Key_{CSR2} 209a 'X' / Key_{AM} 208b 'X' para que lo almacene de manera segura.
39. Mensaje 688: El Sistema 100, envía al Repositorio B del Contenidos 115ba el Contenido $Digital_{CSR1}$ 115 'X' con un contenedor seguro iterativo de una iteración con clave Key_{INT} 210a 'X'.
40. Mensaje 689: El Sistema 100, envía al Avatar Usuario B 112b, la información Huella $Digital_{CSR1}$ 207 'X' / Key_{AU} 208a 'X' y la guarda de manera segura.
41. La distribución de las claves de cifrado Key_{CSR2} 209a 'X' / Key_{AU} 208a 'X' / Key_{AM} 208b 'X' a los avatares del Usuario B 30b, Avatar Master B 111b y Avatar Usuario B 112b, el Sistema 100 distribuye el Contenido Digital 114 'X' al Usuario B 30b transformado en Contenido $Digital_{CSR1}$ 115 'X' y protegido en un contenedor seguro virtual de relación de derechos de autor y de consumidor.
42. Mensaje 690: El Sistema 100, envía al Avatar Master A 111a, la siguiente tripleta de datos: Huella $Digital_{CSR1}$ 207 'Y'/ Key_{CSR2} 209a 'Y'/ Key_{AM} 208b 'Y' para que lo almacene de manera segura.
43. Mensaje 691: El Sistema 100, envía al Repositorio Contenidos A 115a el Contenido $Digital_{CSR1}$ 115 'Y' con un contenedor seguro iterativo de una iteración con clave Key_{INT} 210a 'Y'.
44. Mensaje 692: El Sistema 100, envía al Avatar Usuario A 112a, la información Huella $Digital_{CSR1}$ 207 'Y' / Key_{AU} 208a 'Y' y lo guarda de manera segura.
45. La distribución de las claves de cifrado Key_{CSR2} 209a 'Y' / Key_{AU} 208a 'Y' / Key_{AM} 208b 'Y' a los avatares del Usuario A 30a, Avatar Master A 111a y Avatar Usuario A 112a, el Sistema 100 distribuye el Contenido Digital 114 'Y' al Usuario A 30a transformado en Contenido $Digital_{CSR1}$ 115 'Y' y protegido en un contenedor seguro virtual de relación de derechos de autor y de consumidor.
46. Mensaje 693: El Sistema 100, confirma al Usuario B 30b el intercambio del Contenido $Digital_{CSR1}$ 115 'Y'[Huella $Digital_{CSR1}$ 207 'Y'] por el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] del Usuario A 30a.
47. Mensaje 694: El Sistema 100, confirma al Usuario A 30a el intercambio del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] por el Contenido $Digital_{CSR1}$ 115 'Y'[Huella $Digital_{CSR1}$ 207 'Y'] del Usuario B 30b.

[172] **Distribución en Modalidad de 'Cesión Temporal/Regalo' y Devoluciones de 'Cesión Temporal' o de 'Alquiler'**

[173] La distribución de cesión se realiza cuando un usuario realiza una cesión temporal del contenido digital a otro usuario y no existe una transacción económica entre el usuario que cede el Contenido $Digital_{CSR1}$ 115 y el usuario que recibe temporalmente el uso del Contenido $Digital_{CSR1}$ 115. Durante el periodo de la cesión temporal, el usuario que transfiere temporalmente el contenido digital no podrá hacer uso del contenido digital cedido, mientras que el usuario que recibe la cesión temporal disfrutará del uso del Contenido $Digital_{CSR1}$ 115. Un regalo de un Contenido $Digital_{CSR1}$ 115 se considera como una cesión en la que el tiempo de la cesión es ilimitado.

[174] La devoluciones tanto de una cesión temporal o de un alquiler, aunque sean casuísticas diferentes, a nivel de diagrama de secuencia son idénticas a una cesión temporal, por esa razón se describen de manera conjunta.

[175] Para simplificar el diagrama de secuencia se tiene en cuenta que el usuario ha dado de alta un único Avatar Master y Avatar Usuario. En el caso que el usuario dispusiera de más de un Avatar Master/Usuario, se repetiría los mensajes con cada Avatar Master/Usuario hasta que se borrasen todas las posibles copias y el sistema recibiese la correspondiente confirmación de cada Avatar Master para de esta manera poder comenzar el proceso de cesión o devolución.

[176] También se ha simplificado todo el flujo de mensajes que se produciría entre los Avatar Master a los avatares clones en los diferentes dispositivos digitales sin acceso a una red pública, reflejándolo en la activación 761.

[177] La Figura 7 describe el diagrama de secuencia de distribución de cesión temporal/ regalo y la devolución de una cesión temporal o de un alquiler, y el objetivo de este diagrama de secuencia es detallar una de las posibles secuencias de mensajes y activaciones de los componentes lógicos de la invención para mostrar cómo se resolvería la casuísticas que se tratan en este apartado.

[178] A continuación se describen los mensajes y activaciones de la Figura 7:

1. Mensaje 750: El Usuario A 30a, adquirió a través del Sistema 100 el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'], y realiza una solicitud de devolución/cesión el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] al Usuario B 30b.
2. Mensaje 751: El Sistema 100, valida al Usuario A 30a, a través de su Avatar Usuario A 112a.
3. Mensaje 752: Avatar Usuario A 112a le envía un mensaje al Usuario A 30a, para que se valide y le informa que se va a proceder devolución/cesión del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'].
4. Mensaje 753: Avatar Usuario A 112a le solicita al Usuario A 30a que se au-

tentique, una vez que el usuario se ha validado correctamente.

5. Mensaje 754: Avatar Usuario A 112a confirma al Sistema 100 que el Usuario A 30a se ha autenticado correctamente y el Avatar Usuario A 112a se autentica con el Sistema 100 a través de su firma digital.
6. Mensaje 755: El Sistema 100, valida la integridad del Avatar Master A 111a, y solicita información de las copias en Avatar Master Clone 121 realizadas del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] y no eliminadas.
7. Activación 756: El Avatar Master A 111a obtiene el número de copias distribuidas en los diferentes Avatar Master Clone 121 del Usuario A 30a.
8. Mensaje 757: El Avatar Master A 111a se autentica con el Sistema 100 a través de su firma digital. Informa del número de copias realizadas en Avatar Master Clone 121 del Usuario A 30a y que aún no están borradas.
9. Mensaje 758: El Sistema 100, notifica al Usuario A 30a que se va a proceder devolución/cesión del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] y le informa del número de copias que tiene distribuidas en sus correspondientes Avatar Master Clone 121, y solicita la confirmación del borrado por parte del Usuario A 30a.
10. Mensaje 759: El Usuario A 30a, acepta la devolución/cesión y que se proceda al borrado de todas las copias en los respectivos Avatar Master Clone 121.
11. Mensaje 760: El Sistema 100, notifica al Avatar Master A 111a que se proceda al borrado de todas las copias del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'].
12. Activación 761: El Avatar Master A 111a, comienza el borrado solicitando al Usuario A 30a que conecte todos los dispositivos sin acceso a redes públicas para proceder con la sincronización con el Avatar Master Clone 121 y Avatar Usuario Clone 122 que están en dicho dispositivo. Valida previamente a todos los componentes lógicos con sus respectivas firmas digitales. Este proceso estará activo hasta que estén sincronizados todos los dispositivos digitales en los que el Avatar Master A 111a tiene registrada una sincronización del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'].
13. Mensaje 762: El Avatar Master A 111a sincronizado con todos los Avatar Master Clone 121 y Avatar Usuario Clone 122, y borradas todas las referencias del Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'], se elimina la referencia en el Avatar Usuario A 112a y la suya propia.
14. Mensaje 763: El Avatar Master A 111a borra el Contenido $Digital_{CSR1}$ 115 'X'[Huella $Digital_{CSR1}$ 207 'X'] del Repositorio de Contenidos 115a del Usuario A 30a.
15. Mensaje 764: El Avatar Master A 111a, envía al Sistema 100, vía callback

una notificación del borrado de todas las copias del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] y se puede realizar la devolución/cesión. Al recibir este mensaje el Sistema 100, se aseguran todos los derechos de autor, ya que se han borrado todas las claves de cifrado del Contenido Digital$_{CSR1}$ 115 'X' que se desea devolver o realizar una cesión temporal/regalo.

16. Activación 765: El Sistema 100, listo para devolución/cesión, el Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'], y queda registrado quién es el usuario que lo devuelve/cesión, junto con sus claves de cifrado asociadas Key $_{CSR2}$ 209a 'X' / Key$_{AM}$ 208b 'X' / Key$_{AU}$ 208a 'X'.
17. Mensaje 766: El Sistema 100, notifica al Usuario A 30a realizada la devolución/cesión del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] (esta notificación puede ser vía mail, etc.) y pendiente que el Usuario B 30b reciba la devolución/cesión.
18. Mensaje 767: El Sistema 100, notifica al Usuario B 30b que tiene disponible una devolución/cesión del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] (esta notificación puede ser vía mail, etc.).
19. Mensaje 768: Un Usuario B 30b, al recibir la notificación de que tiene ya disponible una devolución/cesión de Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X']. Envía una notificación de recogida de la devolución/ cesión Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'].
20. Mensaje 769: El Sistema 100, valida al Usuario B 30b a través de su Avatar Usuario B 112b.
21. Mensaje 770: Avatar Usuario B 112b le envía un mensaje al Usuario B 30b para que se valide y le informa que se va a proceder a la devolución/cesión del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'].
22. Mensaje 771: Avatar Usuario B 112b le solicita al Usuario B 30b que se autentique, una vez que el usuario se ha validado correctamente.
23. Mensaje 772: Avatar Usuario B 112b confirma al Sistema 100 que el Usuario B 30b se ha autenticado correctamente y el Avatar Usuario B 112b se autentica con el sistema a través de su firma digital.
24. Mensaje 773: El Sistema 100, valida la integridad del Avatar Master B 111b.
25. Mensaje 774: El Avatar Master B 111b se autentica con el Sistema 100 a través de su firma digital.
26. Activación 775: El Sistema 100, comienza el inicio de la devolución/cesión del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] desde Usuario A 30a al Usuario B 30b.
27. Mensaje 776: El Sistema 100, envía al Avatar Master B 111b, la siguiente tripleta de datos: Huella Digital$_{CSR1}$ 207 'X' / Key$_{CSR2}$ 209a 'X' / Key$_{AM}$ 208b 'X'

para que lo almacene de manera segura.

28. Mensaje 777: El Sistema 100, envía al Repositorio Contenidos B 115ba el Contenido Digital$_{CSR1}$ 115 'X' con un contenedor seguro iterativo de una iteración con clave Key$_{INT}$ 210a 'X'.
29. Mensaje 778: El Sistema 100, envía al Avatar Usuario B 112b el par de datos: Huella Digital$_{CSR1}$ 207 'X' / Key$_{AU}$ 208a 'X' y lo guarda de manera segura.
30. La distribución de las claves Key$_{CSR2}$ 209a 'X' / Key$_{AU}$ 208a 'X' / Key$_{AM}$ 208b 'X' a los avatares del Usuario B 30b, Avatar Master B 111b y Avatar Usuario B 112b, el Sistema 100 distribuye el Contenido Digital 114 'X' al Usuario B 30b transformado en Contenido Digital$_{CSR1}$ 115 'X' y protegido en un contenedor seguro virtual de relación de derechos de autor y de consumidor.
31. Mensaje 779: El Sistema 100, confirma la devolución/cesión con éxito del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] al Usuario B 30b.
32. Mensaje 780: El Sistema 100, confirma la devolución/cesión con éxito del Contenido Digital$_{CSR1}$ 115 'X'[Huella Digital$_{CSR1}$ 207 'X'] al Usuario A 30a.

[179] **Uso y Disfrute de un Usuario de un Contenido Digital con un Contenedor Seguro Virtual de Relación de Derechos de Autor y de Consumidor**

[180] La Figura 8 describe el diagrama de secuencia del uso y disfrute de un usuario que dispone de un contenido digital protegido en un contenedor seguro virtual de relación de derechos de autor y de consumidor, y el objetivo de este diagrama de secuencia es mostrar una de las posibles secuencias de mensajes y activaciones de los componentes lógicos de la invención para exponer como se resolvería la casuística que se tratan en este apartado.

[181] A continuación se describen los mensajes y activaciones de la Figura 8:

1. Mensaje 850: Un Usuario 30, accede a su Reproductor Digital 113.
2. Mensaje 851: El Reproductor Digital 113, recupera del Repositorio Contenido Digitales$_{CSR1}$ 115a toda la meta información de la cabecera de los ficheros, para mostrar la información al Usuario 30.
3. Mensaje 852: El Reproductor Digital 113, se autentica y genera un canal seguro e indica su firma digital al Avatar Master 111.
4. Mensaje 853: Avatar Master 111 también se autentica e indica su firma digital al Reproductor Digital 113.
5. Mensaje 854: Avatar Master 111 se autentica y genera un canal seguro e indica su firma digital al Avatar Usuario 112.
6. Mensaje 855: Avatar Usuario 112 también se autentica e indica su firma digital al Avatar Master 111.
7. Mensaje 856: El Reproductor Digital 113 muestra la lista de Contenidos Digitales$_{CSR1}$ 115 'X' al Usuario 30.

8. Mensaje 857: El Usuario 30 selecciona un Contenido Digital$_{CSR1}$ 115 'Y'.
9. Mensaje 858: El Reproductor Digital 113, recupera del repositorio el Contenido Digital$_{CSR1}$ 115 'Y'.
10. Activación 859: El Reproductor Digital 113, calcula la Huella Digital$_{CSR1}$ 207 'Y' del Contenido Digital$_{CSR1}$ 207 'Y'.
11. Mensaje 860: El Reproductor Digital 113, consulta al Avatar Master 112 con la Huella Digital$_{CSR1}$ 207 'Y' para que le proporcione Key$_{INT}$ 210a 'Y' para poder descifrar los datos 114b del Contenido Digital$_{CSR1}$ 115 'Y' y de esta manera poder reproducir el Contenido Digital$_{CSR1}$ 115 'Y'.
12. Activación 861: El Avatar Master 111 consulta si tiene la Huella Digital$_{CSR1}$ 207 'Y', si existe una entrada, consulta al Avatar Usuario 112.
13. Mensaje 862: Consulta al Avatar Usuario 112 para obtener la información relacionada con la Huella Digital$_{CSR1}$ 207 'Y'.
14. Activación 863: El Avatar Usuario 112 consulta si dispone de una entrada para la Huella Digital$_{CSR1}$ 207 'Y'.
15. Mensaje 864: El Avatar Usuario 112 envía las claves Key$_{AU}$ 208a 'Y' que tiene asociada para la Huella Digital$_{CSR1}$ 207 'Y' al Avatar Master 111.
16. Activación 865: El Avatar Master 111 realiza el descifrado simétrico de Key $_{CSR2}$ 209a 'Y' con la clave Key$_{AM}$ 208b 'Y' y se obtiene Key$_{CSR1}$ 'Y'.
17. Activación 866: El Avatar Master 111 realiza el descifrado simétrico de Key $_{CSR1}$ 'Y' con la clave Key$_{AU}$ 208a 'Y' y se obtiene Key$_{INT}$ 210a 'Y'.
18. Mensaje 867: El Avatar Master 111, envía al Reproductor Digital 113 la clave Key$_{INT}$ 210a 'Y' de la Huella Digital$_{CSR1}$ 207 'Y'.
19. Activación 868: El Reproductor Digital 113 con la clave Key$_{INT}$ 210a 'Y' descifra los datos 114b del Contenido Digital$_{CSR1}$ 115 'Y'[Huella Digital$_{CSR1}$ 207 'Y'] y reproduce Contenido Digital$_{CSR1}$ 115 'Y' para que el Usuario 30 disfrute de su uso.

[182] **Copias de un Contenido Digital con un Contenedor Seguro Virtual de Relación de Derechos de Autor y de Consumidor a diferentes dispositivos digitales de un mismo Usuario**

[183] Un usuario puede copiar los contenidos digitales con contenedor seguro virtual de relación de derechos de autor y de consumidor en sus diferentes dispositivos digitales tanto a sus diferentes Dispositivos Digitales de Usuario sin Acceso a Redes Públicas 120, como a sus Dispositivos Digitales de Usuario con Acceso a Redes Públicas 110.

