(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 635 121**

(51) Int. CI.:

G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.01.2006 E 06100016 (2)**

(97) Fecha y número de publicación de la concesión europea: **03.05.2017 EP 1686504**

(54) Título: **Arquitectura flexible de concesión de licencia en sistemas de gestión de derechos de contenido**

(30) Prioridad:

01.02.2005 US 48087

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.10.2017

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

DEMELLO, MARCO A.;
PARAMASIVAM, MUTHUKRISHNAN;
WAXMAN, PETER D.;
PANDYA, RAVINDRA N.;
BOURNE, STEVEN y
KRISHNASWAMY, VINAY

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

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

DESCRIPCIÓN

Arquitectura flexible de concesión de licencia en sistemas de gestión de derechos de contenido

Campo técnico

La presente invención se refiere a un sistema de gestión de derechos (RM, *rights management*) por medio del cual se proporciona acceso a un contenido digital solo de acuerdo con una licencia digital correspondiente. Más en concreto, la presente invención se refiere a una arquitectura particular de concesión de licencia empleada en relación con dicho sistema de RM, por medio del cual cada licencia puede estar vinculada a una o más autoridades de confianza de raíz y cada licencia puede comprender, en realidad, una pluralidad de documentos de licencia.

Antecedentes de la invención

La gestión de derechos y su cumplimiento es altamente deseable en relación con el contenido digital, tal como audio digital, vídeo digital, texto digital, datos digitales y multimedia digital, etc., en donde dicho contenido digital vaya a ser distribuido a uno o más usuarios. El contenido digital podría ser estático, tal como un documento de texto, por ejemplo, o se podría transmitir por secuencias, tal como el audio / vídeo transmitido por secuencias de un evento en directo. Los modos de distribución típicos incluyen dispositivos tangibles, tales como discos magnéticos (flexibles), una cinta magnética, un disco óptico (compacto) (CD, *compact disc*), etc., y medios intangibles, tales como un tablón electrónico de anuncios, una red electrónica, Internet, etc. Tras ser recibido por el usuario, dicho usuario presenta el contenido digital con la ayuda del software de presentación apropiado, tal como un reproductor de audio, un reproductor de texto, etc., en un ordenador personal u otro hardware.

En un escenario, un propietario de contenido o un propietario de derechos, tal como un autor, un publicador, un difusor, etc., desea distribuir dicho contenido digital a cada uno de dichos usuarios o destinatarios a cambio de un precio de licencia o alguna otra consideración. Entonces, en dicho escenario, el contenido puede ser una grabación de audio, una presentación multimedia, etc. y el fin de la distribución es generar el precio de licencia. Dicho propietario del contenido, si se le presenta la oportunidad, probablemente desee restringir qué puede hacer el usuario con dicho contenido digital. Por ejemplo, al propietario de contenido le gustaría restringir que el usuario copiara y volviera a distribuir dicho contenido a un segundo usuario, al menos de una manera que niegue al propietario del contenido un precio de licencia de dicho segundo usuario.

Además, el propietario del contenido puede desear proporcionar al usuario la flexibilidad para contar con diferentes tipos de licencias de uso a diferentes precios de licencia, mientras que al mismo tiempo se hace que el usuario se atenga a los términos de cualquier tipo de licencia que se compre en la práctica. Por ejemplo, el propietario del contenido puede desear permitir que el contenido digital distribuido sea presentado solo un número limitado de veces, solo por un cierto tiempo total, solo en un cierto tipo de máquina, solo en un cierto tipo de plataforma de presentación, solo por un cierto tipo de usuario, etc.

En otro escenario, un desarrollador de contenido, tal como un empleado o miembro de una organización, desea distribuir dicho contenido digital a otros uno o más empleados o miembros de la organización o a otras personas fuera de la organización, pero le gustaría evitar la presentación del contenido por parte de otras personas. En este caso, la distribución del contenido es más semejante a una compartición de contenido basada en la organización, de una manera confidencial o restringida, en contraposición a una distribución generalizada a cambio de un precio de licencia o alguna otra consideración.

Entonces, en dicho escenario, el contenido puede ser una presentación de documento, hoja de cálculo, base de datos, correo electrónico o similar, de tal modo que pueda ser intercambiado dentro de un entorno de oficina y el desarrollador de contenido puede desear asegurar que el contenido permanece dentro de la organización o entorno de oficina y que no sea presentado por individuos no autorizados tales como, por ejemplo, competidores o adversarios. Una vez más, dicho desarrollador de contenido desea restringir lo que puede hacer un destinatario con dicho contenido digital distribuido. Por ejemplo, al propietario del contenido le gustaría restringir la copia o la redistribución de dicho contenido por parte del usuario a un segundo usuario, al menos de una manera que exponga el contenido fuera de los límites de las personas a las que se ha de permitir presentar el contenido.

Además, el desarrollador de contenido puede desear proporcionar a diversos destinatarios diferentes niveles de derechos de presentación. Por ejemplo, el desarrollador de contenido puede desear permitir que el contenido digital protegido se pueda ver y no se pueda imprimir con respecto a una clase de individuos, y que se pueda ver e imprimir con respecto a otra clase de individuos.

No obstante, en cualquier escenario, después de que haya tenido lugar la distribución, dicho propietario / desarrollador de contenido tiene muy poco o ningún control sobre el contenido digital. Esto es especialmente problemático a la vista del hecho de que prácticamente todos los ordenadores personales incluyen el hardware y el software necesarios para hacer una copia digital exacta de dicho contenido digital y descargar dicha copia digital exacta a un disco magnético u óptico grabable, o enviar dicha copia digital exacta a través de una red, tal como Internet, a cualquier destino.

Por supuesto, como parte de una transacción en la que se distribuye el contenido, el propietario / desarrollador de contenido puede requerir que el usuario / destinatario del contenido digital prometa no redistribuir dicho contenido digital de una manera no deseada. No obstante, dicha promesa es fácil de hacer y de romper. Un propietario / desarrollador de contenido puede intentar evitar la redistribución a través de cualquiera de los diversos dispositivos de seguridad conocidos, que por lo general comprenden el cifrado y el descifrado. No obstante, es probable que sea muy poco lo que evita que un usuario medianamente determinado descifre y cifre el contenido digital, y que guarde dicho contenido digital en una forma no cifrada y, entonces, redistribuya el mismo.

Por lo tanto, se han proporcionado unas arquitecturas y procedimientos de RM y de cumplimiento para permitir la presentación controlada de formas arbitrarias de un contenido digital, en el que dicho control es flexible y puede ser definido por el propietario / desarrollador de contenido digital. Dichas arquitecturas permiten y facilitan dicha presentación controlada en cualquier escenario tal como se ha expuesto en lo que antecede.

Por lo general, una licencia digital está vinculada a una autoridad de confianza de raíz global o casi global, por ejemplo, por medio de una cadena de certificados digitales y, por lo tanto, cualquier entidad que desee autenticar / verificar dicha licencia ha de estar en posesión de la información apropiada en relación con dicha autoridad de confianza de raíz. No obstante, y tal como se podrá apreciar, pueden tener lugar situaciones en las que una entidad, sin que sea su culpa, no se encuentre, de hecho, en posesión de dicha información apropiada y que, por lo tanto, no pueda autenticar / verificar en consecuencia la licencia. Por poner un ejemplo, la información se puede cambiar desde la recepción de una copia por parte de la entidad. En otro ejemplo, la autoridad de confianza de raíz puede haber cambiado.

En cualquiera de estos ejemplos, ha de ser evidente que hacer que la entidad dependa de cualquier autoridad de confianza de raíz particular sin considerar ninguna otra autoridad de confianza de raíz plantea muchos riesgos. En esencia, la entidad siempre depende de la autoridad de confianza de raíz particular y la información de la misma, aún cuando existan o vayan a existir otras autoridades de confianza de raíz, y aún si deja de existir la autoridad de confianza de raíz particular.