[184] Todos los dispositivos digitales deberán tener instalado su Avatar Master Clone 121 y Avatar Usuario Clone 122 del Usuario 30, si es un dispositivo de otro usuario, dicha copia no se podrá realizar.

[185] Para poder reproducir/visualizar/ejecutar el contenidos digitales con contenedor

seguro virtual de relación de derechos de autor y de consumidor tendrá que sincronizar los correspondientes avatares tanto el Avatar Master 111 como el Avatar Usuario 112 con el correspondiente avatar del dispositivo en el que se realiza la copia, Avatar Master Clone 121 y Avatar Usuario Clone 122 respectivamente.

[186] La Figura 9 describe el diagrama de secuencia de como se sincronizan los avatares cuando el usuario realiza la copia de los contenidos digitales con contenedor seguro virtual de relación de derechos de autor y de consumidor a otro dispositivo digital del propio usuario, y el objetivo de este diagrama de secuencia es detallar una de las posibles secuencias de mensajes y activaciones de los componentes lógicos de la invención para exponer como se resolvería la casuística que se trata en este apartado.

[187] A continuación se describen los mensajes y activaciones Figura 9:

1. Mensaje 950: Un Usuario 30, que está accediendo a su Avatar Usuario 112 para realizar una sincronización de contenidos digitales con contenedor seguro virtual de relación de derechos de autor y de consumidor a otro dispositivo digital, después de autenticarse el usuario en su Avatar Usuario 112.
2. Mensaje 951: El Avatar Usuario 112, recupera del repositorio de todos los Contenido Digitales_{CSRI} 115 la meta información de la cabecera de los ficheros, para mostrar la información al usuario.
3. Mensaje 953: El Usuario 30 selecciona una lista de Contenidos Digitales_{CSRI} 115 para clonarlo en otro dispositivo del propio Usuario 30.
4. Mensaje 954: El Avatar Usuario 112, se autentica y genera un canal seguro e indica su firma digital, solicita toda la información de Huellas Digitales_{CSRI} 207 que tiene disponible Avatar Usuario Clone 122.
5. Mensaje 955: El Avatar Usuario Clone 122, se autentica e indica su firma digital al Avatar Usuario 112 y le proporciona toda la información de las Huellas Digitales_{CSRI} 207 de Contenido Digitales_{CSRI} 115.
6. Activación 956: El Avatar Usuario 112, validación de la información y registro de todas las Huellas Digitales_{CSRI} 207 que se van a sincronizar con el Avatar Usuario Clone 122 del dispositivo Digital.
7. Mensaje 957: El Avatar Usuario 112, transfiere todas las Huellas Digitales_{CSRI} 207 junto con las claves asociadas al Avatar Usuario Clone 122.
8. Activación 958: El Avatar Usuario 112, realiza un commit de que la sincronización con el Avatar Usuario Clone 122 ha sido correcta.
9. Mensaje 959: El Avatar Usuario 112, se autentica y genera un canal seguro e indica su firma digital, solicita toda la información de Huellas Digitales_{CSRI} 207 que tiene disponible Avatar Master 111.
10. Mensaje 960: El Avatar Master 111, se autentica e indica su firma digital al Avatar Usuario 112 y le proporciona toda la información de las Huellas

Digitales$_{CSR1}$ 207 de Contenido Digitales$_{CSR1}$ 115.

11. Mensaje 961: El Avatar Usuario 112, le indica al Avatar Master 111 que se sincronice con el Avatar Master Clone 121.
12. Mensaje 962: El Avatar Master 111, se autentica y genera un canal seguro e indica su firma digital, solicita toda la información de Huellas Digitales$_{CSR1}$ 207 que tiene disponible Avatar Master Clone 121.
13. Mensaje 963: El Avatar Master Clone 121, se autentica e indica su firma digital al Avatar Master 111 y le proporciona toda la información de las Huellas Digitales$_{CSR1}$ 207 de Contenido Digitales$_{CSR1}$ 115.
14. Activación 964: El Avatar Master 111, validación de la información y registro de todas las Huellas Digitales$_{CSR1}$ 207 que se van a sincronizar con el Avatar Master Clone 121 del dispositivo digital.
15. Mensaje 965: El Avatar Master 111, transfiere toda la información de control de la sincronización realizada con el dispositivo digital al Sistema 100.
16. Activación 966: El Sistema 100, deja registrada la información de control de la sincronización con el dispositivo digital en la cuenta del usuario.
17. Mensaje 967: El Avatar Master 111, transfiere todas las Huellas Digitales$_{CSR1}$ 207 junto con las claves de cifrado asociadas al Avatar Master Clone 121.
18. Activación 968: El Avatar Master 111, realiza un commit de que la sincronización con el Avatar Master Clone 121 ha sido correcta.
19. Mensaje 969: El Avatar Master 111, indica al Sistema 100 que la sincronización realizada con el dispositivo digital fue Ok.
20. Activación 970: El Sistema 100, deja registrada el commit de la sincronización con el dispositivo digital en la cuenta del usuario.
21. Mensaje 971: El Avatar Master 111, indica al Avatar Usuario 112 que la sincronización realizada con el dispositivo digital fue Ok.
22. Mensaje 972: El Avatar Usuario 112, le indica al Repositorio Contenido Digitales$_{CSR1}$ 115a que se sincronice con el Repositorio Contenido Digitales $_{CSR1}$ 115b del dispositivo digital.
23. Mensaje 973: El repositorio Contenido Digitales$_{CSR1}$ 115a se sincroniza con el repositorio Contenido Digitales$_{CSR1}$ 115b del dispositivo digital.
24. Mensaje 974: El repositorio Contenido Digitales$_{CSR1}$ 115a comunica al Avatar Usuario 112 que la sincronización con el repositorio Contenido Digitales$_{CSR1}$ 115b del dispositivo digital fue correcta.
25. Mensaje 975: El Avatar Usuario 112, comunica al Usuario 30 que la sincronización se realizo correctamente.

[188] **Avatar**

[189] Los avatares de la invención tienen un rol, y es el de representar a un actor que forma

parte del contenedor seguro virtual de relación de derechos. En su rol de representación a un actor mantiene la custodia de al menos una de las claves que permiten descifrar el Contenido $Digital_{CSR1}$ 115 con un contenedor seguro recursivo virtual.

[190] Para formar un contenedor seguro virtual de relación de derechos entre el autor 10 y el consumidor 30 es necesario un avatar por cada actor que forma parte de la relación de derechos: Avatar Master 111 y Avatar Usuario 112, junto con sus respectivos clones que se ejecutan en cada uno de los dispositivos del usuario 30.

[191] Los avatares son componentes lógicos de la invención que son un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario. Este tipo de programas se ejecutan de forma continua (infinita) y aunque se intente cerrar o matar el proceso, este continuará en ejecución o se reiniciará automáticamente, y todo esto sin intervención de terceros y sin dependencia de consola alguna.

[192] Este tipo de funcionamiento es conocido como un 'proceso demonio' en los sistemas operativos Unix/Linux, o los 'servicios' del sistema operativo Windows. Los avatares serán procesos totalmente seguros y la funcionalidad principal es la gestión de las $Claves_{CSR1}$ 208, 209 que le distribuye el Sistema 100, junto con las funcionalidades de gestión de sincronización con otros avatares con su mismo rol pero en diferente dispositivo digital de usuario.

[193] Los avatares tendrán un conjunto de puertos de comunicación, en dónde recibirán los mensajes desde cualquier otro componente lógico de la invención o desde el Sistema 100. Toda comunicación será de manera segura y antes de comenzar se autenticarán a través de la firma digital de cada componente lógico, en el caso que no sea correcta las autenticaciones la comunicación no se establece.

[194] Con los avatares se permite crear en todo momento un contenedor seguro virtual de relación de derechos de autor y de consumidor, si el contenedor seguro virtual de relación de derechos necesita de más entidades con un rol determinado, tan sólo se debería activar un nuevo avatar que represente al nuevo rol en cada uno de los dispositivos digitales de usuarios, y adaptar la lógica del Avatar Master para que consulte al nuevo avatar y así obtener la clave de cifrado que custodia en representación de la nueva entidad.

[195] En un Dispositivo Digital de Usuario con Acceso a Redes Públicas 110 se ejecutan los avatares:

[196] El Avatar Master 111, el rol que tiene en la invención es custodiar que no se infringen los derechos de autor. Almacena de modo seguro la asociación entre la Huella $Digital_{CSR1}$ 207 de un Contenido $Digital_{CSR1}$ 115 con las claves key_{CSR2} 209a y key_{AM} 208b. Además mantiene las siguientes funcionalidades de gestión:

- Sincronización con otros avatares del mismo rol (Avatar Master Clone 121)

pero en otro dispositivo digital del propio usuario 30, este nuevo dispositivo digital de usuario debe pertenecer al mismo propietario, si es de otro propietario/usuario no se sincronizará. La manera de detectarlo se realiza a través de las firmas digitales de los avatares, ya que antes de poder sincronizarse, al avatar clonado debe haber sido dado de alta por el usuario en su cuenta.

- Registro de todas las sincronizaciones realizadas con otros avatares del mismo rol pero en otro dispositivo digital de usuario y qué Huellas Digitales$_{CSR1}$ 207 de Contenido Digital$_{CSR1}$ 115 se han distribuido a cada uno.
- Envío de toda la información de sincronización a la cuenta del usuario del Sistema 100, que el usuario 30 en todo momento podrá consultar.
- Registro del único Avatar Usuario 112 con el cual puede dialogar e intercambiar información dentro del mismo dispositivo digital y que ha sido validado y registrado por el Sistema 100.
- Registro de la firmas digitales del software que realiza la reproducción/visualización/ejecución de un Contenido Digital$_{CSR1}$ 115 y validación que es un software seguro.

[197] El Avatar Usuario 112, el rol que tiene en la invención es de mantener los derechos del consumidor cuando compra un Contenido Digital$_{CSR1}$ 115. Almacena de modo seguro la asociación entre la Huella Digital$_{CSR1}$ 207 de un Contenido Digital$_{CSR1}$ 115 con la clave key$_{AU}$ 208a. Además mantiene las siguientes funcionalidades de gestión:

- Sincronización con otros avatares del mismo rol (Avatar Usuario Clone 122) pero en otro dispositivo digital del usuario 30, este nuevo dispositivo digital debe pertenecer al mismo propietario, si es de otro propietario/usuario no se sincronizará. La manera de detectarlo se hará a realiza a través de las firmas digitales de los avatares, ya que antes de poder sincronizarse, los avatares deben haber sido dado de alta por el usuario en su cuenta.
- Registro de todas las sincronizaciones realizadas con otros avatares del mismo rol pero en otro dispositivo digital de usuario y qué Huellas Digitales$_{CSR1}$ 207 de Contenido Digital$_{CSR1}$ 115 se han distribuido.
- Envío de toda la información de sincronización a la cuenta del usuario del Sistema 100, que el usuario 30 en todo momento podrá consultar.
- Registro del único Avatar Master 111 con el cual puede dialogar e intercambiar información dentro del mismo dispositivo, y que ha sido validado y registrado por el Sistema 100.

[198] En un Dispositivo Digital de Usuario sin Acceso a Redes Públicas 120 se ejecutaran los avatares:

[199] El Avatar Master Clone 121, el rol que tiene en la invención es custodiar que no se infringen los derechos de autor. Almacena de modo seguro la asociación entre la

Huella Digital$_{CSR1}$ 207 de un Contenido Digital$_{CSR1}$ 115 con las claves key$_{CSR2}$ 209a y key$_{AM}$ 208b. Este Avatar no dispone de ninguna funcionalidad de gestión, y solo puede sincronizarse con el Avatar Master 111 del usuario 30.

[200] El Avatar Usuario Clone 122, el rol que tiene en la invención es de mantener los derechos del consumidor cuando compra un contenido digital. Almacena de modo seguro la asociación entre la Huella Digital$_{CSR1}$ 207 de un Contenido Digital$_{CSR1}$ 115 con la clave key$_{AU}$ 208a. Este avatar no dispone de ninguna funcionalidad de gestión, y solo puede sincronizarse con el Avatar Usuario 112 del usuario 30.

[201] **Avatar Delegado en el Sistema**

[202] En un Dispositivo Digital de Usuario con Acceso a Redes Públicas 110, podrá delegar la ejecución de los Avatar Master 111 y Avatar Usuario 112 en el sistema 100, por lo tanto Reproductor Digital 113 se conecta al Avatar Master 111 del usuario que está en el sistema 100 en lugar de consultar al Avatar Master 111 que tendría que estar localmente en el Dispositivo Digital de Usuario con Acceso a Redes Públicas 110.

[203] **El Servidor del Sistema**

[204] El software de los avatares se comunica e interactúa con el software del servidor. Además, los usuarios 30 a través de un navegador web pueden comunicarse e interactuar con el software del servidor.

[205] El componente lógico Sistema 100 de la invención, controla y mantiene un conjunto de base de datos 116 que son usadas para proporcionar las siguientes funcionalidades:

[206] En el plano de usuario:

- Marco funcional para la distribución de los Contenidos Digitales$_{CSR1}$ 115 en las modalidades de primera mano, segunda mano, alquiler, intercambio y cesión temporal/regalo.
- Marco funcional para que el usuario 30 pueda recuperar todos los Contenidos Digitales$_{CSR1}$ 115 que estén vigentes en su cuenta.
- Marco funcional para soportar los avatares delegados por el usuario 30.
- Marco funcional de toda la gestión de un usuario de su cuenta:
    - Registro de todas las sincronizaciones y Huellas Digitales$_{CSR1}$ 207 de un Contenido Digital$_{CSR1}$ 115 y en qué dispositivo digital del usuario existe una copia.
    - Registro de todos los Avatares Clone que dispone el usuario 30 y en que dispositivo digital del usuario están alojados.
    - Otras funcionalidades de gestión de usuario.

[207] En el plano de autor de contenidos digitales y medios autorizados:

- Marco funcional para la gestión y publicación Contenidos Digitales 114.
- Otras funcionalidades de gestión de Autor/Medios Autorizados.

[208] En el plano de Gestión:

- Proporcionar acceso a las diferentes plataformas de pagos para que el usuario pueda adquirir un Contenido Digital$_{CSRI}$ 115.
- Proporcionar el abono a un Usuario/Autor en unidades monetarias.
- Catálogo de Contenidos Digitales$_{CSRI}$ 115 publicados en primera mano, en segunda mano, en alquiler, en intercambio.
- Gestión de las cuentas de usuarios.
- Gestión de la transacción de Contenido Digital$_{CSRI}$ 115 entre los usuarios.

[209] En el plano de Servicio:

- Lógica de servicio para realizar la transformación de un Contenido Digital 114 a un Contenido Digital$_{CSRI}$ 115.
- Lógica de servicio para permitir todos los modelos de distribución.
- Recepción y procesamiento de los callback de los avatares que se comunican con el sistema.
- Integración con plataformas de medios de pagos.
- API de integración con plataformas de terceros.

[210] **Reproducción/Visualización/Ejecución de Contenidos Digitales con un Contenedor Seguro Virtual de Relación de Derechos de Autor y de Consumidor**

[211] El software que realiza la reproducción/visualización/ejecución de un contenido digital con un contenedor seguro virtual de relación de derechos de autor y de consumidor previamente deberá darse de alta en el Avatar Master que reside en el dispositivo digital y/o sistema, y que el Avatar Master tras validar que es un software seguro y registrarlo con un software seguro y de confianza, se podrán establecer conexiones de comunicación.

[212] El software que realiza la reproducción/visualización/ejecución de un contenido digital con un contenedor seguro virtual de relación de derechos de autor y de consumidor para poder realizar el descifrado Contenido Digital$_{CSRI}$ 115, obtendrá su Huella Digital$_{CSRI}$ 207, con la huella digital obtenida, se comunicará con el avatar master que resida en el dispositivo digital y/o sistema, la comunicación se realiza siempre de manera segura y deben estar autenticados con su firma digital.

[213] A través del canal de comunicación entre el software de reproducción/visualización/ejecución y el avatar master, el avatar master le enviará la clave para poder realizar el descifrado del contenido digital con un contenedor seguro virtual de relación de derechos de autor y de consumidor a partir de la Huella Digital$_{CSRI}$ 207 enviada por el software de reproducción/visualización/ejecución al avatar master que reside en el dispositivo digital.