Por consiguiente, existe la necesidad de una arquitectura más flexible para definir las licencias digitales y el funcionamiento de las mismas. En particular, existe una necesidad de dicha arquitectura que prevea múltiples autoridades de confianza de raíz y que permita que una licencia especifique por sí misma cada autoridad de confianza de raíz que se pueda emplear para autenticar / verificar la misma. Además, para efectuar dicha arquitectura, existe una necesidad de un nuevo tipo de licencia que comprenda una pluralidad de documentos de licencia.

El documento US 2003 / 187801 desvela una revocación de contenido y modificación de licencia en un sistema de DRM y en un dispositivo informático. La licencia incluye una licencia de derechos digitales, una clave de descifrado, una forma digital procedente del servidor de licencia y un certificado que el servidor de licencia obtuvo previamente del servidor de contenido, indicando tal certificado que el servidor de licencia tiene la autoridad procedente del servidor de contenido para emitir la licencia.

Con la presentación del contenido, basándose en el certificado procedente de la licencia, la caja negra aplica la clave pública de servidor de contenido de reciente obtención para satisfacer su propia necesidad de que el certificado sea válido, lo que quiere decir que el servidor de licencia que emitió la licencia tenía la autoridad procedente del servidor de contenido para obrar de este modo.

Sumario de la invención

Las necesidades que se han mencionado en lo que antecede se satisfacen, al menos en parte, por medio de la presente invención en la que la licencia digital autoriza la presentación de un fragmento correspondiente de contenido digital en un dispositivo informático y en la que el contenido está en una forma cifrada y se puede descifrar de acuerdo con una clave de descifrado (KD). La licencia se emite a un usuario y tiene una porción de descifrado y una porción de autorización.

A la porción de descifrado solo accede el usuario a quien se emite la licencia y tiene la clave de descifrado (KD) y la validación de la información incluye una identificación de una autoridad de confianza de raíz. La porción de autorización expone derechos concedidos en relación con el contenido digital y unas condiciones que se han de satisfacer para ejercer los derechos concedidos y tiene una firma digital que se valida de acuerdo con la autoridad de confianza de raíz identificada en la porción de descifrado.

El usuario a quien se emite la licencia accede a la porción de descifrado y emplea la información de validación en la misma para validar la firma digital de la porción de autorización. Dicho usuario ejerce los derechos en la porción de autorización solo si las condiciones de la porción de autorización así lo permiten. Los derechos son ejercidos mediante el descifrado del contenido cifrado con la clave de descifrado (KD) de la porción de descifrado y mediante la presentación del contenido descifrado. Cabe destacar que no es necesario que la licencia esté vinculada a autoridad de confianza de raíz particular alguna.

Breve descripción de los dibujos

El sumario anterior, así como la siguiente descripción detallada de las realizaciones de la presente invención, se entenderán mejor cuando se lean junto con los dibujos adjuntos. Para fines de ilustración de la presente invención, en los dibujos se muestran unas realizaciones que son las actualmente preferidas. No obstante, se ha de entender que la presente invención no se limita a las disposiciones y a los medios precisos que se muestran. En los dibujos:

la figura 1 es un diagrama de bloques que representa un entorno informático no limitante a modo de ejemplo en el que se puede implementar la presente invención;
la figura 2 es un diagrama de bloques que representa un entorno de red a modo de ejemplo que tiene una diversidad de dispositivos informáticos en los cuales se puede implementar la presente invención;
la figura 3 es un diagrama de bloques que muestra una arquitectura de cumplimiento de un ejemplo de un sistema basado en confianza, incluyendo una licencia digital de acuerdo con una realización de la presente invención;
la figura 4 es un diagrama de bloques que muestra la licencia de la figura 3 con mayor detalle y que incluye una porción de autorización y una porción de descifrado de acuerdo con una realización de la presente invención;
la figura 5 es un diagrama de flujo que muestra unas etapas clave que se realizan durante la emisión de la licencia de las figuras 3 y 4 de acuerdo con una realización de la presente invención; y
la figura 6 es un diagrama de flujo que muestra unas etapas clave que se realizan cuando se emplea la licencia de las figuras 3 y 4 para presentar un contenido de acuerdo con una realización de la presente invención.

Descripción detallada de la invención

ENTORNO INFORMÁTICO

La figura 1 y la explicación siguiente pretenden proporcionar una descripción general breve de un entorno informático adecuado en el que se puede implementar la presente invención. No obstante, se ha de entender que está contemplado el uso de dispositivos informáticos portátiles, de mano y de otro tipo en relación con la presente invención. A pesar de que a continuación se describe un ordenador de uso general, esto no es sino un ejemplo y la presente invención describe solo un cliente fino que tenga una interoperabilidad e interacción de servidor de red. Por lo tanto, la presente invención se puede implementar en un entorno de servicios alojados en red en los que están cifrados muy pocos recursos de cliente, o una cantidad mínima de los mismos, por ejemplo, un entorno de red en el que el dispositivo de cliente sirve únicamente como un buscador o interfaz para la Red Mundial (World Wide Web).

A pesar de que no se requiere, la presente invención se puede implementar por medio de una interfaz de programación de aplicaciones (API, *application programming interface*), para ser usada por un desarrollador y / o incluida dentro del software de búsqueda de la red que se describirá en el contexto general de las instrucciones ejecutables por ordenador, tales como módulos de programa, que están siendo ejecutados por uno o más ordenadores, tales como estaciones de trabajo de cliente, servidores u otros dispositivos. Por lo general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos y similares que realizan tareas particulares e implementan tipos de datos abstractos particulares. Por lo general, la funcionalidad de los módulos de programa puede ser combinada o distribuida según se desee en diversas realizaciones. Además, los expertos en la materia apreciarán que la presente invención se puede poner en práctica con otras configuraciones del sistema informático. Otros entornos, configuraciones y / o sistemas informáticos bien conocidos, que pueden ser adecuados para su uso con la presente invención, incluyen, pero no se limitan a, ordenadores personales (PC, *personal computer*), cajeros automáticos, ordenadores de servidor y ordenadores de mano o portátiles, sistemas de multiprocesadores, sistemas basados en microprocesadores, electrónica de consumo programable, PC de red, miniordenadores, ordenadores de gran sistema y similares. La presente invención también se puede poner en práctica en entornos informáticos distribuidos, en los que las tareas son realizadas por dispositivos de procesamiento remotos que están vinculados a través de una red de comunicaciones u otro medio de transmisión de datos. En un entorno informático distribuido, los módulos de programa pueden estar ubicados en unos medios de almacenamiento informático tanto locales como remotos, incluyendo dispositivos de almacenamiento en memoria.

Por lo tanto, la figura 1 ilustra un ejemplo de un entorno de sistema informático 100 adecuado en el que se puede implementar la presente invención, a pesar de que, tal como se ha puesto de manifiesto en lo que antecede, el entorno de sistema informático 100 solo es un ejemplo de un entorno informático adecuado y no pretende sugerir limitación alguna en lo que respecta al alcance de uso o la funcionalidad de la presente invención. Tampoco se ha de interpretar el entorno informático 100 como que tiene dependencia o requisito alguno relacionado con cualquiera o una combinación de componentes ilustrados en el entorno operativo 100 a modo de ejemplo.

Haciendo referencia a la figura 1, un sistema a modo de ejemplo para implementar la presente invención incluye un dispositivo informático de uso general en la forma de un ordenador 110. Los componentes del ordenador 110 pueden incluir, pero no se limitan a, una unidad de procesamiento 120, una memoria de sistema 130 y un bus de sistema 121 que conecta diversos componentes de sistema, incluyendo la memoria de sistema para la unidad de procesamiento 120. El bus de sistema 121 puede ser cualquiera de diversos tipos de estructuras de bus, incluyendo un bus de memoria o controlador de memoria, un bus de periféricos y un bus local usando cualquiera de una diversidad de arquitecturas de bus. A modo de ejemplo, y no de limitación, tales arquitecturas incluyen el bus de

Arquitectura Estándar de la Industria (ISA, *Industry Standard Architecture*), el bus de Arquitectura de Microcanal (MCA, *Micro Channel Architecture*), el bus de ISA Potenciada (EISA, *Enhanced ISA*), el bus local de la Asociación para Estándares Electrónicos y de Vídeo (VESA, *Video Electronics Standards Association*) y el bus de Interconexión de Componentes Periféricos (PCI, *Peripheral Component Interconnect*), que también se conoce como bus *Mezzanine* (entresuelo).