[214] **Protección de los Derechos de Autor a través de la Invención**

[215] Los derechos de autor siempre están protegidos por la invención por lo siguiente:

[216] Un contenido digital 114, nunca se distribuye a un usuario 30. En el dispositivo digital existe un contenido digital con un contenedor seguro virtual de relación de derechos de autor y de consumidor, es decir, el Contenido $Digital_{CSR1}$ 115 que al disponer de un contenedor seguro recursivo virtual, puede existir todas las copias que el usuario desee tener en cualquier medio de almacenamiento.

[217] Con los Avatar Master 111 y el Avatar Usuario 112 se establecen nexos virtuales de relación entre el autor 10 y el usuario 30, por lo tanto, sólo lo podrá reproducir el usuario que ha comprado el contenido digital a través del Sistema 100, ya que aunque se copie el Contenido $Digital_{CSR1}$ 115 a otro usuario, el Avatar de Usuario 112 no dispondrá de la clave para poder realizar el descifrado del Contenido $Digital_{CSR1}$ 115. Cuando el usuario crea una cuenta en el Sistema 100, quedan registrados los Avatar Master 111 y el Avatar Usuario 112, y tanto el avatar master y el avatar usuario sólo podrán dialogar entre ellos y sus respectivos avatares clonados en otros dispositivos digitales del mismo usuario y registrados en el Sistema 100.

[218] Para que se pueda realizar cualquier distribución de segunda mano, intercambio, alquiler, cesión temporal/regalo, el Avatar Master 111 que reside en el dispositivo digital del usuario se sincroniza con todos los avatares clonados en otros dispositivos y se elimina la Huella $Digital_{CSR1}$ 207 del Contenido $Digital_{CSR1}$ 115 que se desea vender en segunda mano, intercambiar, alquilar, ceder temporalmente o regalar. Si la sincronización no se realiza con éxito, la distribución no se realiza, y sólo cuando la sincronización se realiza en todos los avatares en dónde reside una entrada de la Huella $Digital_{CSR1}$ 207 del Contenido $Digital_{CSR1}$ 115 es cuando se realiza la distribución solicitada por el usuario. En el Sistema 100 y en los Avatar Master 111/Avatar Usuario 112 están registradas las sincronizaciones con los avatares clones y en qué dispositivo digital del usuario reside, para que el usuario pueda conectarlo y de esta manera realizar el borrado de la huella digital en el dispositivo digital en el que existe la copia.

[219] **Conservación de los Derechos del Consumidor a través de la Invención**

[220] Los derechos de consumidor se mantienen a través de la invención por lo siguiente:

[221] Puede realizar todas las copias que deseen en cualquier dispositivo digital en el que exista un Avatar Master Clone 121 y Avatar Usuario Clone 122 del consumidor.

[222] No existe limitación por el Sistema 100 para reproducir/visualizar/ejecutar, las únicas limitaciones son las del software que realiza la reproducción/visualización/ejecución de un contenido digital con un contenedor seguro virtual de relación de derechos de autor y de consumidor.

[223] Dispone de las modalidades de distribución de segunda mano, intercambio, alquiler, cesión temporal/regalo del Contenido $Digital_{CSR1}$ 115.

Reivindicaciones

[Reivindicación 1] Método de generación de un contenedor seguro recursivo virtual (200) que establece nexos virtuales de relación a un fichero digital (114) mediante la generación de contenedores seguros iterativos tanto al fichero digital (114) como a las claves de cifrado (203; 210). Los cifrados que se pueden realizar en cada iteración son mediante técnicas de cifrado simétrico o con técnicas de cifrados asimétricos y el orden en que se realizan los cifrados simétricos/asimétricos no es condicionante ni limitante. Cuando se realiza un cifrado en una iteración se puede realizar sobre el resultado obtenido de un cifrado anterior si previamente ya se hizo un cifrado, **caracterizado** por:

a) Como datos de entrada: Fichero digital (114); Modelo contenedor seguro recursivo (204); Lista de claves de cifrado externas (203).

b) Como resultado del método de generación del contenedor seguro recursivo virtual: Fichero digital protegido (115); Huella digital (207) del fichero digital protegido (115); Lista de claves de cifrado sin contenedor seguro iterativo (208); Lista de claves de cifrado con un contenedor seguro iterativo (209).

c) Como componentes lógicos: Un Controlador Lógico Generador Contenedor Seguro Recursivo Virtual (202); Un Cifrador Simétrico/ Asimétrico (205) que realiza cifrados simétricos/asimétricos en la cabecera (114a)/datos (114b)/todo del fichero digital (114); Un Cifrador Simétrico/Asimétrico de Texto/Claves (206) que realiza cifrados simétricos/asimétricos en las claves de cifrado (203; 210); Un Generador de Claves Simétrica/Asimétrica (201) que genera claves simétricas/asimétricas de cifrado aleatorias (210); Un Generador Resumen Criptográfico (211) que calcula la huella digital (207).

d) El Controlador Lógico Generador Contenedor Seguro Recursivo Virtual (202) con los componentes lógicos: Una Estructura de Objetos de Datos (202a) que es una estructura de datos dinámica que mantiene la evolución de transformación de cada objeto de datos en cada iteración; Un Analizador Datos de Entrada (202b) que valida que son correctos los datos de entrada; Un Controlador de Objetos de Datos (202c) que gestiona la Estructura de Objetos de Datos (202a) y prepara los objetos de datos; Un Actualizador Objetos de Datos (202n) que actualiza la Estructura de Objetos de Datos (202a) con el estado de transformación de todos los objetos de datos al finalizar una iteración.

[Reivindicación 2] El método según la reivindicación 1, en el que el Controlador Lógico Generador Contenedor Seguro Recursivo Virtual (202) tiene la lógica funcional:

a) Validación que los datos de entrada son correctos con el Analizador Datos de Entrada (202b), si no son correctos se termina con error.

b) Crear/actualizar y gestionar la Estructura de Objetos de Datos (202a) y determinar/preparar los objetos de datos a procesar en la iteración en curso con el Controlador de Objetos de Datos (202c).

c) Lógicas de decisión que determinan la acción a realizar según la definición de la iteración en curso del modelo contenedor seguro recursivo (204): lógica de decisión (202d) si la clave simétrica/ asimétrica a usar se genera aleatoriamente con el Generador de Claves Simétrica/Asimétrica (201) o se obtiene de las claves externas (203), lógica de decisión (202e) si realizar con técnicas de cifrado simétrico (205a) un cifrado en la cabecera (114a) del fichero digital (114), lógica de decisión (202f) si realizar con técnicas de cifrado simétrico (205b) un cifrado en los datos (114b) del fichero digital (114), lógica de decisión (202g) si realizar con técnicas de cifrado simétrico (205c) un cifrado en todo el fichero digital (114), lógica de decisión (202h) si realizar con técnicas de cifrado simétrico (206a) un cifrado en una clave de cifrado, lógica de decisión (202i) si realizar con técnicas de cifrado asimétrico (205d) un cifrado en la cabecera (114a) del fichero digital (114), lógica de decisión (202j) si realizar con técnicas de cifrado asimétrico (205e) un cifrado en los datos (114b) del fichero digital (114), lógica de decisión (202k) si realizar con técnicas de cifrado asimétrico (205f) un cifrado en todo el fichero digital (114) y lógica de decisión (202m) si realizar con técnicas de cifrado asimétrico (206b) un cifrado en una clave de cifrado.

d) Actualiza la Estructura de Objetos de Datos (202a) con el estado de transformación de todos los objetos de datos y si se crea una clave aleatoria de cifrado simétrica añade una nueva entrada o si es una clave asimétrica añade dos nuevas entradas (pública/privada) con el Actualizador Objetos de Datos (202n).

e) Lógica de decisión (202o) para determinar si finaliza la secuencia de cifrados definidos en el modelo contenedor seguro recursivo (204). Si hay otra iteración, volver al punto b) de la lógica funcional descrita, si no hay más iteraciones, generar la huella digital (207) con el Generador Resumen Criptográfico (211) y se termina.

[Reivindicación 3] El método según la reivindicación 1, en el que el fichero digital (114) es un libro electrónico, un archivo digital de video, un archivo digital de música, una aplicación informática o cualquier fichero digital que para su uso y/o disfrute sea necesario un dispositivo digital.

[Reivindicación 4] El método según la reivindicación 1, en el que el objeto de datos en el que aplicar una técnica de cifrado para realizar un cifrado en una iteración es: en la cabecera del fichero digital (114a), o en los datos del fichero digital (114b), o en todo el fichero digital (114), o en una clave de cifrado (203; 210), o en una parte de los objetos de datos citados.

[Reivindicación 5] El método según la reivindicación 1, en el que el modelo de contenedor seguro recursivo (204) define una secuencia de cifrados simétricos/ asimétricos e indica en cada iteración: el objeto de datos, la técnica de cifrado a utilizar simétrico/asimétrico y la clave de cifrado a utilizar (si es externa (203) o se genera aleatoriamente (210) por el Generador de Claves Simétrica/Asimétrica (201)).

[Reivindicación 6] El método según la reivindicación 1, en el que las claves externas (203) define una lista de claves de cifrado y para cada clave de cifrado tiene asociado un identificador único, y el identificador único se utiliza en el modelo de contenedor seguro recursivo (204) para identificar la clave de cifrado a usar en una iteración.

[Reivindicación 7] El método según la reivindicación 1, en el que la clave simétrica/ asimétrica de cifrado se genera aleatoriamente (210), cada clave de cifrado tiene un identificador único, y para un cifrado asimétrico la clave de cifrado a utilizar para realizar el cifrado en la iteración en curso, si usar la clave pública o utilizar la clave privada, se indica en el modelo de contenedor seguro recursivo (204).

[Reivindicación 8] El método según la reivindicación 1, en el que el fichero digital protegido (115) es el fichero digital (114) con cifrados simétricos/asimétricos de manera iterativa: en la cabecera del fichero digital y/o en los datos del fichero digital y/o en todo el fichero digital de datos. El orden en que se realizan los cifrados simétricos/asimétricos, parcial o totalmente, en el fichero digital no es condicionante ni limitante.

[Reivindicación 9] El método según la reivindicación 1, con técnicas de resumen criptográfico donde la lógica asigna al fichero protegido (115) una huella digital (207) obtenida tras aplicar una técnica de resumen criptográfico con el Generador Resumen Criptográfico (211).

[Reivindicación 10] El método según la reivindicación 1, en el que la lista de claves de cifrado sin contenedor seguro iterativo (208) son claves (203; 210) sin

cifrados simétricos/asimétricos y la lista de claves de cifrado con un contenedor seguro iterativo (209) son claves (203; 210) en la que se ha realizado cifrados simétricos/asimétricos de manera iterativa. El orden en que se realizan los cifrados simétricos/asimétricos, parcial o totalmente, en la clave de cifrado no es condicionante ni limitante

[Reivindicación 11] El método según la reivindicación 1, en el que el descifrado del contenedor seguro recursivo virtual se realiza con descifrados simétricos/asimétricos de manera inversa a como se realizaron los cifrados simétricos/asimétricos aplicados para generar los contenedores seguros iterativos, es decir, se procesa el modelo de contenedor seguro recursivo (204) de manera inversa, desde el final al inicio y se realiza un descifrado simétrico o asimétrico según indica la iteración, en el caso de cifrado asimétrico, si se cifró con la clave pública se usa la clave privada, y si se cifró con la clave privada se usa la clave pública.

[Reivindicación 12] Método de generación de un contenedor seguro virtual de relación de derechos **caracterizado** por establecer nexos virtuales de relación de derechos entre entidades utilizando el método de contenedor seguro recursivo virtual (200) y la distribución de manera única de al menos una de las claves de cifrado (208; 209) relacionadas con la huella digital (207) del fichero protegido (115) a cada uno de los avatares que están en uno o más dispositivos digitales de usuario con acceso a redes públicas (110) y/o en el sistema (100).

[Reivindicación 13] El método según la reivindicación 12, en el que el dispositivo digital de usuario con acceso a redes públicas (110) es un ordenador personal, un portátil, un dispositivo de música/vídeo digital, un lector de libros electrónicos, un iTablet, etc. y el dispositivo digital de usuario tiene acceso a una red de comunicaciones pública (130).

[Reivindicación 14] El método según la reivindicación 12, en el que el avatar es un proceso informático no interactivo que se ejecuta en segundo plano y no es controlado directamente por el usuario y cada avatar representa a una entidad que forma parte del contenedor seguro virtual de relación de derechos. El avatar custodia de manera única y segura, de al menos una de las claves de cifrado (208; 209) relacionadas con la huella digital (207) del fichero protegido (115).

[Reivindicación 15] El método según la reivindicación 12, en el que los nexos virtuales de relación de derechos son entre un autor (10) y un consumidor (30).

[Reivindicación 16] El método según la reivindicación 15, en el que el Avatar Master (111) representa al autor (10) y el Avatar Usuario (112) al consumidor (30),

se ejecutan en uno o más dispositivos digitales de usuario con acceso a redes públicas (110) y/o en el sistema (100), y el Avatar Master Clone (121) y el Avatar Usuario Clone (122) residen en uno o más dispositivos digitales de usuario sin acceso a redes públicas (120).

[Reivindicación 17] El método según la reivindicación 16, en el que el dispositivo digital de usuario sin acceso a redes públicas (120) es un dispositivo de música digital, eBooks, iTablet, etc. y sólo tiene acceso a una red de comunicaciones local (131) (USB, bluetooth, etc.) y se comunica con un dispositivo digital de usuario con acceso a redes públicas (110).

[Reivindicación 18] El método según la reivindicación 15, en el que los nexos virtuales de relación de derechos incluyen a más entidades y forman un contenedor seguro virtual de derechos que incluye a más entidades.

[Reivindicación 19] El método según la reivindicación 18, en el que una entidad es un distribuidor, un órgano regulador, una empresa, una asociación jurídica o cualquier tipo de medio autorizado.

[Reivindicación 20] El método según la reivindicación 18, donde cada entidad tiene asociada un avatar que la representa en el contenedor seguro virtual de relación de derechos y custodia de manera única y segura, de al menos una de las claves de cifrado (208; 209) relacionadas con la huella digital (207) del fichero protegido (115). El avatar se ejecuta en uno o más dispositivos digitales de usuario con acceso a redes públicas (110) y/o en el sistema (100), y un avatar clone que se ejecuta en uno o más dispositivos digitales de usuario sin acceso a redes públicas (120).

[Reivindicación 21] El método según la reivindicación 20, en el que un avatar puede implementar varios roles representando por cada rol a una entidad, y recibe al menos una clave de cifrado (208; 209) a custodiar de manera única por cada una de las entidades que representa el avatar.