El ordenador 110 incluye, por lo general, una diversidad de medios legibles por ordenador. Los medios legibles por ordenador pueden ser cualesquiera medios disponibles a los que se pueda acceder por medio del ordenador 110, e incluyen unos medios tanto volátiles como no volátiles, extraíbles y no extraíbles. A modo de ejemplo y no de limitación, los medios legibles por ordenador pueden comprender medios de almacenamiento informático y medios de comunicación. Los medios de almacenamiento informático incluyen unos medios tanto volátiles como no volátiles, extraíbles y no extraíbles implementados en cualquier procedimiento o tecnología para el almacenamiento de información, tales como instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. Los medios de almacenamiento informático incluyen, pero no se limitan a, RAM, ROM, EEPROM, flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD, *digital versatile disk*) u otro almacenamiento de disco óptico, casetes magnéticos, cintas magnéticas, almacenamientos de disco magnético u otros dispositivos de almacenamiento magnético o cualquier otro medio que pueda ser usado para almacenar la información deseada y al cual se pueda acceder por medio del ordenador 110. Los medios de comunicación incorporan, por lo general, instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada, tal como una onda portadora u otro mecanismo de transporte e incluyen cualquier medio de entrega de información. La expresión “señal de datos modulada” quiere decir una señal que tiene una o más de sus características ajustadas o cambiadas de un modo tal como para codificar la información de la señal. A modo de ejemplo y no de limitación, los medios de comunicación incluyen medios cableados, tales como una red cableada o una conexión cableada directa, y medios inalámbricos, tales como medios acústicos, RF, infrarrojos y otros medios inalámbricos. Las combinaciones de cualquiera de los anteriores han de quedar incluidas dentro del alcance de los medios legibles por ordenador.

La memoria de sistema 130 incluye unos medios de almacenamiento informático en la forma de una memoria volátil y / o no volátil, tal como una memoria solo de lectura (ROM, *read only memory*) 131 y una memoria de acceso aleatorio (RAM, *random access memory*) 132. Un sistema básico de entrada / salida 133 (BIOS, *basic input / output system*), que contiene las rutinas básicas que ayudan a transferir información entre los elementos dentro del ordenador 110, tales como durante el arranque, por lo general es almacenado en la ROM 131. La RAM 132 contiene, por lo general, datos y / o módulos de programa a los que se puede acceder inmediatamente y / o sobre los que se puede estar operando en la actualidad por medio de la unidad de procesamiento 120. A modo de ejemplo y no de limitación, la figura 1 ilustra el sistema operativo 134, los programas de aplicación 135, otros módulos de programa 136 y los datos de programa 137.

El ordenador 110 también puede incluir otros medios de almacenamiento informático extraíbles / no extraíbles y volátiles / no volátiles. Solo a modo de ejemplo, la figura 1 ilustra una unidad de disco duro 141 que lee o escribe en unos medios magnéticos no extraíbles no volátiles, una unidad de disco magnético 151 que lee o escribe en un disco magnético extraíble no volátil 152, y una unidad de disco óptico 155 que lee o escribe en un disco óptico extraíble / volátil 156, tal como un CD-ROM u otros medios ópticos. Otros medios de almacenamiento informático extraíbles / no extraíbles y volátiles / no volátiles que se pueden usar en el sistema operativo a modo de ejemplo incluyen, pero no se limitan a, casetes de cinta magnética, tarjetas de memoria flash, discos versátiles digitales, cintas digitales de vídeo, RAM de estado sólido, memorias ROM de estado sólido, y similares. La unidad de disco duro 141, por lo general, se conecta al bus de sistema 121 a través de una interfaz de memoria no extraíble tal como la interfaz 140 y la unidad de disco magnético 151 y la unidad de disco óptico 155, por lo general, se conectan al bus de sistema 121 por una interfaz de memoria extraíble, tal como la interfaz 150.

Las unidades y sus medios de almacenamiento informático asociados que se han descrito en lo que antecede y que se ilustran en la figura 1 proporcionan el almacenamiento de instrucciones legibles por ordenador, estructuras de datos, módulos del programa y otros datos para el ordenador 110. Por ejemplo, en la figura 1 la unidad de disco duro 141 se ilustra como el sistema operativo de almacenamiento 144, los programas de aplicación 145, otros módulos de programa 146 y los datos de programa 147. Obsérvese que todos estos componentes pueden ser, o bien directamente o bien el mismo que o bien diferentes del sistema operativo 134, los programas de aplicación 135, otros módulos de programa 136 y los datos de programa 137. El sistema operativo 144, los programas de aplicación 145, otros módulos de programa 146 y los datos de programa 147 tienen números diferentes en las figuras para ilustrar que, como mínimo, son copias diferentes. Un usuario puede introducir comandos e información en el ordenador 110 a través de los dispositivos de entrada, tal como un teclado 162 y un dispositivo apuntador 161, al que se hace referencia comúnmente como ratón, una bola de seguimiento o una almohadilla táctil. Otros dispositivos de entrada (que no se muestran) pueden incluir un micrófono, una palanca de control, un controlador para juegos, una antena parabólica, un escáner o similares. Estos y otros dispositivos de entrada con frecuencia se conectan a la unidad de procesamiento 120 a través de una interfaz de entrada del usuario 160 que está conectada al bus de sistema 121, pero puede estar conectada por otra interfaz y estructuras del bus, tal como un puerto paralelo, un puerto de juegos, o un bus serie universal (USB, *universal serial bus*).

Un monitor 191 u otro tipo de dispositivo de pantalla también está conectado al bus de sistema 121 por medio de una interfaz, tal como una interfaz de vídeo 190. Una interfaz de gráficos 182, tal como una interfaz Northbridge, también puede ser conectada al bus de sistema 121. La interfaz Northbridge es un conjunto de chips que se comunica con la CPU, o la unidad de procesamiento central 120 y asume la responsabilidad de las comunicaciones del puerto acelerado de gráficos (AGP, *accelerated graphics port*). Una o más unidades de procesamiento de gráficos (GPU, *graphics processing unit*) 184 se pueden comunicar con la interfaz de gráficos 182. En este aspecto, las GPU 184 incluyen, por lo general, almacenamiento en memoria en chip, tales como almacenamientos de registro y las GPU 184 se comunican con una memoria de vídeo 186. No obstante, las CPU 184 no son sino un ejemplo de un coprocesador y, por lo tanto, se puede incluir una diversidad de dispositivos de coprocesamiento en el ordenador 110. Un monitor 191 u otro tipo de dispositivo de pantalla también está conectado al bus de sistema 121 por medio de una interfaz, tal como la interfaz de vídeo 190, la cual puede, a la vez, comunicarse con la memoria de vídeo 186. Además del monitor 191 los ordenadores también pueden incluir otros dispositivos periféricos de salida, tales como unos altavoces 197 y una impresora 196, que pueden estar conectados a través de una interfaz de periféricos de salida 195.

El ordenador 110 puede operar en un entorno de red usando conexiones lógicas a uno o más ordenadores remotos, tales como el ordenador remoto 180. El ordenador remoto 180 puede ser un ordenador personal, un servidor, un enrutador, una PC de red, un dispositivo del mismo nivel u otro nodo de red común, que por lo general incluye muchos o todos los elementos que se han descrito en lo que antecede en relación con el ordenador 110, a pesar de que solo se ilustra un dispositivo de almacenamiento en memoria 181 en la figura 1. Las conexiones lógicas ilustradas en la figura 1 incluyen una red de área local (LAN, *local area network*) 171 y una red de área amplia (WAN, *wide area network*) 173, pero también pueden incluir otras redes. Dichos entornos de red son un lugar común en las oficinas, redes informáticas empresariales, intranets y Internet.