[Reivindicación 22] Un sistema (100) de distribución de ficheros digitales protegidos que incluye: Una lógica de gestión de autor (10) para publicar contenidos ficheros digitales (114); Una lógica de gestión del usuario (30); Adaptado para conceder al usuario (30) un paquete de software: Avatar Master (111), Avatar Usuario (112) y un Reproductor Digital (113) asignando a cada elemento del paquete software (111; 112; 113) un par de claves pública-privada asociadas con un usuario (30); Un dispositivo de usuario con acceso a redes públicas (110) adaptado para recibir dicho paquete de software (111; 112; 113). **Caracterizado** por:
a) El usuario (30) debe estar dado de alta en el sistema (100) y tener instalado el paquete software (111; 112; 113) en el dispositivo de

usuario con acceso a redes públicas (110) con el que luego accede a todas las funcionalidades que le proporciona el sistema (100).

b) Sólo distribuye ficheros digitales protegidos (115) a un usuario (30) que un autor (10) o un medio autorizado (20) lo publica en el sistema (100) con un contenedor seguro virtual de relación de derechos.

c) Las claves de cifrado (208; 209) resultado del método contenedor seguro recursivo virtual (200) son: 'key_{CSR2} (209a)' que es la clave de cifrado 'key_{INT} (210a)' con un contenedor seguro iterativo de dos iteraciones donde key_{INT} (210a) es una clave simétrica de cifrado creada aleatoriamente que genera el contenedor seguro iterativo de una iteración en los datos (114b) fichero digital (114) , 'key_{AU} (208a)' que es una clave simétrica de cifrado creada aleatoriamente utilizada para generar el contenedor seguro iterativo en la primera iteración de key_{INT} (210a) y 'key_{AM} (208b)' que es la clave simétrica de cifrado creada aleatoriamente usada para generar el contenedor seguro iterativo en la segunda iteración de key_{INT} (210a). Para cada nueva entidad en el contenedor seguro virtual de relación de derechos, se realiza una nueva iteración en el contenedor seguro iterativo de key_{INT} (210a) con una nueva clave simétrica de cifrado creada aleatoriamente.

d) Establece conexiones seguras con el Avatar Master (111) que se ejecuta en un dispositivo de usuario con acceso a redes públicas (110) del usuario (30) y valida su integridad mediante su firma digital y le distribuye un conjunto de claves de cifrado (208; 209) asociadas a la huella digital (207) del fichero digital protegido (115) distribuido.

e) Establece conexiones seguras con el Avatar Usuario (112) que se ejecuta en un dispositivo de usuario con acceso a redes públicas (110) del usuario (30) y valida su integridad mediante su firma digital y le distribuye un conjunto de claves de cifrado (208; 209) asociadas a la huella digital (207) del fichero digital protegido (115) distribuido.

f) El Avatar Master (111) puede sincronizarse con otro Avatar Master y/o Avatar Master Clone (121) del usuario (30). El sistema (100) a cada nuevo avatar master o avatar master clone le asigna un nuevo par de claves pública-privada asociadas con el usuario (30).

g) El Avatar Usuario (112) puede sincronizarse con otro Avatar Usuario y/o Avatar Usuario Clone (122) del usuario (30). El sistema (100) a cada nuevo avatar usuario o avatar usuario clone le asigna un nuevo par de claves pública-privada asociadas con el usuario (30).

h) Toda la comunicación entre los avatares es segura y de confianza, y

se valida la integridad de cada avatar mediante su firma digital.
i) Toda la comunicación entre el Avatar Master (111) y el reproductor Digital (113) es segura y de confianza, y se valida la integridad del avatar/reproductor digital mediante sus firmas digitales.
j) Toda la comunicación entre el Avatar Master Clone (121) y el reproductor Digital (113) es segura y de confianza, y se valida la integridad del avatar/reproductor digital mediante sus firmas digitales.
k) El usuario (30) puede tener uno o más reproductores Digitales (113) y están registrados en su cuenta de usuario en el sistema (30) y el sistema (100) le asigna a cada uno un nuevo par de claves pública-privada asociadas con el usuario (30).
l) Mantiene por cada usuario (30) el registro de todas las sincronizaciones del Avatar Master (111) con sus Avatar Master Clone (121) y el dispositivo digital en que reside cada avatar master clone.

[Reivindicación 23] Un sistema (100) según la reivindicación 22, en el que la distribución se realiza en la modalidad de primera mano de un fichero digital protegido (115) a un usuario (30), **caracterizado** porque el sistema (100) distribuye el fichero digital protegido (115) al repositorio del usuario (30), envía al Avatar Master (111) la tripleta de datos: huella digital (207) del fichero digital protegido (115), la clave Key_{CSR2} (209a) y la clave Key_{AM} (208b) y envía al Avatar Usuario (112) el par de datos: huella digital (207) del fichero digital protegido (115) y la clave Key_{AU} (208a).

[Reivindicación 24] Un sistema (100) según con cualquiera de las reivindicaciones 22 a 23, en el que la distribución, además se realiza en la modalidad de segunda mano o de alquiler de un fichero digital protegido (115) del usuario A (30a) al usuario B (30b), **caracterizado** porque el sistema (100) solicita al Avatar Master (111a) del usuario A (30a) que se eliminen todas las referencias de la huella digital (207) del fichero digital protegido (115) de todos los avatares en donde se haya realizado una copia de la huella digital (207) del fichero digital protegido (115). Cuando el Avatar Master (111a) elimina todas las referencias de la huella digital (207) del fichero digital protegido (115) de todos los avatares, vía callback se lo comunica al sistema (100). Cuando el sistema (100) recibe la confirmación del Avatar Master (111a) del usuario A (30a) distribuye:
a) El fichero digital protegido (115) al repositorio del usuario B (30b).
b) Al Avatar Master (111b) del usuario B (30b) la tripleta de datos: huella digital (207) del fichero digital protegido (115), la clave Key_{CSR2}

(209a) y la clave Key_{AM} (208b).

c) Al Avatar Usuario (112b) del usuario B (30b) el par de datos: huella digital (207) del fichero digital protegido (115) y la clave Key_{AU} (208a).

[Reivindicación 25] Un sistema (100) según la reivindicación 24, en el que el alquiler lo realiza un medio autorizado (20) a un usuario (30).

[Reivindicación 26] Un sistema (100) según con cualquiera de las reivindicaciones 22 a 25, en el que la distribución, además se realiza en la modalidad de intercambio de un fichero digital protegido A (115) del usuario A (30a) al usuario B (30b), y de un fichero digital protegido B (115) del usuario B (30b) al usuario A (30a), **caracterizado** porque el sistema (100):

a) Solicita al Avatar Master (111a) del usuario A (30a) que se eliminen todas las referencias de la huella digital (207) del fichero digital protegido A (115) de todos los avatares en donde se haya realizado una copia de la huella digital (207) del fichero digital protegido A (115). Cuando el Avatar Master (111a) elimina todas las referencias de la huella digital (207) del fichero digital protegido A (115) de todos los avatares, vía callback se lo comunica al sistema (100).

b) Solicita al Avatar Master (111b) del usuario B (30b) que se eliminen todas las referencias de la huella digital (207) del fichero digital protegido B (115) de todos los avatares en donde se haya realizado una copia de la huella digital (207) del fichero digital protegido B (115). Cuando el Avatar Master (111b) elimina todas las referencias de la huella digital (207) del fichero digital protegido B (115) de todos los avatares, vía callback se lo comunica al sistema (100).

c) Cuando el sistema (100) recibe la confirmación del Avatar Master (111a) del usuario A (30a) y del Avatar Master (111b) del usuario B (30b), el sistema (100) realiza las distribuciones:

I) El fichero digital protegido B (115) del usuario B (30b) al repositorio del usuario A (30a).

II) Al Avatar Master (111a) del usuario A (30a) la tripleta de datos: huella digital (207) del fichero digital protegido B (115), la clave Key_{CSR2} B (209a) y la clave Key_{AM} B (208b).

III) Al Avatar Usuario (112a) del usuario A (30a) el par de datos: huella digital (207) del fichero digital protegido B (115) y la clave Key_{AU} B (208a).

IV) El fichero digital protegido A (115) del usuario A (30a) al repositorio del usuario B (30b).

V) Al Avatar Master (111b) del usuario B (30b) la siguiente tripleta de

datos: huella digital (207) del fichero digital protegido A (115), la clave Key_{CSR2} A (209a) y la clave Key_{AM} A (208b).

VI) Al Avatar Usuario (112b) del usuario B (30b) el siguiente par de datos: huella digital (207) del fichero digital protegido A (115) y la clave Key_{AU} A (208a).

[Reivindicación 27] Un sistema (100) según con cualquiera de las reivindicaciones 22 a 26, en el que la distribución, además se realiza en la modalidad de cesión temporal/regalo o la devolución de un fichero digital protegido (115) del usuario A (30a) al usuario B (30b), **caracterizado** porque el sistema (100) solicita al Avatar Master (111a) del usuario A (30a) que se eliminen todas las referencias de la huella digital (207) del fichero digital protegido (115) de todos los avatares en donde se haya realizado una copia de la huella digital (207) del fichero digital protegido (115). Cuando el Avatar Master (111a) elimina todas las referencias huella digital (207) del fichero digital protegido (115) de todos los avatares, vía callback se lo comunica al sistema (100). Cuando el sistema (100) recibe la confirmación del Avatar Master (111a) del usuario A (30a), distribuye:

a) El fichero digital protegido (115) al repositorio del usuario B (30b).

b) Al Avatar Master (111b) del usuario B (30b) la tripleta de datos: huella digital (207) del fichero digital protegido (115), la clave Key_{CSR2} (209a) y la clave Key_{AM} (208b).

c) Al Avatar Usuario (112b) del usuario B (30b) el par de datos: huella digital (207) del fichero digital protegido (115) y la clave Key_{AU} (208a).

[Reivindicación 28] Un sistema (100) según con cualquiera de las reivindicaciones 22 a 27, en el que el sistema (100) distribuye un fichero digital protegido (115) con un contenedor seguro de relación de derechos de autor, de consumidor y otras entidades. El usuario (30) tiene instalado por cada entidad un avatar con un par de claves pública-privada asignadas por el sistema (100) asociadas con un usuario (30), y a cada avatar se le distribuye de manera única de al menos una de las claves de cifrado (208; 209) relacionadas con la huella digital (207) del fichero protegido (115).

[Reivindicación 29] Un sistema (100) según con cualquiera de las reivindicaciones 22 a 28, en el que el sistema (100) interactúa con una pasarela de pagos (130) para realizar abonos y liquidaciones a autores (10), a medios de autorizados (20), a usuarios (30) y a otras entidades.

REIVINDICACIONES MODIFICADAS
recibidas por la oficina Internacional el 17 Febrero 2013 (17.02.2013)

1. Método de generación de un contenedor seguro recursivo virtual (200) y de generación de un contenedor seguro virtual de relación de derechos que generan nexos virtuales de relación, en donde el método de generación de un contenedor seguro recursivo virtual (200) establece nexos virtuales de relación a un fichero digital (114) mediante la creación de contenedores seguros iterativos tanto al fichero digital (114) como a las claves de cifrado (203; 210) y el método de generación de un contenedor seguro virtual de relación de derechos establece nexos virtuales de relación entre entidades a través de la distribución de manera única de al menos una de las claves de cifrado (208; 209) relacionadas con la huella digital (207) del fichero protegido (115) a cada uno de unos avatares **caracterizado por que;**

- los cifrados de los contenedores seguros iterativos que se pueden realizar en cada iteración son mediante técnicas de cifrado simétrico o de cifrado asimétrico en donde el orden en que se realizan los cifrados simétricos/asimétricos no es condicionante ni limitante;
- cada uno de los avatares representa al menos a una entidad en el contenedor seguro virtual de relación de derechos y custodia de manera única y segura, de al menos una de las claves de cifrado (208; 209) relacionadas con la huella digital (207) del fichero protegido (115);
- cada uno de los avatares se ejecuta en uno o más dispositivos digitales de usuario con acceso a redes públicas (110) y/o en el sistema (100), y cada uno de los avatares clone se ejecuta en uno o más dispositivos digitales de usuario sin acceso a redes públicas (120);
- el método de generación de un contenedor seguro recursivo virtual (200) consiste en:
    a) como objetos de datos de entrada: Fichero digital (114); Modelo contenedor seguro recursivo (204); Lista de claves de cifrado externas (203);
    b) como objetos de datos de salida: Fichero digital protegido (115); Huella digital (207) del fichero digital protegido (115); Lista de claves de cifrado sin contenedor seguro iterativo (208); Lista de claves de cifrado con un contenedor seguro iterativo (209);
    c) con los componentes lógicos:
        I) Controlador Lógico Generador Contenedor Seguro Recursivo Virtual (202) que contiene la lógica funcional para crear nexos virtuales de relación en el fichero digital (114);
        II) Cifrador Simétrico/Asimétrico (205) que realiza cifrados simétricos/asimétricos en la cabecera (114a)/datos (114b)/todo del fichero digital (114);
        III) Cifrador Simétrico/Asimétrico de Texto/Claves (206) que realiza cifrados simétricos/asimétricos en las claves de cifrado (203; 210);
        IV) Generador de Claves Simétrica/Asimétrica (201) que genera claves simétricas/asimétricas de cifrado aleatorias (210);
        V) Generador Resumen Criptográfico (211) que calcula la huella digital (207);
- el método de generación de un contenedor seguro virtual de relación de derechos consiste en:
    a) con la lista de claves de cifrado sin contenedor seguro iterativo (208) y con la lista de claves de cifrado con un contenedor seguro iterativo (209) obtenidas a partir del método de la generación de un contenedor seguro recursivo virtual (200);

b) distribuir de manera única de al menos una de las claves de cifrado (208; 209) relacionadas con la huella digital (207) del fichero protegido (115) a cada uno de los avatares;

c) generar diferentes modalidades de relación de derechos mediante la redistribución de manera única de al menos una de las claves de cifrado (208; 209) relacionadas con la huella digital (207) del fichero protegido (115) entre unos avatares que ceden la relación de derechos a otros avatares que reciben la relación de derechos.

2. El método según la reivindicación 1, en el que el Controlador Lógico Generador Contenedor Seguro Recursivo Virtual (202) está **caracterizado por** los componentes funcionales;

- una Estructura de Objetos de Datos (202a) que es una estructura de datos dinámica que mantiene la evolución de transformación de cada objeto de datos en cada iteración;
- un Analizador Datos de Entrada (202b) que valida que son correctos los datos de entrada;
- un Controlador de Objetos de Datos (202c) que gestiona la Estructura de Objetos de Datos (202a) y prepara los objetos de datos;
- un Actualizador Objetos de Datos (202n) que actualiza la Estructura de Objetos de Datos (202a) con el estado de transformación de todos los objetos de datos al finalizar una iteración;

y con la lógica funcional:

a) validación que los datos de entrada son correctos con el Analizador Datos de Entrada (202b), si no son correctos se termina con error;

b) crear/actualizar y gestionar la Estructura de Objetos de Datos (202a) y determinar/preparar los objetos de datos a procesar en la iteración en curso con el Controlador de Objetos de Datos (202c);

c) lógicas de decisión que determinan la acción a realizar según la definición de la iteración en curso del modelo contenedor seguro recursivo (204):

I) lógica de decisión (202d) si la clave simétrica/asimétrica a utilizar se genera aleatoriamente con el Generador de Claves Simétrica/Asimétrica (201) o se obtiene de las claves externas (203);

II) lógica de decisión (202e) si realizar con técnicas de cifrado simétrico (205a) un cifrado en la cabecera (114a) del fichero digital (114);

III) lógica de decisión (202f) si realizar con técnicas de cifrado simétrico (205b) un cifrado en los datos (114b) del fichero digital (114);

IV) lógica de decisión (202g) si realizar con técnicas de cifrado simétrico (205c) un cifrado en todo el fichero digital (114);

V) lógica de decisión (202h) si realizar con técnicas de cifrado simétrico (206a) un cifrado en una clave de cifrado;

VI) lógica de decisión (202i) si realizar con técnicas de cifrado asimétrico (205d) un cifrado en la cabecera (114a) del fichero digital (114);

VII) lógica de decisión (202j) si realizar con técnicas de cifrado asimétrico (205e) un cifrado en los datos (114b) del fichero digital (114);

VIII) lógica de decisión (202k) si realizar con técnicas de cifrado asimétrico (205f) un cifrado en todo el fichero digital (114);

IX) lógica de decisión (202m) si realizar con técnicas de cifrado asimétrico (206b) un cifrado en una clave de cifrado;

d) actualiza la Estructura de Objetos de Datos (202a) con el estado de transformación de todos los objetos de datos y si se crea una clave aleatoria de cifrado simétrica añade una nueva entrada o si es una clave asimétrica añade dos nuevas entradas (pública/privada) con el Actualizador Objetos de Datos (202n);

e) lógica de decisión (202o) para determinar si finalizar la secuencia de cifrados definidos en el modelo contenedor seguro recursivo (204);

I) si hay otra iteración, volver al punto b) de la lógica funcional descrita;

II) si no hay más iteraciones, generar la huella digital (207) del fichero digital protegido (115) con el Generador Resumen Criptográfico (211) y se termina.

3. El método según la reivindicación 1, en el que el fichero digital (114) es un libro electrónico, un archivo digital de video, un archivo digital de música, una aplicación informática o cualquier fichero digital que para su uso y/o disfrute sea necesario un dispositivo digital.

4. El método según la reivindicación 1, en el que el objeto de datos en el que aplicar una técnica de cifrado para realizar un cifrado en una iteración es: en la cabecera del fichero digital (114a), o en los datos del fichero digital (114b), o en todo el fichero digital (114), o en una clave de cifrado (203; 210), o en una parte de los objetos de datos citados.