Cuando se usa en un entorno de red LAN, el ordenador 110 está conectado a la red LAN 171 a través de una interfaz o adaptador de red 170. Cuando se usa en un entorno de red WAN, el ordenador 110 por lo general incluye un módem 172 u otros medios para establecer comunicaciones por la red WAN 173, tal como Internet. El módem 172, que puede ser interno o externo, puede ser conectado al bus de sistema 121 por medio de la interfaz de entrada del usuario 160 u otro mecanismo apropiado. En un entorno de red, los módulos de programa ilustrados en relación con el ordenador 110 o porciones de los mismos pueden almacenados en un dispositivo de almacenamiento en memoria remota. A modo de ejemplo y no de limitación, la figura 1 ilustra programas de aplicación remotos 185 como que residen en un dispositivo de memoria 181. Se ha de apreciar que las conexiones de red que se muestran son a modo de ejemplo y que se pueden usar también cualesquiera otros medios para establecer un enlace de comunicaciones entre los ordenadores.

Un experto en la materia podrá apreciar que un ordenador 110 u otro dispositivo de cliente se puede emplear como parte de una red informática. En este aspecto, la presente invención se refiere a cualquier sistema informático que tenga cualquier número de unidades de almacenamiento en memoria y cualquier número de aplicaciones y procedimientos que tienen lugar en cualquier número de unidades o volúmenes de almacenamiento. La presente invención se puede aplicar a un entorno con ordenadores de servidor y ordenadores de cliente que estén desplegados en un entorno de red, que tenga almacenamiento remoto o local. La presente invención también puede ser aplicada a un sistema informático independiente que tenga una funcionalidad de lenguaje de programación y capacidades de interpretación y ejecución.

La informática distribuida facilita la compartición de los recursos y servicios informáticos por medio del intercambio directo entre los dispositivos y los sistemas informáticos. Estos recursos y servicios incluyen el intercambio de información, el almacenamiento temporal y el almacenamiento de discos para los archivos. La informática distribuida aprovecha la conectividad de la red, permitiendo que los clientes saquen provecho de su potencia colectiva para beneficiar a la totalidad de la empresa. En este aspecto, una diversidad de dispositivos pueden tener aplicaciones, objetos o recursos que pueden interactuar para implicar técnicas de autenticación de la presente invención para la canalización o canalizaciones de gráficos de confianza.

La figura 2 proporciona un diagrama esquemático de un entorno informático distribuido o de red a modo de ejemplo. El entorno informático distribuido comprende los objetos informáticos 10a, 10b, etc. y los objetos o dispositivos informáticos 110a, 110b, 110c, etc. Estos objetos pueden comprender programas, procedimientos, almacenes de datos, lógicas programables, etc. Los objetos pueden comprender porciones de los mismos dispositivos o dispositivos diferentes, tales como PDA, televisores, reproductores de MP3, televisiones, ordenadores personales, etc. Cada objeto se puede comunicar con otro objeto por medio de la red de comunicaciones 14. Esta red puede comprender por sí misma otros objetos informáticos y dispositivos informáticos que proporcionan servicios al sistema de la figura 2. De acuerdo con un aspecto de la presente invención, cada objeto 10 o 110 puede contener una aplicación que podría solicitar las técnicas de autenticación de la presente invención para la canalización o canalizaciones de gráficos de confianza.

También se ha de apreciar que un objeto, tal como 110c, puede ser alojado en otro dispositivo informático 10 o 110. Por lo tanto, a pesar de que el entorno físico ilustrado puede mostrar los dispositivos conectados como ordenadores, dicha ilustración es únicamente a modo de ejemplo y el entorno físico puede, como alternativa, ser ilustrado o descrito como que comprende diversos dispositivos digitales, tales como PDA, televisores, reproductores de MP3,

etc., objetos de software tales como interfaces, objetos COM y similares.

Existe una diversidad de sistemas, componentes y configuraciones de red que soportan los entornos informáticos distribuidos. Por ejemplo, los sistemas informáticos pueden ser conectados entre sí por sistemas cableados o inalámbricos, o por redes locales o redes ampliamente distribuidas. En la actualidad, muchas de las redes están conectadas a Internet, lo cual proporciona la infraestructura para la informática ampliamente distribuida y comprende muchas redes diferentes.

En los entornos informáticos domésticos, existen al menos cuatro medios de transporte de red dispares que pueden soportar cada uno un protocolo único, tales como una línea de alimentación, datos (tanto inalámbrico como cableado), voz (por ejemplo, teléfono) y medios de entretenimiento. La mayor parte de los dispositivos de control en el hogar, tales como los interruptores de luz y electrodomésticos, pueden usar la línea de alimentación para la conectividad. Los servicios de datos pueden entrar en el hogar como una banda de transmisión (por ejemplo, o bien como un módem de DSL o bien de Cable) y se accede a los mismos dentro del hogar usando la conectividad, o bien inalámbrica (por ejemplo, HomeRF u 802.11b) o bien cableada (por ejemplo, Home PNA, Cat 5, incluso línea de alimentación). El tráfico de voz puede entrar al hogar, o bien como cableado (por ejemplo, Cat 3), o bien inalámbrico (por ejemplo, teléfonos celulares) y se puede distribuir dentro del hogar usando el cableado Cat 3. Los medios de entretenimiento pueden entrar al hogar, a través de o bien satélite o bien cable y por lo general se distribuyen en el hogar usando un cable coaxial. Las normas IEEE 1394 y DVI también están surgiendo como interconexiones digitales para grupos de dispositivos de medios. Todos estos entornos de red y otros que puedan surgir como normas de protocolo pueden ser interconectados para formar una intranet que puede ser conectada al mundo exterior por medio de Internet. En resumen, existe una diversidad de fuentes dispares para el almacenamiento y transmisión de datos y, por consiguiente, al progresar, los dispositivos informáticos requerirán medios de protección del contenido en todas las porciones de la canalización de procesamiento de datos.

“Internet” se refiere, por lo general, a una colección de redes e interfaces de comunicación que usan el conjunto de protocolo TCP / IP, que es bien conocido en la técnica de las redes informáticas. El TCP / IP es un acrónimo de “*Transport Control Protocol / Interface Program*, Programa de Interfaz / Protocolo de Control de Transporte”. Internet se puede describir como un sistema de redes informáticas remotas distribuidas gráficamente interconectadas por ordenadores que ejecutan los protocolos de red que permiten que los usuarios interactúen y compartan la información por las redes. Debido a que dicha información ampliamente difundida es compartida, las redes remotas tales como Internet han evolucionado por lo general hasta dar un sistema abierto para el cual los desarrolladores pueden diseñar aplicaciones de software para realizar operaciones o servicios especializados, esencialmente sin restricción.

Por lo tanto, la infraestructura de red hace posible una multitud de topologías de red, tales como arquitecturas de cliente / servidor, de punto a punto o híbridas. El “cliente” es un miembro de una clase o grupo que usa los servicios de otra clase o grupo con el cual no está relacionado. Por lo tanto, en informática, un cliente es un procedimiento, es decir, en un sentido amplio, un conjunto de instrucciones o tareas que solicitan un servicio proporcionado por otro programa. Los procedimientos de cliente usan el servicio solicitado sin tener que “conocer” detalle alguno de funcionamiento acerca de otro programa o el propio servicio. En una arquitectura de cliente / servidor, en concreto un sistema de red, un cliente es, por lo general, un ordenador que accede a los recursos de red compartidos proporcionados por otro ordenador (por ejemplo, un servidor). En el ejemplo de la figura 2, los ordenadores 110a, 110b, etc., se pueden considerar como clientes y el ordenador 10a, 10b, etc., se puede considerar como el servidor en el que el servidor 10a, 10b, etc., mantiene los datos que se replican entonces en los ordenadores de cliente 110a, 110b, etc.