5. El método según la reivindicación 1, en el que el modelo de contenedor seguro recursivo (204) define una secuencia de cifrados simétricos/asimétricos e indica en cada iteración: el objeto de datos, la técnica de cifrado a utilizar simétrico/asimétrico y la clave de cifrado a utilizar (si es externa (203) o se genera aleatoriamente (210) por el Generador de Claves Simétrica/Asimétrica (201)).

6. El método según la reivindicación 1, en el que las claves externas (203) define una lista de claves de cifrado y para cada clave de cifrado tiene asociado un identificador único, y el identificador único se utiliza en el modelo de contenedor seguro recursivo (204) para identificar la clave de cifrado a usar en una iteración.

7. El método según la reivindicación 1, en el que la clave simétrica/asimétrica de cifrado se genera aleatoriamente (210), cada clave de cifrado tiene un identificador único, y para un cifrado asimétrico la clave de cifrado a utilizar para realizar el cifrado en la iteración en curso, si usar la clave pública o utilizar la clave privada, se indica en el modelo de contenedor seguro recursivo (204).

8. El método según la reivindicación 1, en el que el fichero digital protegido (115) es el fichero digital (114) con cifrados simétricos/asimétricos de manera iterativa: en la cabecera del fichero digital y/o en los datos del fichero digital y/o en todo el fichero digital de datos. El orden en que se realizan los cifrados simétricos/asimétricos, parcial o totalmente, en el fichero digital no es condicionante ni limitante.

9. El método según la reivindicación 1, con técnicas de resumen criptográfico donde la lógica asigna al fichero protegido (115) una huella digital (207) obtenida tras aplicar una técnica de resumen criptográfico con el Generador Resumen Criptográfico (211).

10. El método según la reivindicación 1, en el que la lista de claves de cifrado sin contenedor seguro iterativo (208) son claves (203; 210) sin cifrados simétricos/asimétricos y la lista de claves de cifrado con un contenedor seguro iterativo (209) son claves (203; 210) en la que se ha realizado cifrados simétricos/asimétricos de manera iterativa. El orden en que se realizan los cifrados simétricos/asimétricos, parcial o totalmente, en la clave de cifrado no es condicionante ni limitante.

11. El método según la reivindicación 1, en el que el descifrado del contenedor seguro recursivo virtual se realiza con descifrados simétricos/asimétricos de manera inversa a como se realizaron los cifrados simétricos/asimétricos aplicados para generar los contenedores seguros iterativos, es decir, se procesa el modelo de contenedor seguro recursivo (204) de manera inversa, desde el final al inicio y se realiza un descifrado simétrico o asimétrico según indica la iteración, en el caso de cifrado asimétrico, si se cifró con la clave pública se usa la clave privada, y si se cifró con la clave privada se usa la clave pública.

12. El método según la reivindicación 1, en el que el dispositivo digital de usuario con acceso a redes públicas (110) es un ordenador personal, un portátil, un dispositivo de música/vídeo digital, un lector de libros electrónicos, un iTablet, etc. y el dispositivo digital de usuario tiene acceso a una red de comunicaciones pública (130).

13. El método según la reivindicación 1, en el que el dispositivo digital de usuario sin acceso a redes públicas (120) es un dispositivo de música digital, eBooks, iTablet, etc. y sólo tiene acceso a una red de comunicaciones local (131) (USB, bluetooth, etc.) y se comunica con un dispositivo digital de usuario con acceso a redes públicas (110).

14. El método según la reivindicación 1, en el que el avatar es un proceso informático no interactivo que se ejecuta en segundo plano y no es controlado directamente por el usuario y cada avatar representa a una entidad que forma parte del contenedor seguro virtual de relación de derechos. El avatar custodia de manera única y segura, de al menos una de las claves de cifrado (208; 209) relacionadas con la huella digital (207) del fichero protegido (115).

15. El método según la reivindicación 1, en el que un avatar puede implementar varios roles representando por cada rol a una entidad, y recibe al menos una clave de cifrado (208; 209) a custodiar de manera única por cada una de las entidades que representa el avatar.

16. El método según la reivindicación 1, en el que los nexos virtuales de relación de derechos son entre dos entidades: un autor (10) y un consumidor (30).

17. El método según la reivindicación 16, en el que el Avatar Master (111) representa al autor (10) y el Avatar Usuario (112) al consumidor (30), se ejecutan en uno o más dispositivos digitales de usuario con acceso a redes públicas (110) y/o en el sistema (100), y el Avatar Master Clone (121) y

el Avatar Usuario Clone (122) residen en uno o más dispositivos digitales de usuario sin acceso a redes públicas (120).

18. El método según la reivindicación 16, en el que los nexos virtuales de relación de derechos incluyen a más entidades y forman un contenedor seguro virtual de derechos que incluye a más entidades.

19. El método según la reivindicación 18, en el que una entidad es un distribuidor, un órgano regulador, una empresa, una asociación jurídica o cualquier tipo de medio autorizado.

20. El método según la reivindicación 1, en el que las modalidades de relación de derechos son:
- primera mano, cuando los avatares reciben por primera vez la relación de derechos asociados a la huella digital (207) del fichero digital protegido (115);
- segunda mano o de alquiler, cuando la relación de derechos de unos avatares se transfieren a otros avatares, en donde: se eliminan todas las referencias de la relación de derechos de la huella digital (207) del fichero digital protegido (115) de todos los avatares en donde haya una referencia de la huella digital (207) del fichero digital protegido (115), y se envía la relación de derechos asociados a la huella digital (207) del fichero digital protegido (115) a los avatares receptores;
- intercambio, cuando la relación de derechos de unos avatares se intercambian con los de otros avatares, en donde: se eliminan todas las referencias de la relación de derechos de la huella digital (207) de los ficheros digitales protegidos (115) que se van a intercambiar de todos los avatares en donde haya una referencia de la huella digital (207) de cada uno de los ficheros digitales protegidos (115) que se van a intercambiar, y se envía la relación de derechos asociados a la huella digital (207) de cada fichero digital protegido (115) que se va a intercambiar a los avatares receptores respectivamente;
- cesión temporal/regalo o devolución, cuando la relación de derechos de unos avatares se transfieren a otros avatares temporalmente o indefinidamente, en donde: se eliminan todas las referencias de la relación de derechos de la huella digital (207) del fichero digital protegido (115) de todos los avatares en donde haya una referencia de la huella digital (207) del fichero digital protegido (115), y se envía la relación de derechos asociados a la huella digital (207) del fichero digital protegido (115) a los avatares receptores.

21. Un sistema (100) de distribución de ficheros digitales protegidos (115) que incluye;
- lógica de gestión de autor (10) para publicar contenidos ficheros digitales (114);
- lógica de gestión del usuario (30);
- lógica para permitir diferentes modalidades de distribución de ficheros digitales protegidos (115):
    a) distribución en modalidad de primera mano, un usuario (30) compra un fichero digital protegido (115) directamente en el sistema (100);
    b) distribución en modalidad de segunda mano, un usuario (30a) vende un fichero digital protegido (115) a otro usuario (30b) a través del sistema (100);
    c) distribución en modalidad de alquiler, un medio autorizado alquila un fichero digital protegido (115) a un usuario (30) a través del sistema (100);

d) distribución en modalidad de intercambio, dos usuarios (30a; 30b) intercambian dos ficheros digitales protegidos (115) a través del sistema (100);

e) distribución en modalidad de cesión; un usuario (30a) realiza una cesión temporal de un fichero digital protegido (115) a otro usuario (30b) a través del sistema (100);

- adaptado para conceder al usuario (30) un paquete de software: Avatar Master (111), Avatar Usuario (112) y un Reproductor Digital (113) asignando a cada elemento del paquete software (111; 112; 113) un par de claves pública-privada asociadas con un usuario (30);

caracterizado por que el usuario (30) está dado de alta en el sistema (100) y tiene instalado el paquete software (111; 112; 113) en el dispositivo de usuario con acceso a redes públicas (110) adaptado para recibir dicho paquete de software (111; 112; 113) con el que luego accede a todas las funcionalidades que le proporciona el sistema (100), y el sistema (100) está:

- adaptado para distribuir ficheros digitales protegidos (115) a un usuario (30) que un autor (10) o un medio autorizado (20) que previamente lo ha publicado en el sistema (100) con un contenedor seguro virtual de relación de derechos;

- programado para que las claves de cifrado (208; 209) resultado del método contenedor seguro recursivo virtual (200) sean: 'key_{CSR2} (209a)' que es la clave de cifrado 'key_{INT} (210a)' con un contenedor seguro iterativo de dos iteraciones donde key_{INT} (210a) es una clave simétrica de cifrado creada aleatoriamente que genera el contenedor seguro iterativo de una iteración en los datos (114b) del fichero digital (114), 'key_{AU} (208a)' que es una clave simétrica de cifrado creada aleatoriamente utilizada para generar el contenedor seguro iterativo en la primera iteración de key_{INT} (210a) y 'key_{AM} (208b)' que es la clave simétrica de cifrado creada aleatoriamente usada para generar el contenedor seguro iterativo en la segunda iteración de key_{INT} (210a);

- configurado para que por cada nueva entidad en el contenedor seguro virtual de relación de derechos, se realice una nueva iteración en el contenedor seguro iterativo de key_{INT} (210a) con una nueva clave simétrica de cifrado creada aleatoriamente;

- programado para que por cada modelo de distribución de ficheros digitales protegidos (115) se realice lo siguiente:

a) establecer conexiones seguras con el Avatar Master (111) que se ejecuta en un dispositivo de usuario con acceso a redes públicas (110) del usuario (30) y valida su integridad mediante su firma digital y le distribuye un conjunto de claves de cifrado (208; 209) asociadas a la huella digital (207) del fichero digital protegido (115) distribuido;

b) establecer conexiones seguras con el Avatar Usuario (112) que se ejecuta en un dispositivo de usuario con acceso a redes públicas (110) del usuario (30) y valida su integridad mediante su firma digital y le distribuye un conjunto de claves de cifrado (208; 209) asociadas a la huella digital (207) del fichero digital protegido (115) distribuido;

c) el Avatar Master (111) puede sincronizarse con otro Avatar Master y/o Avatar Master Clone (121) del usuario (30). El sistema (100) a cada nuevo avatar master o avatar master clone le asigna un nuevo par de claves pública-privada asociadas con el usuario (30);

d) el Avatar Usuario (112) puede sincronizarse con otro Avatar Usuario y/o Avatar Usuario Clone (122) del usuario (30). El sistema (100) a cada nuevo avatar usuario o avatar usuario clone le asigna un nuevo par de claves pública-privada asociadas con el usuario (30);

e) todos los avatares (111; 112; 121; 122) guardan de manera segura su par de claves públicas-privadas y todas las relaciones de derechos asociadas con el usuario (30) en un medio local de almacenamiento cifrado (fichero, base de datos, etc.);

f) toda la comunicación entre los avatares es segura y de confianza, y se valida la integridad de cada avatar mediante su firma digital;

g) toda la comunicación entre el Avatar Master (111) y el reproductor Digital (113) es segura y de confianza, y se valida la integridad del avatar/reproductor digital mediante sus firmas digitales;

h) toda la comunicación entre el Avatar Master Clone (121) y el reproductor Digital (113) es segura y de confianza, y se valida la integridad del avatar/reproductor digital mediante sus firmas digitales.

i) el usuario (30) puede tener uno o más reproductores Digitales (113) y están registrados en su cuenta de usuario en el sistema (30) y el sistema (100) le asigna a cada uno un nuevo par de claves pública-privada asociadas con el usuario (30) que guardan en un medio local de almacenamiento cifrado (fichero, base de datos, etc.);

j) mantiene por cada usuario (30) el registro de todas las sincronizaciones del Avatar Master (111) con sus Avatar Master Clone (121) y el dispositivo digital en que reside cada avatar master clone;

k) el sistema (100) permite interactuar con una pasarela de pagos (130) para realizar abonos y liquidaciones a autores (10), a medios de autorizados (20), a usuarios (30) y a otras entidades.

l) el sistema (100) proporciona diferentes posibilidades al usuario (30) para vender/intercambiar/ceder el fichero digital protegido (115) con otros usuarios del sistema (100) en donde:

I) en la modalidad de primera mano, el Avatar Master (111) y el Avatar Usuario (112) recibirán las correspondientes claves de cifrado del contenedor seguro virtual de relación de derechos asociadas a las huella digital (207) del fichero digital protegido (115) y el usuario se descarga el fichero digital protegido (115);

II) en las modalidades de segunda mano/alquiler, a través del sistema (100) los correspondientes Avatar Master (111) y los Avatar Usuario (112) de cada usuario se redistribuyen las correspondientes claves de cifrado del contenedor seguro virtual de relación de derechos asociadas a las huella digital (207) del fichero digital protegido (115) y el usuario que compra/alquila se descarga el correspondiente fichero digital protegido (115);

III) en la modalidad de intercambio, a través del sistema los correspondientes Avatar Master (111) y los Avatar Usuario (112) de cada usuario se intercambiaran las correspondientes claves de cifrado del contenedor seguro virtual de relación de derechos asociadas a las huella digital (207) del fichero digital protegido (115) y cada usuario se descarga el correspondiente fichero digital protegido (115) intercambiado;

IV) en la modalidad de cesión temporal, a través del sistema (100) los correspondientes Avatar Master (111) y los Avatar Usuario (112) de cada usuario se redistribuyen las correspondientes claves de cifrado del contenedor seguro virtual de relación de derechos

asociadas a las huella digital (207) del fichero digital protegido (115) y el usuario que recibe la cesión temporal se descarga el correspondiente fichero digital protegido (115).

22. Un sistema (100) según las reivindicaciones 20 y 21, en el que la distribución se realiza en la modalidad de primera mano de un fichero digital protegido (115) a un usuario (30), **caracterizado por que** el sistema (100) está adaptado, programado y configurado para distribuir: el fichero digital protegido (115) al repositorio del usuario (30); enviar al Avatar Master (111) la tripleta de datos: huella digital (207) del fichero digital protegido (115), la clave Key_{CSR2} (209a) y la clave Key_{AM} (208b); y enviar al Avatar Usuario (112) el par de datos: huella digital (207) del fichero digital protegido (115) y la clave Key_{AU} (208a).

23. Un sistema (100) según la reivindicación 20 y con cualquiera de las reivindicaciones 21 a 22, en el que la distribución, además se realiza en la modalidad de segunda mano o de alquiler por un medio autorizado (20) de un fichero digital protegido (115) del usuario A (30a) al usuario B (30b), **caracterizado por que** el sistema (100) está programado y configurado para:

- solicitar al Avatar Master (111a) del usuario A (30a) que se eliminen todas las referencias de la huella digital (207) del fichero digital protegido (115) de todos los avatares en donde haya una referencia de la huella digital (207) del fichero digital protegido (115);
- cuando el Avatar Master (111a) elimina todas las referencias de la huella digital (207) del fichero digital protegido (115) de todos los avatares, vía callback se lo comunica al sistema (100);
- cuando el sistema (100) recibe la confirmación del Avatar Master (111a) del usuario A (30a), está adaptado para distribuir:
  a) el fichero digital protegido (115) al repositorio del usuario B (30b);
  b) al Avatar Master (111b) del usuario B (30b) la tripleta de datos: huella digital (207) del fichero digital protegido (115), la clave Key_{CSR2} (209a) y la clave Key_{AM} (208b);
  c) al Avatar Usuario (112b) del usuario B (30b) el par de datos: huella digital (207) del fichero digital protegido (115) y la clave Key_{AU} (208a).