Un servidor es, por lo general, un sistema informático remoto al que se puede acceder por medio de una red remota, tal como Internet. El procedimiento de cliente se puede encontrar activo en un primer sistema informático y el procedimiento de servidor se puede encontrar activo en un segundo sistema informático, comunicándose entre sí a través de un medio de comunicación, proporcionando de este modo una funcionalidad distribuida y permitiendo que múltiples clientes aprovechen las capacidades de recopilación de información de servidor.

El cliente y el servidor se comunican entre sí usando la funcionalidad proporcionada por la capa de protocolo. Por ejemplo, el Protocolo de Transferencia de Hipertexto (HTTP, *Hypertext Transfer Protocol*) es un protocolo común que se usa junto con la Red Mundial (WWW, *World Wide Web*). Por lo general, la dirección de la red informática, tal como el Localizador Universal de Recursos (URL, *Universal Resource Locator*), o una dirección de un protocolo de Internet (IP, *Internet Protocol*) se usa para identificar el servidor o los ordenadores de cliente entre sí. La dirección de la red puede ser a la que se hace referencia como Dirección del Localizador Universal de Recursos. Por ejemplo, la comunicación se puede proporcionar a través de un medio de comunicación. En particular, el cliente y el servidor pueden estar conectados entre sí por medio de conexiones de TCP / IP para una comunicación de alta capacidad.

Por lo tanto, la figura 2 ilustra un entorno distribuido de red a modo de ejemplo, como un servidor en comunicación con ordenadores de cliente por medio de la red / bus en el que se puede emplear la presente invención. Con mayor detalle, un número de servidores 10a, 10b, etc., son interconectados por medio de la red / bus de comunicaciones 14, que puede ser una red LAN, WAN, intranet, Internet, etc., con un número de dispositivos informáticos remotos de cliente 110a, 110b, 110c, 110d, 110e, etc., tales como un ordenador portátil, un ordenador de mano, un cliente fino,

un electrodoméstico en red y otros dispositivos, tales como un VCR, una TV, un horno, una luz, un calentador y similares, de acuerdo con la presente invención. Por lo tanto, está contemplado que la presente invención puede ser aplicable a cualquier dispositivo informático en conexión con el cual sea deseable procesar, almacenar y presentar un contenido seguro desde una fuente de confianza.

En un entorno de red en el que la red / bus de comunicaciones 14 es Internet, por ejemplo, los servidores 10 pueden ser servidores de la Web con los cuales los clientes 110a, 110b, 110c, 110d, 110e, etc., se comunican por medio de uno cualquiera de un número de protocolos conocidos, tales como HTTP. Los servidores 10 también pueden servir como clientes 110, tal como puede ser característico de un entorno informático distribuido. Las comunicaciones pueden ser cableadas o inalámbricas, en donde sea apropiado. Los dispositivos de cliente 110 pueden comunicarse, o no, por medio de la red / bus de comunicaciones 14 y pueden tener unas comunicaciones independientes asociadas con los mismos. Por ejemplo, en el caso de una TV o de un VCR, puede haber, o no, un aspecto de red para el control del mismo. Cada ordenador de cliente 110 y el ordenador de servidor 10 pueden estar equipados con diversos módulos de programa de aplicación u objetos 135 y con conexiones o acceso a diferentes tipos de elementos u objetos de almacenamiento, por los que se pueden almacenar archivos o, a los que se pueden descargar o migrar una porción o porciones de archivos. Por lo tanto, la presente invención se puede usar en un entorno de red informático que tiene unos ordenadores de cliente 110a, 110b, etc., que pueden acceder a, e interactuar con, una red informática / bus 14 y unos ordenadores de servidor 10a, 10b, etc., que pueden interactuar con los ordenadores de cliente 110a, 110b, etc., y otros dispositivos 111 y bases de datos 20.

Visión de conjunto de la gestión de derechos (RM)

Tal como es sabido, y haciendo referencia a continuación a la figura 3, la gestión de derechos (RM, *Rights Management*) y su cumplimiento es altamente deseable en relación con el contenido digital 32, tal como audio digital, vídeo digital, texto digital, datos digitales, multimedia digital, etc., en donde dicho contenido digital 32 se va a distribuir a los usuarios. Tras ser recibido por el usuario, dicho usuario presenta el contenido digital 32 con la ayuda de un dispositivo de presentación apropiado, tal como un reproductor de medios, pantalla de textos, etc., en un ordenador personal 34 o similar.

Por lo general, el propietario o desarrollador de contenido (en lo sucesivo en el presente documento, el “propietario”) que distribuye dicho contenido digital 32 desea restringir lo que puede hacer el usuario con dicho contenido digital distribuido 2. Por ejemplo, el propietario del contenido puede desear restringir la copia y la redistribución de dicho contenido 32 por parte del usuario a un segundo usuario, o puede desear permitir que el contenido digital distribuido 32 sea presentado solo un número limitado de veces, solo por un cierto tiempo total, solo en cierto tipo de máquina, solo en cierto tipo de plataforma de presentación, o solo por un cierto tipo de usuario, etc.

No obstante, después de que haya tenido lugar la distribución, dicho propietario del contenido tiene muy poco o ningún control sobre el contenido digital 32. Un sistema de RM 30 permite entonces la presentación controlada de formas arbitrarias de un contenido digital 32 en las que dicho control es flexible y se puede ser definido por el propietario de dicho contenido digital. Por lo general, el contenido 32 se distribuye al usuario en la forma de un paquete 33 por medio cualquier canal de distribución apropiado. El paquete de contenido digital 33, tal como se distribuye, puede incluir el contenido digital 32 cifrado con una clave de cifrado / descifrado (KD) simétrica (es decir, (KD (CONTENIDO))), así como otra información que identifica el contenido, la forma de adquirir una licencia para dicho contenido, etc.

El sistema de RM basado en confianza 30 permite que un propietario del contenido digital 32 especifique las reglas de licencia que se han de satisfacer antes de que se permita que dicho contenido digital 32 sea presentado en un dispositivo informático 34 del usuario. Dichas reglas de licencia pueden incluir un requisito temporal que se ha mencionado en lo que antecede y pueden estar incorporadas dentro de una licencia digital o documento de uso (en lo sucesivo en el presente documento, ‘licencia’) 36 que el dispositivo informático del usuario / usuario 34 (en lo sucesivo en el presente documento, dichas expresiones son intercambiables a menos que las circunstancias requieran lo contrario) ha de obtener del propietario del contenido o un agente del mismo. Dicha licencia 36 también incluye la clave de descifrado (KD) para descifrar el contenido digital, tal vez cifrado de acuerdo con una clave que puede ser descifrada por el dispositivo informático 34 del usuario. Tal como se aprecia en la figura 3, dicha clave de cifrado es una clave pública del dispositivo informático 34 del usuario (PU-BB), y el dispositivo informático 34 del usuario presumiblemente tiene la clave privada (PR-BB) correspondiente por medio de la cual puede ser descifrado (PU-BB (KD)).

El propietario del contenido de un fragmento de contenido digital 32 ha de confiar en que el dispositivo informático 34 del usuario acate las reglas y requisitos especificados por dicho propietario del contenido en la licencia 36, es decir, que el contenido digital 32 no será presentado a menos que las reglas y requisitos dentro de la licencia 36 sean satisfechos. Preferentemente, entonces, el dispositivo informático 34 del usuario está dotado de un componente o mecanismo de confianza 38 que no presentará el contenido digital 32 excepto de acuerdo con las reglas de licencia incorporadas en la licencia 36 asociada con el contenido digital 32 y obtenida por el usuario.

El componente de confianza 38 tiene, por lo general, un evaluador de licencia 40 que determina si la licencia 36 es válida, revisa las reglas y requisitos de licencia en dicha licencia válida 36, y determina sobre la base de las reglas y

requisitos de licencia revisados, sí el usuario solicitante tienen derecho a presentar el contenido digital solicitado 32 de la manera buscada, entre otras cosas. Tal como se podrá entender, el evaluador de licencia 40 es de confianza en el sistema de RM 30 para llevar a cabo los deseos del propietario del contenido digital 32 de acuerdo con las reglas y requisitos en la licencia 36, y el usuario no ha de ser capaz de alterar fácilmente dicho elemento de confianza para fin alguno, ya sea o no inicuo.

Se ha de entender que las reglas y requisitos en la licencia 36 pueden especificar si el usuario tiene derecho a presentar el contenido digital 32 sobre la base de cualquiera de diversos factores, incluyendo quién es el usuario, en dónde está ubicado el usuario, qué tipo de dispositivo informático que está usando el usuario, qué aplicación de representación está invocando el sistema de RM 30, la fecha, la hora, etc. Además, las reglas y requisitos en la licencia 36 pueden limitar la licencia 36 a un número de presentaciones previamente determinado o a un tiempo de presentación previamente determinado, por ejemplo. Por lo tanto, el componente de confianza 38 puede necesitar consultar un reloj 42 en el dispositivo informático 34.

Las reglas y requisitos pueden ser especificados en la licencia 36 de acuerdo con cualquier lenguaje y sintaxis apropiados. Por ejemplo, el lenguaje puede simplemente especificar atributos y valores que se han de satisfacer (FECHA ha de ser posterior a X, por ejemplo), o puede requerir que se realicen funciones de acuerdo con una secuencia de comandos especificada (SI FECHA es mayor que X, ENTONCES HACER ... , por ejemplo).

Tras la determinación por parte del evaluador de licencia 40 de que la licencia 36 es válida y que el usuario satisface las reglas y requisitos de la misma, entonces se puede presentar el contenido digital 32. En particular, para presentar el contenido 32, la clave de descifrado (KD) se obtiene de la licencia 32 y se aplica a (KD (CONTENIDO)) del paquete del contenido 33 para dar como resultado el contenido real 32 y, de hecho, entonces es presentado el contenido real 32.

Tal como se ha expuesto en lo que antecede, en la licencia 36 con (PU-BB (KD)) autoriza, de hecho, a una entidad que posee (PR-BB) a acceder a (KD) y, por lo tanto, a acceder al contenido 32 cifrado de acuerdo con dicha (KD) suponiendo, por supuesto, que la entidad acate todas las condiciones que se exponen en la licencia 36. Por lo tanto, tal como se podrá apreciar, pueden existir otros tipos de licencias 36 dentro del sistema de RM 30.

Por ejemplo, se puede apreciar que, en un escenario, el autor o publicador 44 del contenido 32 puede autorizar a un emisor de licencia 46 particular a emitir una licencia 36 para el contenido 32 correspondiente mediante la provisión de una licencia de publicación 36p al emisor de licencia 46. Tal como se puede apreciar, dicha licencia de publicación 36p es similar a la licencia 36 ya que dicha licencia de publicación 36p probablemente incluye la clave de descifrado (KD) para descifrar el contenido digital 32, cifrado en este caso de acuerdo con una clave pública del emisor de licencia (PU-BB). De un modo similar, la licencia de publicación 36p probablemente incluye las reglas y requisitos para presentar el contenido 32. No obstante, en este caso, dichas reglas y requisitos se van a insertar en la licencia 36 según se emita por parte del emisor de licencia 46, y no son especialmente aplicables a dicho emisor de licencia 46.

A pesar de que se ha de observar que la licencia de publicación 36p puede incluir, de hecho, otras reglas y requisitos que son, de hecho, aplicables al emisor de licencia 46. Por consiguiente, el emisor de licencia 46 ha de incluir un componente de confianza 38 con un evaluador de licencia 40 de una manera similar a la del dispositivo informático 34 del usuario.

Cabe destacar que cada tipo de licencia 36, 36p, etc., tal como se ha mencionado, por lo general incluye una firma digital para fines de autenticación / verificación y cada firma digital se valida con referencia a un certificado digital de una autoridad de confianza de raíz o una serie de dichos certificados que conducen de vuelta a dicha autoridad de confianza de raíz. Cabe resaltar que cada certificado incluye una firma digital con fines de autenticación / verificación, y cada firma está construida sobre la base de una clave privada y se valida de acuerdo con una clave pública correspondiente.

Tal como se puede apreciar, en una cadena de certificados que conducen de una autoridad de confianza de raíz a una licencia 36, 36p, etc. particular, el certificado digital de raíz de la autoridad de confianza de raíz es firmado sobre la base de una clave pública de la autoridad de confianza de raíz y se valida sobre la base de una clave pública correspondiente, la cual se supone que está disponible para la entidad de verificación. Para cada uno de los otros certificados digitales de la cadena y para las licencias 36, 36p, etc., al final de la cadena, dicho otro certificado o licencia 36, 36p, etc., es firmado sobre la base de una clave privada particular y es validado sobre la base de una clave pública correspondiente tal como se obtiene del siguiente certificado en la cadena hacia la autoridad de confianza de raíz.

Por consiguiente, para validar una licencia 36, 36p, etc., se encuentra una cadena correspondiente de certificados de vuelta a una autoridad de confianza de raíz, se encuentra una clave pública correspondiente de dicha autoridad de confianza de raíz, y la clave pública encontrada de la autoridad de confianza de raíz se emplea para validar el certificado de raíz y, suponiendo que dicha validación tiene éxito, una clave pública está ubicada en el certificado raíz y se emplea para validar el siguiente certificado en la cadena. El procedimiento se repite hasta el último certificado en la cadena, punto en el que se encuentra una clave pública en la misma y se emplea para validar la

licencia 36, 36p, etc. Por supuesto, si falla cualquiera de las validaciones, el procedimiento termina y la licencia 36, 36p, etc., no se valida. Por lo general, a menos que se valide, un sistema de RM 30 no aceptará como válida una licencia 36, 36p, etc.

Definición de la autoridad de confianza de raíz dentro de una licencia

Tal como se podrá apreciar a continuación, la validación de una licencia 36, 36p, etc., (en lo sucesivo en el presente documento, la licencia 36) requiere que una autoridad de validación, tal como un componente de confianza 38, ya esté en posesión de la clave pública de la autoridad de confianza de raíz que se corresponde con dicha licencia 36, tal como es definida por la cadena de certificados de la misma. No obstante, tal como se ha indicado en lo que antecede, pueden tener lugar situaciones en las que una entidad, sin que sea su culpa, no se encuentre, de hecho, en posesión de dicha clave pública, por cualquiera de una diversidad de razones. Por supuesto, todas las cadenas de certificados podrían conducir de vuelta a una sola autoridad de confianza de raíz global o casi global, pero dicha dependencia de una o unas pocas raíces de autoridad, centraliza innecesariamente tal confianza de raíz y es problemático que la confianza de raíz centralizada quede comprometida o falle de otra manera.

Por consiguiente, en una realización de la presente invención, una licencia 36 puede definir cualquier autoridad de confianza de raíz particular, al incluir con la misma una clave pública que se corresponde con la misma, mediante lo cual la clave pública se emplea entonces para empezar por la validación de una cadena de certificados adjuntos a dicha licencia 36. Como resultado, no es necesario que entidad de validación alguna se encuentre ya en posesión de clave pública particular alguna de autoridad de confianza de raíz particular alguna sino que, en su lugar, puede obtener dicha clave pública sobre la base de la licencia 36 correspondiente que se va a validar en última instancia sobre la base de dicha clave pública. Por lo tanto, dicha entidad de validación no está vinculada a autoridad de confianza de raíz particular alguna sino que, en su lugar, puede validar casi cualquier licencia 36 que esté vinculada, a través de una cadena correspondiente de certificados, con cualquier autoridad de confianza de raíz designada.