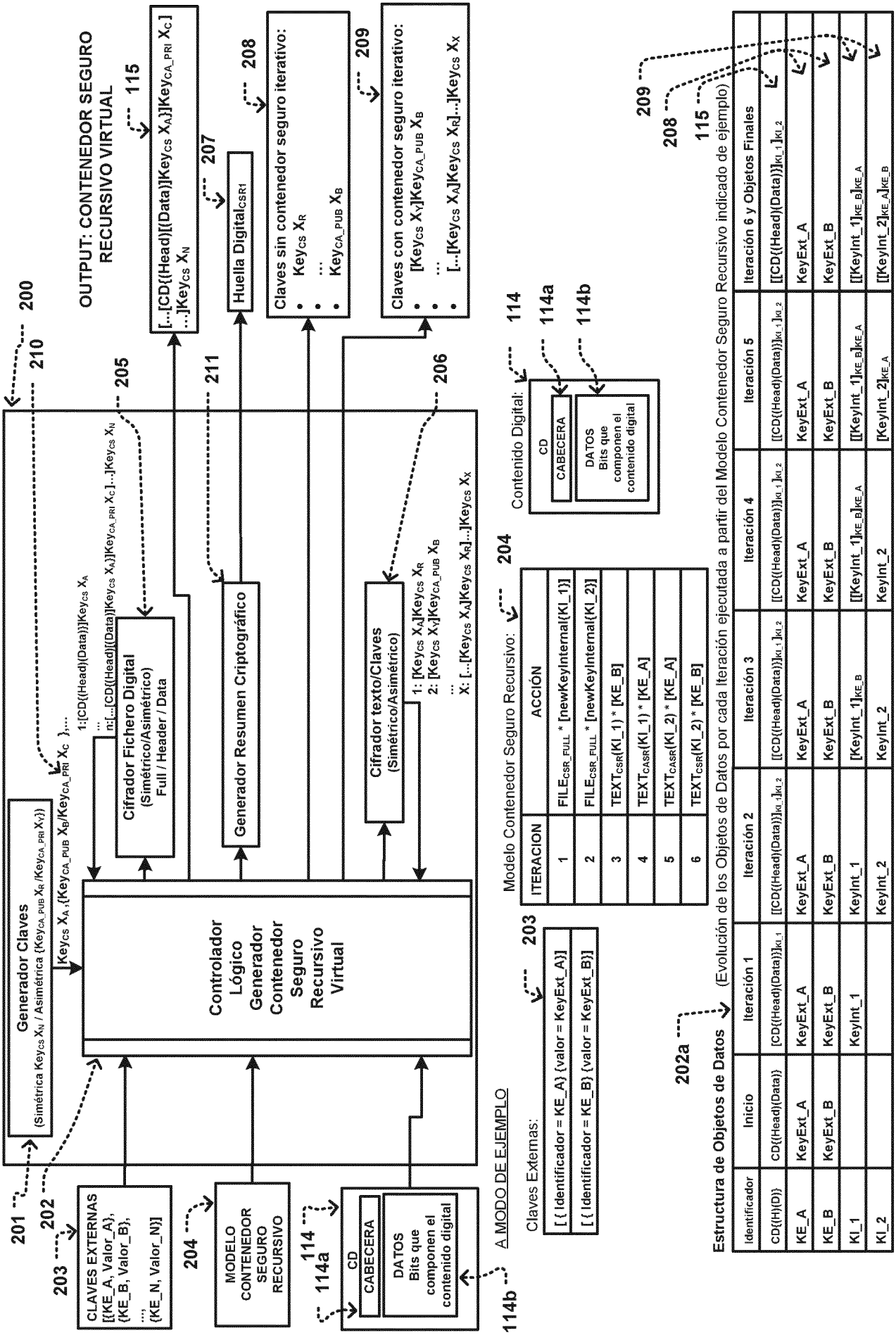
24. Un sistema (100) según la reivindicación 20 y con cualquiera de las reivindicaciones 21 a 23, en el que la distribución, además se realiza en la modalidad de intercambio de un fichero digital protegido A (115) del usuario A (30a) al usuario B (30b), y de un fichero digital protegido B (115) del usuario B (30b) al usuario A (30a), **caracterizado por que** el sistema (100) está programado y configurado para:

- solicitar al Avatar Master (111a) del usuario A (30a) que se eliminen todas las referencias de la huella digital (207) del fichero digital protegido A (115) de todos los avatares en donde haya una referencia de la huella digital (207) del fichero digital protegido A (115);
- cuando el Avatar Master (111a) elimina todas las referencias de la huella digital (207) del fichero digital protegido A (115) de todos los avatares, vía callback se lo comunica al sistema (100);
- solicitar al Avatar Master (111b) del usuario B (30b) que se eliminen todas las referencias de la huella digital (207) del fichero digital protegido B (115) de todos los avatares en donde haya una referencia de la huella digital (207) del fichero digital protegido B (115);

- cuando el Avatar Master (111b) elimina todas las referencias de la huella digital (207) del fichero digital protegido B (115) de todos los avatares, vía callback se lo comunica al sistema (100);
- cuando el sistema (100) recibe la confirmación del Avatar Master (111a) del usuario A (30a) y del Avatar Master (111b) del usuario B (30b), el sistema (100) está adaptado para distribuir:
  a) el fichero digital protegido B (115) del usuario B (30b) al repositorio del usuario A (30a);
  b) al Avatar Master (111a) del usuario A (30a) la tripleta de datos: huella digital (207) del fichero digital protegido B (115), la clave Key_{CSR2} B (209a) y la clave Key_{AM} B (208b);
  c) al Avatar Usuario (112a) del usuario A (30a) el par de datos: huella digital (207) del fichero digital protegido B (115) y la clave Key_{AU} B (208a);
  d) el fichero digital protegido A (115) del usuario A (30a) al repositorio del usuario B (30b);
  e) al Avatar Master (111b) del usuario B (30b) la siguiente tripleta de datos: huella digital (207) del fichero digital protegido A (115), la clave Key_{CSR2} A (209a) y la clave Key_{AM} A (208b);
  f) al Avatar Usuario (112b) del usuario B (30b) el siguiente par de datos: huella digital (207) del fichero digital protegido A (115) y la clave Key_{AU} A (208a).

25. Un sistema (100) según la reivindicación 20 y con cualquiera de las reivindicaciones 21 a 24, en el que la distribución, además se realiza en la modalidad de cesión temporal/regalo o la devolución de un fichero digital protegido (115) del usuario A (30a) al usuario B (30b), **caracterizado por que** el sistema (100) está programado y configurado para:
- solicitar al Avatar Master (111a) del usuario A (30a) que se eliminen todas las referencias de la huella digital (207) del fichero digital protegido (115) de todos los avatares en donde haya una referencia de la huella digital (207) del fichero digital protegido (115);
- cuando el Avatar Master (111a) elimina todas las referencias huella digital (207) del fichero digital protegido (115) de todos los avatares, vía callback se lo comunica al sistema (100);
- cuando el sistema (100) recibe la confirmación del Avatar Master (111a) del usuario A (30a), está adaptado para distribuir:
  a) el fichero digital protegido (115) al repositorio del usuario B (30b);
  b) al Avatar Master (111b) del usuario B (30b) la tripleta de datos: huella digital (207) del fichero digital protegido (115), la clave Key_{CSR2} (209a) y la clave Key_{AM} (208b);
  c) al Avatar Usuario (112b) del usuario B (30b) el par de datos: huella digital (207) del fichero digital protegido (115) y la clave Key_{AU} (208a).

26. Un sistema (100) según la reivindicación 20 y con cualquiera de las reivindicaciones 21 a 25, en el que el sistema (100) está programado y configurado para distribuir un fichero digital protegido (115) con un contenedor seguro de relación de derechos de autor, de consumidor y otras entidades, en donde:
- el usuario (30) tiene instalado por cada entidad un avatar con un par de claves pública-privada asignadas por el sistema (100) asociadas con un usuario (30) y que se guardan en un medio local de almacenamiento cifrado (fichero, base de datos, etc.);
- a cada avatar de cada entidad se le distribuye de manera única de al menos una de las claves de cifrado (208; 209) relacionadas con la huella digital (207) del fichero protegido (115).



Estructura de Objetos de Datos (Evolución de los Objetos de Datos por cada iteración ejecutada a partir del Modelo Contenedor Seguro Recursivo indicado de ejemplo)

Identificador	Inicio	Iteración 1	Iteración 2	Iteración 3	Iteración 4	Iteración 5	Iteración 6 y Objetos Finales
CD{{H}{D}}	CD{{Head}{Data}}	[CD{{Head}{Data}}]$_{KI\_1}$	[[CD{{Head}{Data}}]$_{KI\_1}$]$_{KI\_2}$	[[CD{{Head}{Data}}]$_{KI\_1}$]$_{KI\_2}$	[[CD{{Head}{Data}}]$_{KI\_1}$]$_{KI\_2}$	[[CD{{Head}{Data}}]$_{KI\_1}$]$_{KI\_2}$	[[CD{{Head}{Data}}]$_{KI\_1}$]$_{KI\_2}$
KE_A	KeyExt_A	KeyExt_A	KeyExt_A	KeyExt_A	KeyExt_A	KeyExt_A	KeyExt_A
KE_B	KeyExt_B	KeyExt_B	KeyExt_B	KeyExt_B	KeyExt_B	KeyExt_B	KeyExt_B
KI_1		KeyInt_1	[KeyInt_1]$_{KE\_B}$	[[KeyInt_1]$_{KE\_B}$]$_{KE\_A}$	[[KeyInt_1]$_{KE\_B}$]$_{KE\_A}$	[[KeyInt_1]$_{KE\_B}$]$_{KE\_A}$	[[KeyInt_1]$_{KE\_B}$]$_{KE\_A}$
KI_2			KeyInt_2	KeyInt_2	[KeyInt_2]$_{KE\_A}$	[KeyInt_2]$_{KE\_A}$	[[KeyInt_2]$_{KE\_A}$]$_{KE\_B}$

Figura 1

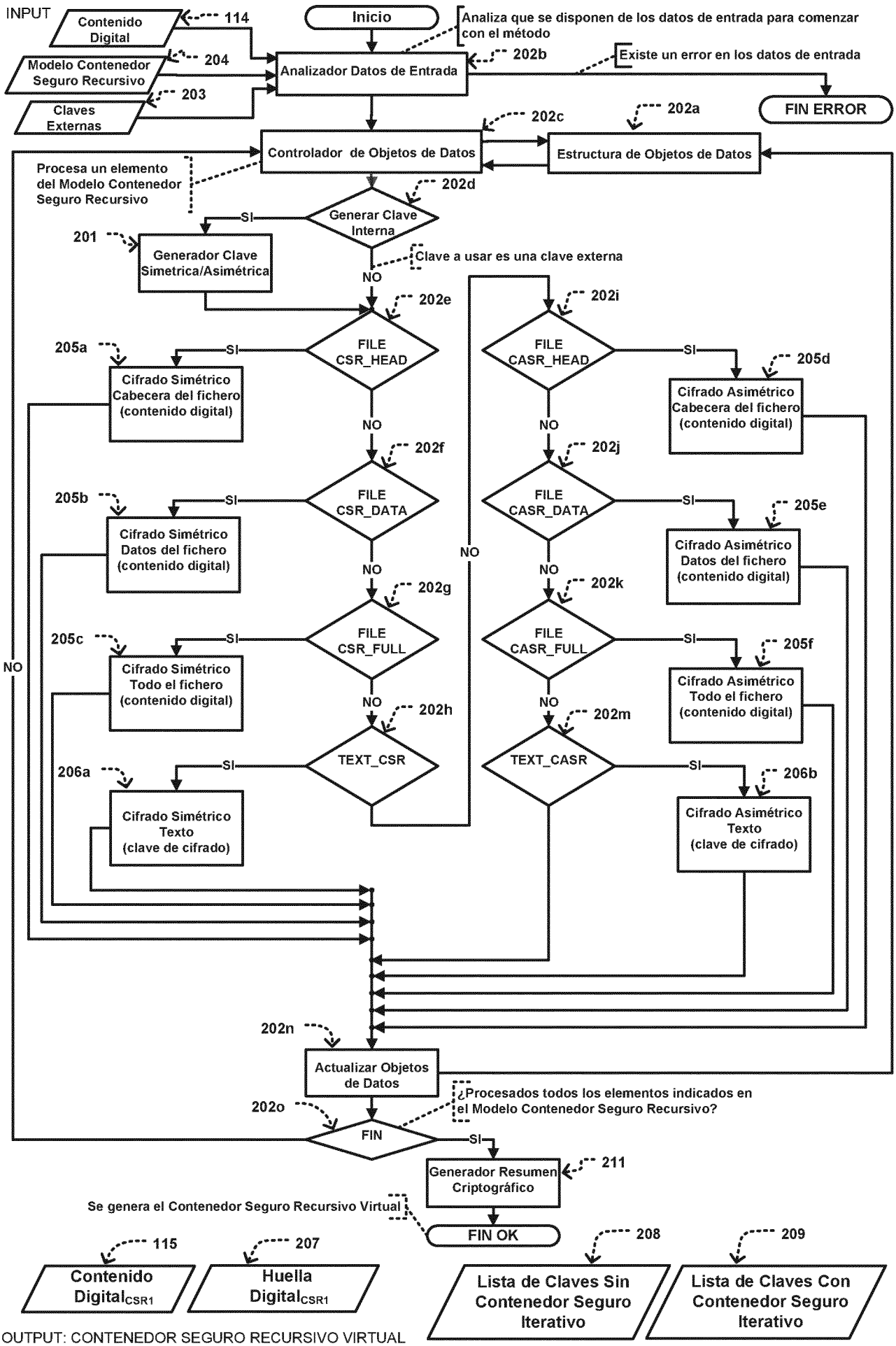

INPUT
Contenido Digital
114
Modelo Contenedor Seguro Recursivo
204
Claves Externas
203
Inicio
Analiza que se disponen de los datos de entrada para comenzar con el método
Analizador Datos de Entrada
202b
Existe un error en los datos de entrada
FIN ERROR
202c
202a
Controlador de Objetos de Datos
Estructura de Objetos de Datos
Procesa un elemento del Modelo Contenedor Seguro Recursivo
202d
Generar Clave Interna
SI
201
Generador Clave Simetrica/Asimétrica
Clave a usar es una clave externa
NO
202e
FILE CSR_HEAD
205a
Cifrado Simétrico Cabecera del fichero (contenido digital)
202i
FILE CASR_HEAD
205d
Cifrado Asimétrico Cabecera del fichero (contenido digital)
202f
FILE CSR_DATA
205b
Cifrado Simétrico Datos del fichero (contenido digital)
202j
FILE CASR_DATA
205e
Cifrado Asimétrico Datos del fichero (contenido digital)
202g
FILE CSR_FULL
205c
Cifrado Simétrico Todo el fichero (contenido digital)
202k
FILE CASR_FULL
205f
Cifrado Asimétrico Todo el fichero (contenido digital)
202h
TEXT_CSR
206a
Cifrado Simétrico Texto (clave de cifrado)
202m
TEXT_CASR
206b
Cifrado Asimétrico Texto (clave de cifrado)
202n
Actualizar Objetos de Datos
202o
¿Procesados todos los elementos indicados en el Modelo Contenedor Seguro Recursivo?
FIN
211
Generador Resumen Criptográfico
Se genera el Contenedor Seguro Recursivo Virtual
FIN OK
115
207
208
209
Contenido Digital$_{CSR1}$
Huella Digital$_{CSR1}$
Lista de Claves Sin Contenedor Seguro Iterativo
Lista de Claves Con Contenedor Seguro Iterativo
OUTPUT: CONTENEDOR SEGURO RECURSIVO VIRTUAL