Obsérvese, no obstante, que incluir la clave pública de una autoridad de confianza de raíz, con una licencia 36 que se va a validar, hace en esencia, de este modo, que la licencia 36 se pueda validar a sí misma, lo cual tal como se podría apreciar, no es aceptable por lo general como una práctica de seguridad. Por consiguiente, en una realización de la presente invención y tal como se aprecia en la figura 4, la licencia 36 está separada en al menos dos porciones, incluyendo una porción de descifrado 36d y una porción de autorización 36a, cada una de las cuales ha de ser poseída por un usuario que intente emplear dicha licencia 36 para presentar el contenido 32 correspondiente. Cabe destacar que a la porción de descifrado 36d solo puede acceder el usuario a quien fue emitida la licencia 36, mientras que a la porción de autorización 36 pueden acceder otros, pero tiene una firma que se valida con una información en la porción de descifrado 36d. Por lo tanto, con dichas porciones 36a, 36d la porción de autorización 36 no se puede validar a sí misma. Obsérvese que la licencia 36 puede contener otras porciones sin apartarse del espíritu y el alcance de la presente invención.

En una realización de la presente invención y sin dejar de hacer referencia a la figura 4, la porción de autorización 36a de una licencia 36 identifica al emisor de la licencia 36, incluye una concesión de derechos específica, tal como por ejemplo, presentar un fragmento del contenido 32 de una o más maneras particulares, emitir un tipo de licencia 36, etc., y puede incluir una identificación del contenido relevante 32. Además, la porción de autorización 36a puede especificar uno o mas usuarios o tipos de usuarios particulares que pueden usar la porción de autorización 36a de la licencia 36 y, para cada usuario / tipo de usuario especificado, las condiciones que se han de satisfacer en relación con el uso de la licencia 36.

Cabe destacar que la porción de autorización 36a incluye una firma digital basada al menos en una porción de los elementos que se han mencionado en lo que antecede, en la que la firma conduce de vuelta a una autoridad de confianza de raíz particular que tiene un par de claves pública / privada particular (PU-ROOT, PR-ROOT). Es decir, y tal como se podrá apreciar, la firma (S (PR-ROOT)) puede estar basada en PR-ROOT o puede incluir una cadena de certificados que conducen de vuelta a un último certificado como una firma basada en PR-ROOT. En cualquier caso, y como se ha de apreciar, la firma (S (PR-ROOT)) puede ser validada sobre la base de la aplicación apropiada de (PU-ROOT), o bien directamente o bien por medio de la cadena de certificados, cualquiera que pueda ser el caso.

No obstante, obsérvese que la propia porción de autorización 36a no contiene dicha (PU-ROOT). En su lugar, en una realización de la presente invención, la porción de descifrado 36d contiene la clave de raíz (PU-ROOT) junto con la clave de descifrado (KD) para descifrar el contenido 32 correspondiente. Además, la porción de descifrado 36d puede incluir otros derechos y condiciones además de los derechos y condiciones expuestos en la porción de autorización 36a. Resulta aún más destacable que la porción de descifrado 36d ha de expresar como un derecho / condición que la clave de descifrado (KD) en la misma no se puede emplear a menos que la clave de raíz (PU-ROOT) en la misma se emplee para validar la firma en la porción de autorización 36a correspondiente.

La porción de descifrado 36d probablemente no está firmada digitalmente, a pesar de que dicha firma digital se pueda proporcionar sin apartarse del espíritu y el alcance de la presente invención. Tal como se puede apreciar, si está firmada dicha firma probablemente tendría que ser validada sobre la base de (PU-ROOT) suponiendo que la clave raíz de validación no ha de estar vinculada al dispositivo informático 34 del usuario. No obstante, y una vez más, la inclusión de (PU-ROOT) dentro de la porción de descifrado 36d en la que dicha porción de descifrado 36d se

valida sobre la base de dicha (PU-ROOT) hace que la porción de descifrado 36d se pueda validar a sí misma, lo cual no es, tal como se podrá apreciar, aceptable por lo general como una práctica de seguridad.

En su lugar, en una realización de la presente invención, la porción de descifrado 36d está cifrada para proteger las claves en la misma, en la que la clave de cifrado se selecciona de tal modo que la clave de descifrado correspondiente está disponible para el dispositivo informático 34 del usuario. Tal como se puede apreciar, hacer esto tiene el beneficio adicional de que la porción de descifrado 36d está vinculada al dispositivo informático 34 del usuario por medio de dicha clave de descifrado. Tal como también se puede apreciar, hacer esto tiene el beneficio adicional de que la clave de descifrado puede ser cualquiera de una diversidad de claves siempre que dicha clave de descifrado esté disponible para el dispositivo informático 34 del usuario.

Por ejemplo, en una realización de la presente invención, la clave de descifrado es una clave privada que se corresponde con una clave pública que se emplea como la clave de cifrado, tal como se muestra en la figura 4. Por lo tanto, el dispositivo informático 34 del usuario puede tener, el mismo, dicho par de claves pública / privada, o puede tener acceso a un par de claves pública / privada del propio usuario, o el componente de confianza 38 en el dispositivo informático 34 del usuario puede tener dicho par de claves pública / privada. En cualquier situación de este tipo, la clave pública es proporcionada al constructor de la licencia 36 y, en particular, de la porción de descifrado 36d para su uso en el cifrado de la misma, mientras que la clave privada se mantiene confidencial para descifrar la porción de descifrado 36d.

Como alternativa, la clave de descifrado y la clave de cifrado pueden ser la misma, caso en el cual dicho constructor y el dispositivo informático 34 del usuario pueden establecer un secreto compartido para generar una clave simétrica de este tipo (que no se muestra). Por supuesto, el dispositivo informático del usuario tendría entonces que almacenar de manera segura esa clave simétrica para su recuperación futura.

Haciendo referencia a continuación a la figura 5, con la disposición que se ha expuesto hasta el momento en relación con las figuras 3 y 4, la presentación del contenido 32 en el dispositivo informático 34 de un usuario se logra de la siguiente manera. De manera preliminar y sobre la base de alguna identificación apropiada dentro del contenido 32, el dispositivo informático 34 del usuario y el componente de confianza 38 en el mismo son dirigidos a un servidor de licencia, tal como el emisor de licencia 46 de la figura 3, que puede emitir una licencia 36 que se corresponde con el contenido, y se emite una solicitud a dicho servidor de licencia 46 para dicha licencia 36 (la etapa 501). Por lo general, una solicitud de ese tipo incluye un certificado o similar que identifica o bien el usuario, o bien el dispositivo informático 34 del usuario, o bien el componente de confianza 38 o similar, en el que el certificado incluye en el mismo una clave pública (PU-USER). Sobre la base de la solicitud que incluye el certificado, el servidor de licencia 46 decide entonces si emite una licencia 36 en respuesta. Tal como se puede apreciar, dicha decisión puede estar basada en cualesquiera factores apropiados sin apartarse del espíritu y el alcance de la presente invención.

Suponiendo que el servidor de licencia 46 decide, de hecho, emitir la licencia 36 (la etapa 503), dicho servidor de licencia construye la porción de descifrado 36d y la porción de autorización 36 en la forma expuesta en lo que antecede (la etapa 505), firma la porción de autorización 36a sobre la base de la clave de raíz (PU-ROOT) en la porción de descifrado 36d (la etapa 507) y cifra la porción de descifrado 36d sobre la base de la clave pública (PU-USER) del certificado con la solicitud (la etapa 509). Obsérvese en el presente caso que cada solicitud como en la etapa 501, incluye una clave pública (PU-USER) diferente, en la que dicha (PU-USER) se emplea para cifrar la porción de descifrado 36d de la licencia 36 solicitada y, por consiguiente, cada porción de descifrado 36d correspondiente es diferente. No obstante, la porción de autorización 36a probablemente no difiere de la misma manera, debido a que dicha porción de autorización se ha de firmar para ser validada sobre la base de la misma clave de raíz (PU-ROOT). Por consiguiente, de hecho puede ser el caso que una porción de descifrado 36d diferente se construya como en la etapa 505, y cifrada como en la etapa 509 en respuesta a cada solicitud, pero que solo se construya una porción individual de autorización común 36a como en la etapa 505 y se firme como en la etapa 507 y la porción individual de autorización 36a se puede aplicar a todas las solicitudes.