Figura 2

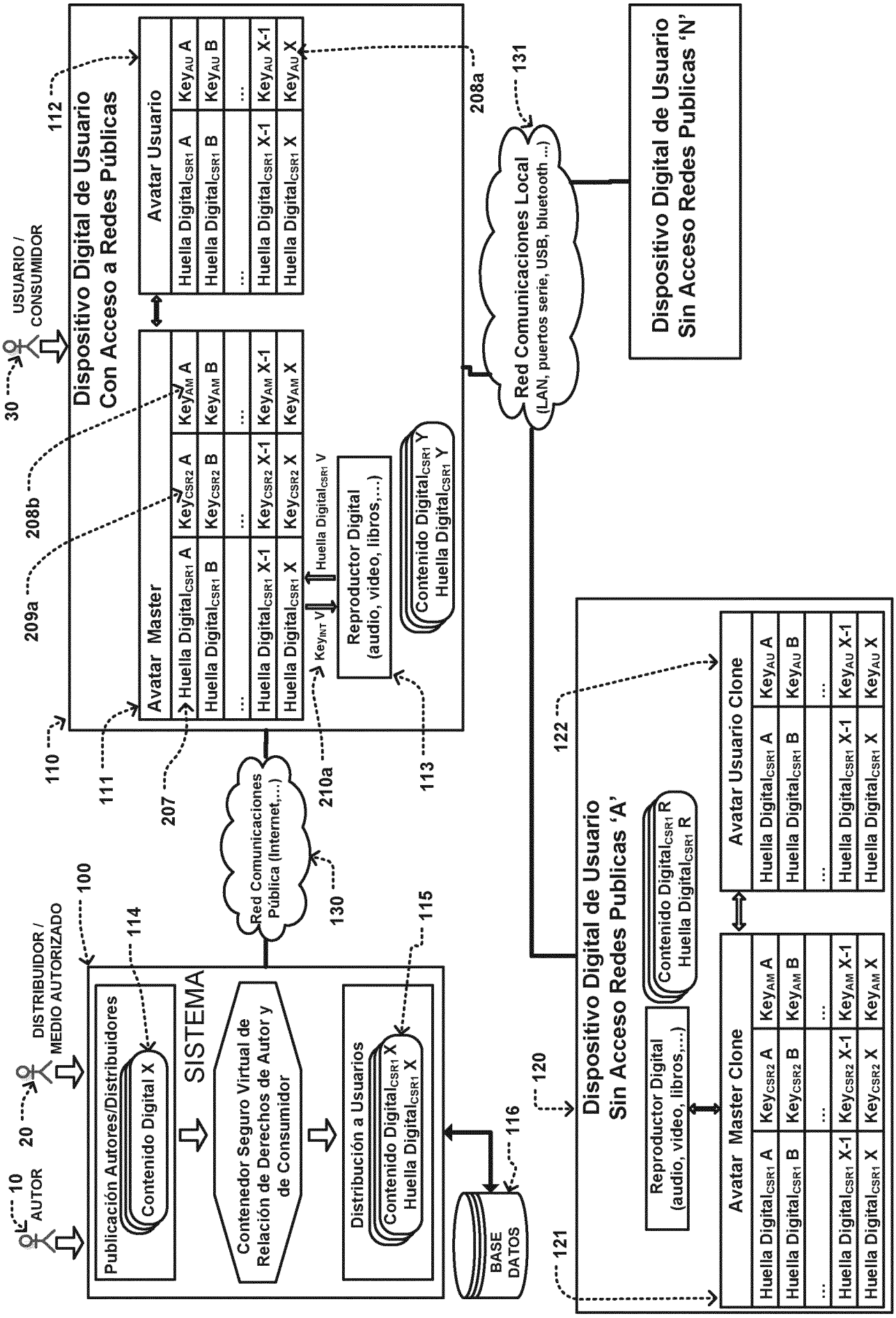

10
AUTOR
20
DISTRIBUIDOR / MEDIO AUTORIZADO
100
SISTEMA
Publicación Autores/Distribuidores
Contenido Digital X
114
Contenedor Seguro Virtual de Relación de Derechos de Autor y de Consumidor
Distribución a Usuarios
Contenido Digital$_{CSR1}$ X
Huella Digital$_{CSR1}$ X
115
BASE DATOS
116
Red Comunicaciones Pública (Internet,...)
130
210a
30
USUARIO / CONSUMIDOR
Dispositivo Digital de Usuario Con Acceso a Redes Públicas
110
112
Avatar Usuario
Avatar Master
Huella Digital$_{CSR1}$ A
Huella Digital$_{CSR1}$ B
Huella Digital$_{CSR1}$ X-1
Huella Digital$_{CSR1}$ X
Key$_{AU}$ A
Key$_{AU}$ B
Key$_{AU}$ X-1
Key$_{AU}$ X
Key$_{AM}$ A
Key$_{AM}$ B
Key$_{AM}$ X-1
Key$_{AM}$ X
Key$_{CSR2}$ A
Key$_{CSR2}$ B
Key$_{CSR2}$ X-1
Key$_{CSR2}$ X
111
207
209a
208b
Key$_{INT}$ V
Huella Digital$_{CSR1}$ V
Reproductor Digital (audio, video, libros,...)
113
Contenido Digital$_{CSR1}$ Y
Huella Digital$_{CSR1}$ Y
208a
131
Red Comunicaciones Local (LAN, puertos serie, USB, bluetooth ...)
Dispositivo Digital de Usuario Sin Acceso Redes Publicas 'N'
122
Avatar Usuario Clone
120
Dispositivo Digital de Usuario Sin Acceso Redes Publicas 'A'
Contenido Digital$_{CSR1}$ R
Huella Digital$_{CSR1}$ R
Reproductor Digital (audio, video, libros,...)
121
Avatar Master Clone

Figura 3

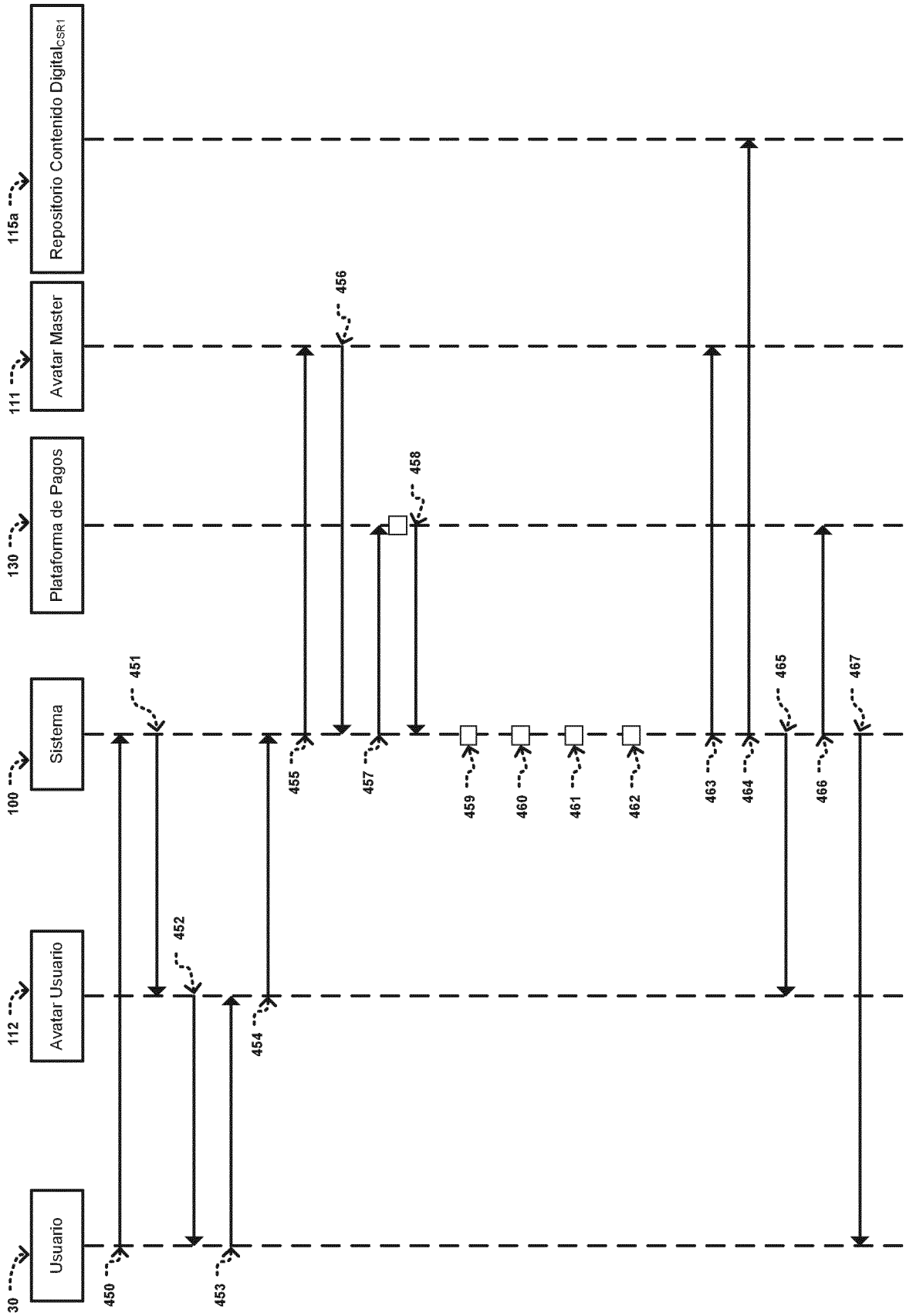

Repositorio Contenido Digital$_{CSR1}$
115a
Avatar Master
111
Plataforma de Pagos
130
Sistema
100
Avatar Usuario
112
Usuario
30
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467

Figura 4

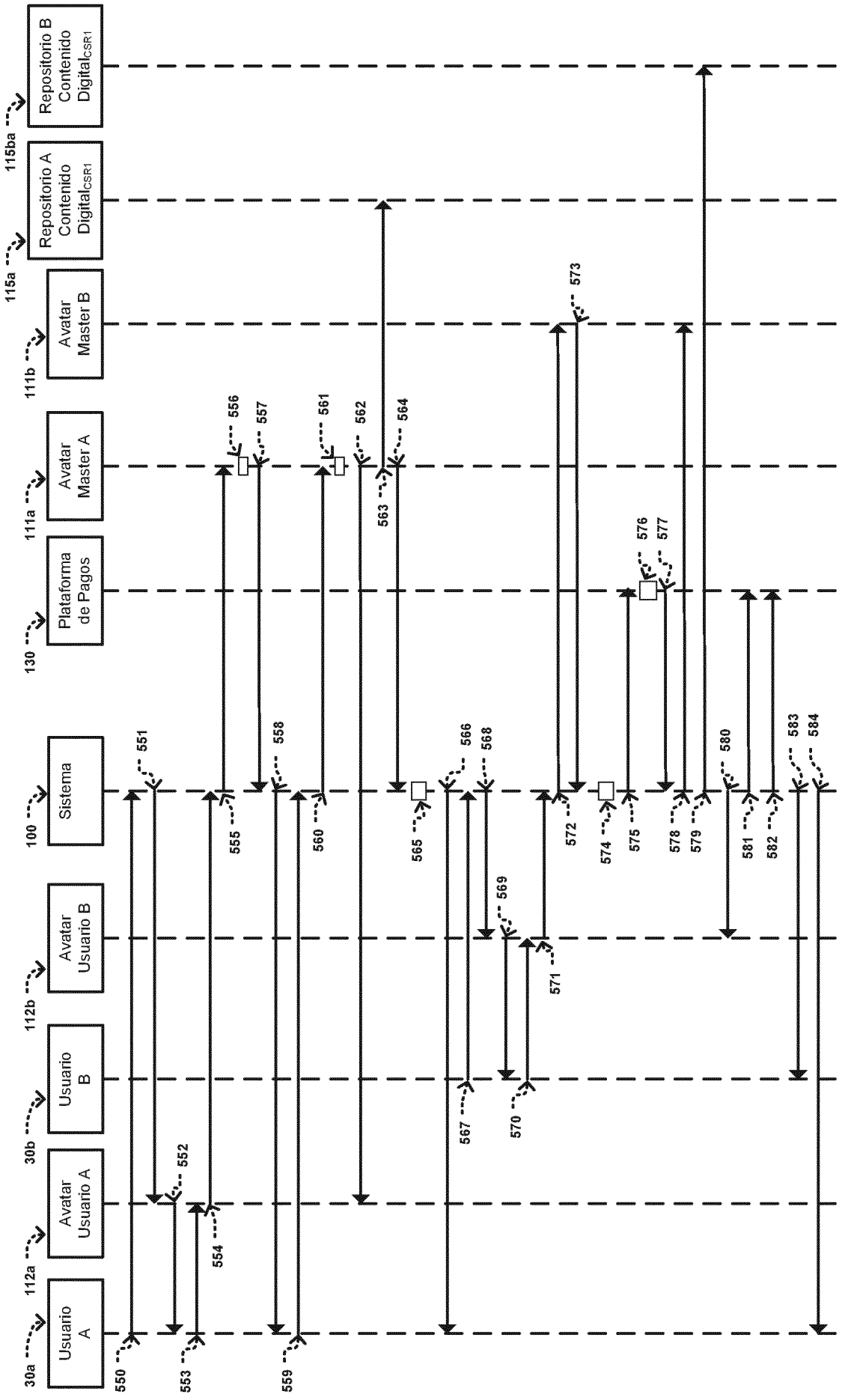

Usuario A
30a
112a
Avatar Usuario A
30b
Usuario B
112b
Avatar Usuario B
100
Sistema
130
Plataforma de Pagos
111a
Avatar Master A
111b
Avatar Master B
115a
Repositorio A Contenido Digital CSR1
115ba
Repositorio B Contenido Digital CSR1
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584

Figura 5

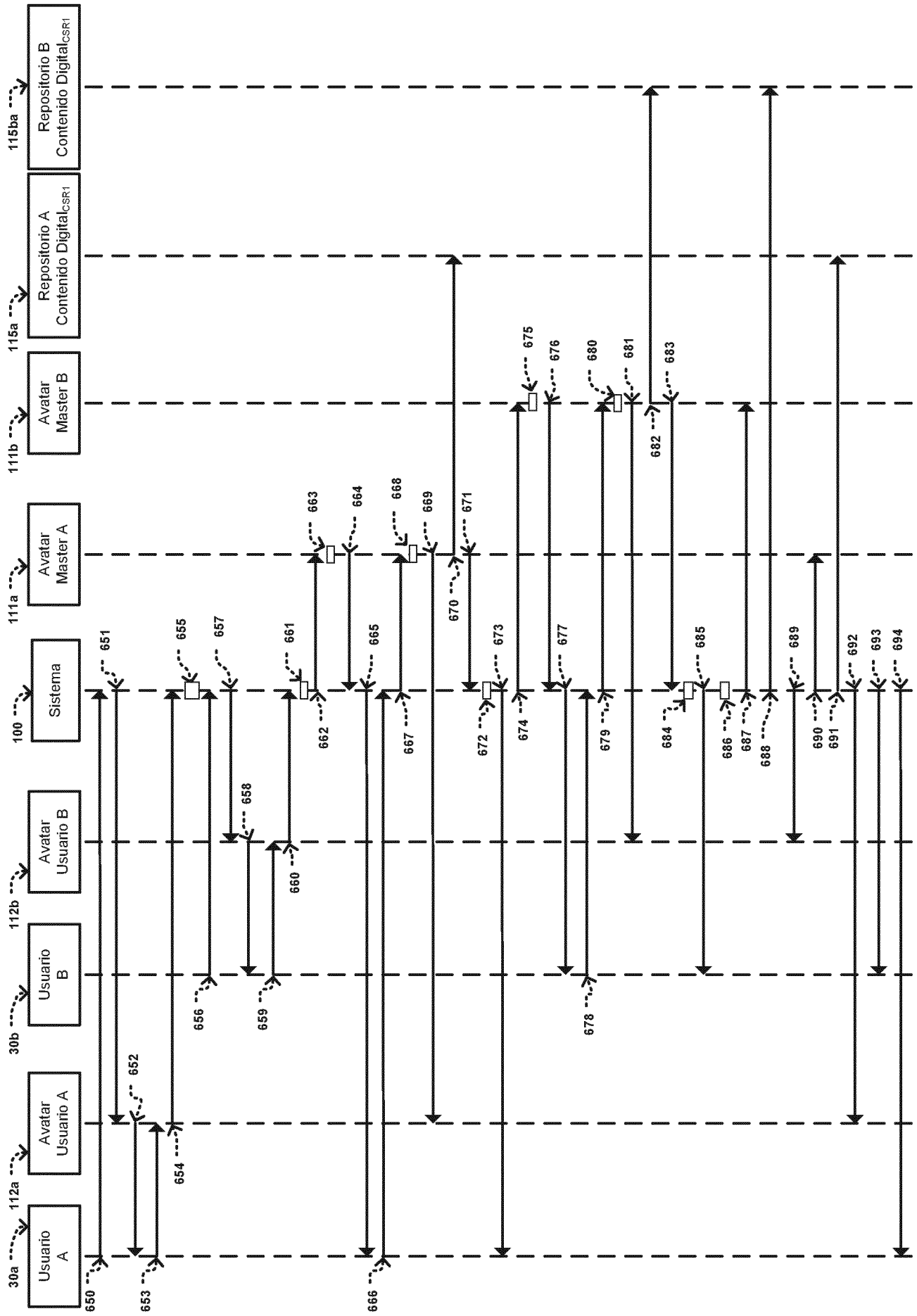

30a Usuario A
112a Avatar Usuario A
30b Usuario B
112b Avatar Usuario B
100 Sistema
111a Avatar Master A
111b Avatar Master B
115a Repositorio A Contenido Digital CSR1
115ba Repositorio B Contenido Digital CSR1
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694

Figura 6

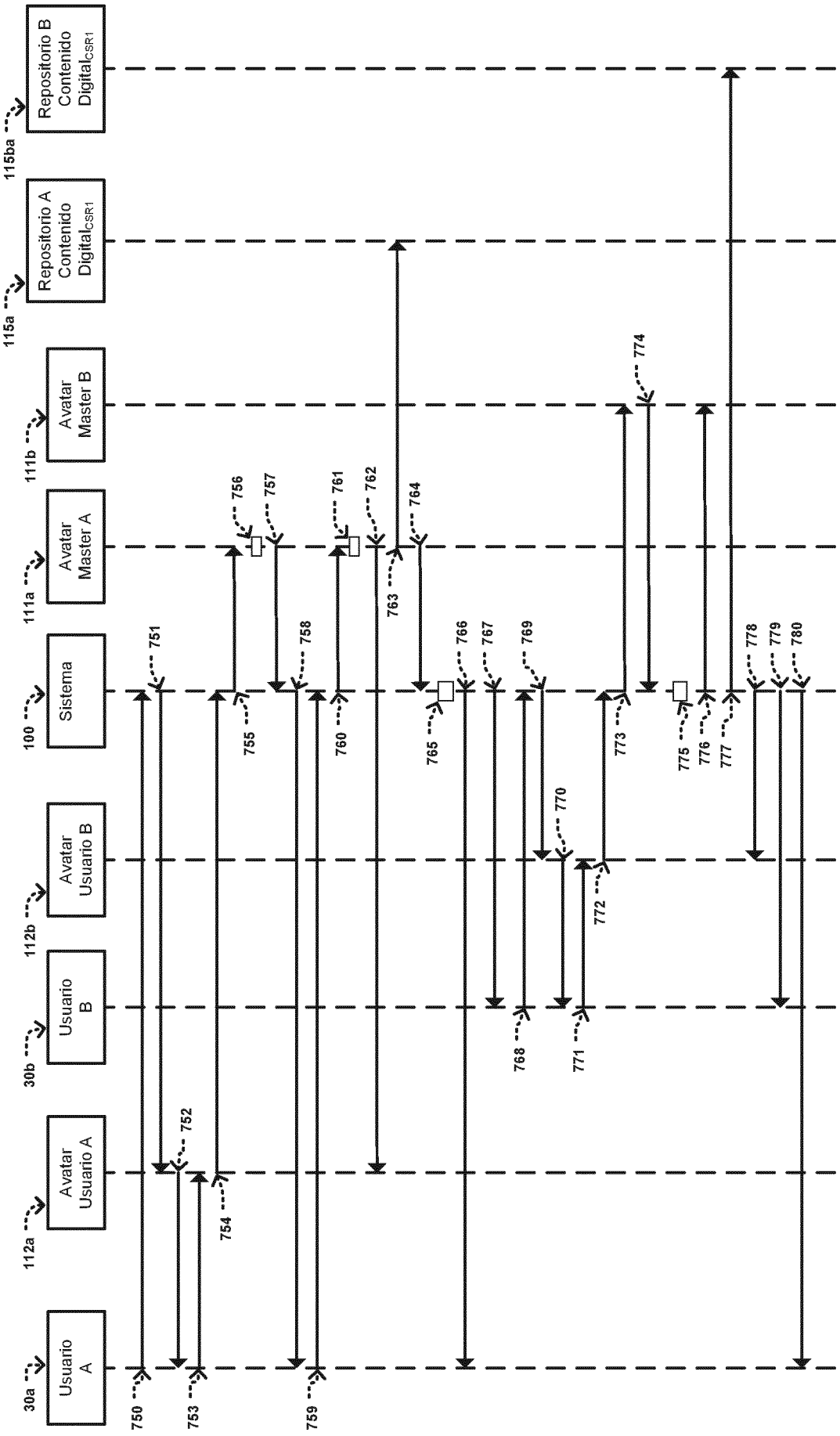

Usuario A
30a
Avatar Usuario A
112a
Usuario B
30b
Avatar Usuario B
112b
Sistema
100
Avatar Master A
111a
Avatar Master B
111b
Repositorio A Contenido Digital$_{CSR1}$
115a
Repositorio B Contenido Digital$_{CSR1}$
115ba
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780

Figura 7

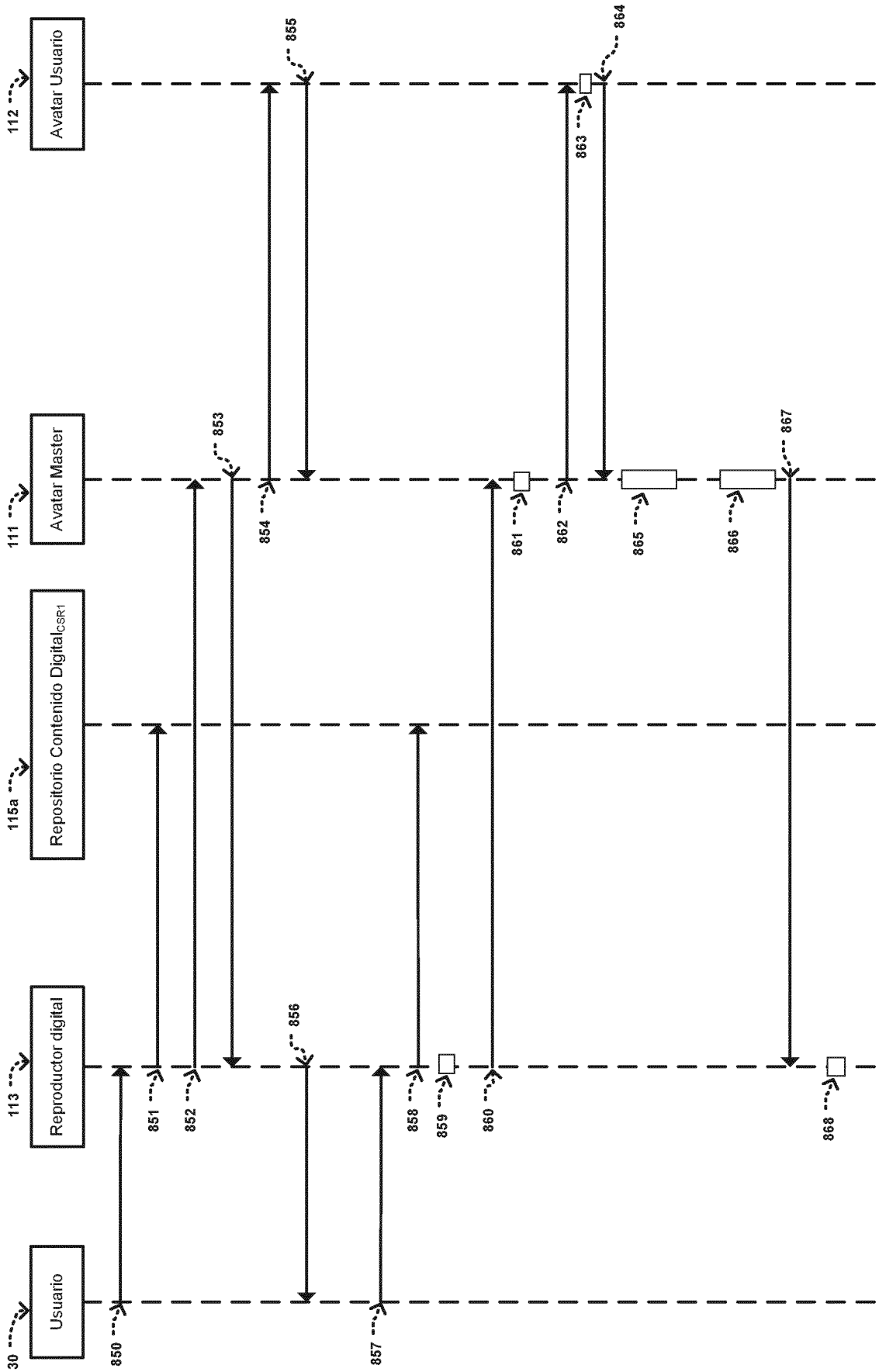

Avatar Usuario
112
Avatar Master
111
Repositorio Contenido Digital$_{CSR1}$
115a
Reproductor digital
113
Usuario
30
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868

Figura 8

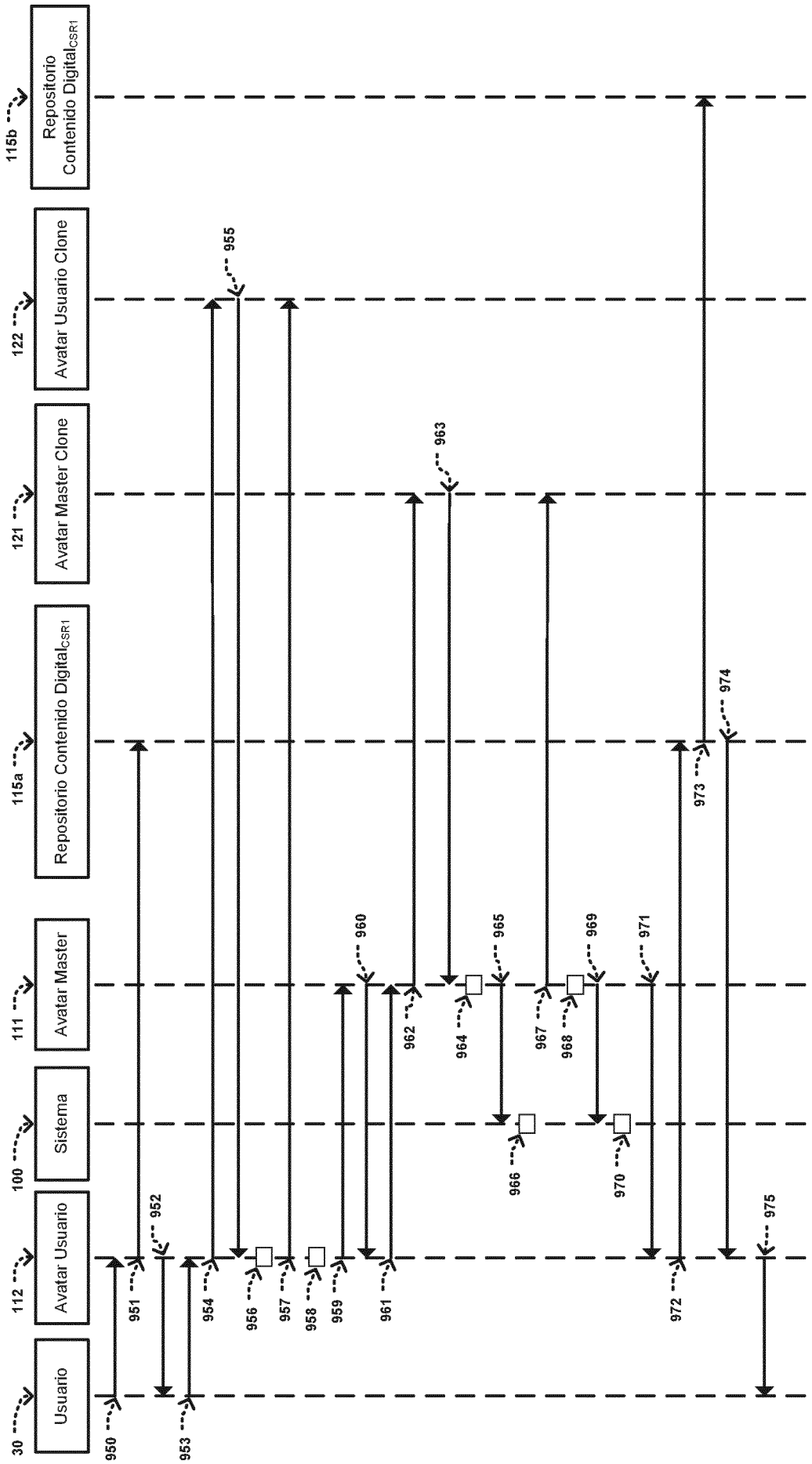

Usuario
Avatar Usuario
Sistema
Avatar Master
Repositorio Contenido Digital$_{CSR1}$
Avatar Master Clone
Avatar Usuario Clone
Repositorio Contenido Digital$_{CSR1}$
30
112
100
111
115a
121
122
115b
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975

Figura 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ES2012/070208

A. CLASSIFICATION OF SUBJECT MATTER

G06Q20/12 (2012.01)
H04L9/14 (2006.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, INVENES, WPI, XPI3E, XPIETF, XPESP, XPESP2, XPETSI, XPAIP, COMPDX, INSPEC, TDB, XPIEE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	6-3-2010, Yang Liu; Chi Zhang; PengZhou Zhang, "Design of a DRM System for Electronic Document Publication" Second International Workshop on Education Technology and Computer Science (ETCS), 2010; págs. 311 - 314; ISBN 978-1-4244-6388-6 ; ISBN 1-4244-6388-2	1, 23
A	WO WO2005093989 A1 (SMART INTERNET TECHNOLOGY) 6-10-2005,	1, 23
A	US 2011161680 A1 (CLEVERSAFE) 30-6-2011,	1,23

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance.
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure use, exhibition, or other means.
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other documents , such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12/12/2012	**(17/12/2012)**
Name and mailing address of the ISA/ OFICINA ESPAÑOLA DE PATENTES Y MARCAS Paseo de la Castellana, 75 - 28071 Madrid (España) Facsimile No.: 91 349 53 04	Authorized officer M. Muñoz Sanchez Telephone No. 91 3495349

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/ES2012/070208

Patent document cited in the search report	Publication date	Patent family member(s)	Publication date
US2011161680 A	30.06.2011	NONE	
WO2005093989 A	06.10.2005	AU2005226064 A	06.10.2005
		EP1735939 A	27.12.2006
		EP20050714318	29.03.2005
		CN101002421 A	18.07.2007
		US2007219917 A	20.09.2007
		JP2007531127 A	01.11.2007

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº
PCT/ES2012/070208

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD
G06Q20/12 (2012.01)
H04L9/14 (2006.01)
De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)
G06Q, H04L

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)
EPODOC, INVENES, WPI, XPI3E, XPIETF, XPESP, XPESP2, XPETSI, XPAIP, COMPDX, INSPEC, TDB, XPIEE

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
A	Yang Liu; Chi Zhang; PengZhou Zhang, "Design of a DRM System for Electronic Document Publication" Second International Workshop on Education Technology and Computer Science (ETCS), 2010; págs. 311 - 314; 6-3-2010; ISBN 978-1-4244-6388-6 ; ISBN 1-4244-6388-2	1, 23
A	WO WO2005093989 A1 (SMART INTERNET TECHNOLOGY) 6-10-2005,	1, 23
A	US 2011161680 A1 (CLEVERSAFE) 30-6-2011,	1,23

☐ En la continuación del recuadro C se relacionan otros documentos ☒ Los documentos de familias de patentes se indican en el anexo

* Categorías especiales de documentos citados:
"A" documento que define el estado general de la técnica no considerado como particularmente relevante.
"E" solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.
"L" documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada).
"O" documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio.
"P" documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.
"T" documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención.
"X" documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.
"Y" documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.
"&" documento que forma parte de la misma familia de patentes.

Fecha en que se ha concluido efectivamente la búsqueda internacional.	Fecha de expedición del informe de búsqueda internacional.
12/12/2012	**17 de diciembre de 2012 (17/12/2012)**
Nombre y dirección postal de la Administración encargada de la búsqueda internacional OFICINA ESPAÑOLA DE PATENTES Y MARCAS Paseo de la Castellana, 75 - 28071 Madrid (España) Nº de fax: 91 349 53 04	Funcionario autorizado M. Muñoz Sanchez Nº de teléfono 91 3495349

INFORME DE BÚSQUEDA INTERNACIONAL

Informaciones relativas a los miembros de familias de patentes

Solicitud internacional nº

PCT/ES2012/070208

Documento de patente citado en el informe de búsqueda	Fecha de Publicación	Miembro(s) de la familia de patentes	Fecha de Publicación
US2011161680 A	30.06.2011	NINGUNO	
WO2005093989 A	06.10.2005	AU2005226064 A	06.10.2005
		EP1735939 A	27.12.2006
		EP20050714318	29.03.2005
		CN101002421 A	18.07.2007
		US2007219917 A	20.09.2007
		JP2007531127 A	01.11.2007