En cualquier caso, el servidor de licencia 46, en respuesta a la solicitud del dispositivo informático 34 del usuario, devuelve al mismo la licencia 36 incluyendo la porción de autorización 36a y la porción de descifrado 36d (la etapa 511). No obstante, obsérvese que la porción de autorización 36a no ha de ser necesariamente específica de licencia 36 particular alguna y, por consiguiente, puede de hecho ser común a múltiples licencias 36. Por consiguiente, de hecho puede ser el caso que la porción de descifrado 36d se construya como en la etapa 505 en respuesta a cada solicitud, pero que una porción de autorización 36a se construya como en la etapa 505 solo si el solicitante no posee ya dicha porción de autorización 36a. De manera correspondiente, si el solicitante ya posee, de hecho, dicha porción de autorización 36a, no es necesario que el servidor de licencia 46 construya la misma como en la etapa 505, y no es necesario que devuelva la misma como en la etapa 511.

Haciendo referencia a continuación a la figura 6, se aprecia que un dispositivo informático 34 del usuario en posesión de una porción de descifrado 36d y una porción de autorización 36a de una licencia 36 que se corresponde con el contenido 32 cifrado descifra y presenta dicho contenido 32 de la siguiente manera.

De forma preliminar, sobre la base del contenido 32, el dispositivo informático 34 del usuario localiza la licencia 36, o al menos la porción de descifrado 36d de la misma (la etapa 601). Por lo tanto, el dispositivo informático 34 del

usuario descifra la misma de acuerdo con cualquiera que sea el esquema de cifrado que haya sido empleado para cifrar dicha porción de descifrado 36d (la etapa 603). Por ejemplo, por ejemplo, si la porción de descifrado 36d o una porción de la misma está cifrada sobre la base de la clave pública del usuario (PU-USER), entonces el dispositivo informático 34 del usuario aplica la clave privada (PU-USER) correspondiente para revelar dicha porción de descifrado 36d o una porción de la misma.

Además, el dispositivo informático 34 del usuario revisa los derechos / condiciones expuestos en la porción de descifrado 36d y determina si dichos derechos permiten la presentación del contenido 32 de la manera buscada y que dichas condiciones sean satisfechas (la etapa 605). Cabe destacar que dicha determinación incluye asegurar que la clave de descifrado (KD) de la porción de descifrado 36 no se emplee a menos que la clave de raíz (PU-ROOT) en la misma se emplee para validar la firma de la porción de autorización 36a correspondiente. Obsérvese que, si es el caso que los derechos / condiciones no estén cifrados dentro de la porción de descifrado 36d, puede tener lugar la etapa 605 antes que la etapa 603, y la etapa 603 se puede evitar en el caso en el que dichos derechos / condiciones no permitan la presentación del contenido 32 de la manera buscada. Obsérvese también que, si los derechos / condiciones o cualquier parte de la porción de descifrado 36d no están cifrados, dichas partes han de ser al menos la base para una firma digital y dicha firma digital ha de ser verificada para asegurar la misma frente manipulaciones indebidas.

Suponiendo que los derechos / condiciones de la porción de descifrado 36d permitan la presentación del contenido 32 de la manera buscada, el dispositivo informático 34 del usuario obtiene la clave de raíz (PU-ROOT) y la clave de descifrado (KD) para descifrar el contenido 32 correspondiente de la porción de descifrado 36d (la etapa 607), localiza la porción de autorización 36a (la etapa 608) y, entonces, emplea dicha (PU-ROOT) para validar la firma digital (S (PR-ROOT)) de la porción de autorización 36a (la etapa 609). Dicha validación se puede realizar de cualquier manera apropiada sin apartarse del espíritu y el alcance de la presente invención. Dicha validación es conocida o ha de ser evidente para el público relevante y, por lo tanto, no es necesario que se exponga en la presente descripción con detalle alguno.

Suponiendo que la validación tiene éxito, el dispositivo informático 34 del usuario puede revisar entonces los derechos / condiciones expuestos en la porción de autorización 36a y determinar si dichos derechos permiten la presentación del contenido 32 de la manera buscada y que dichas condiciones sean satisfechas (la etapa 611). Obsérvese que la etapa 611 puede tener lugar antes que la etapa 609 y la etapa 609 se puede evitar en el caso en el que dichos derechos / condiciones no permitan la presentación del contenido 32 de la manera buscada.

Suponiendo que los derechos / condiciones en la porción de autorización 36a permitan la presentación del contenido 32 de la manera buscada, el dispositivo informático 34 del usuario emplea la clave de descifrado (KD) tal como se obtuvo en la etapa 607 para, de hecho, descifrar el contenido 32 cifrado (la etapa 613) y, entonces, presenta dicho contenido 32 cifrado (la etapa 615).

Conclusión

La programación necesaria para efectuar los procedimientos que se realizan en relación con la presente invención, es relativamente sencilla y ha de ser evidente para el público de programación relevante. Por consiguiente, dicha programación no se adjunta a la presente descripción. Entonces, se puede emplear cualquier programación particular para efectuar la presente invención sin apartarse del espíritu y el alcance de la misma.

En la presente invención se proporciona una arquitectura flexible para definir una licencia digital 36 y el funcionamiento de la misma. La arquitectura prevé múltiples autoridades de confianza de raíz y permite que una licencia 36 especifique por sí misma cada autoridad de confianza de raíz que se puede emplear para autenticar / verificar la misma. Para efectuar dicha arquitectura, la licencia 36 incluye una porción de descifrado 36d que está cifrada de una manera tal que solo puede acceder a la misma un usuario o grupo de usuarios particular, y una porción de autorización 36a que ha de ser validada sobre la base de una clave obtenida de la porción de descifrado 36d.

Se ha de apreciar que se podrían hacer cambios a las realizaciones que se han descrito en lo que antecede sin apartarse de los conceptos inventivos de la misma. Por lo tanto, se ha de entender que la presente invención no se limita a las realizaciones particulares que se desvelan, sino que tiene por objeto cubrir las modificaciones que se encuentren dentro del espíritu y el alcance de la presente invención, tal como se define mediante las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un medio legible por ordenador que tiene almacenado en el mismo una estructura digital que define una licencia digital (36) que autoriza la presentación de un fragmento correspondiente de un contenido digital (32) en un dispositivo informático (34), estando el contenido en una forma cifrada y pudiendo descifrarse de acuerdo con una clave de descifrado (KD), emitiéndose la licencia a un usuario y comprendiendo:

una porción de descifrado (36d) a la que puede acceder solo el usuario a quien se emite la licencia y que tiene una clave de descifrado (KD) y que valida una información que incluye una identificación de una autoridad de confianza de raíz; y
una porción de autorización (36a) que expone unos derechos concedidos en relación con el contenido digital y unas condiciones que se han de satisfacer para ejercer los derechos concedidos, teniendo la porción de autorización una firma digital que se valida de acuerdo con la autoridad de confianza de raíz identificada en la porción de descifrado,
en el que la información de validación en la porción de descifrado permite que el usuario a quien se emite la licencia, tras acceder a la porción de descifrado, valide la firma digital en la porción de autorización, y los derechos en la porción de autorización pueden ser ejercidos por el usuario solo si las condiciones en la porción de autorización así lo permiten, ejerciéndose los derechos mediante el descifrado del contenido cifrado con la clave de descifrado (KD) de la porción de descifrado y la presentación del contenido descifrado,
en el que la porción de descifrado tiene unas condiciones que se han de satisfacer, incluyendo una condición de que la clave de descifrado (KD) en la misma no se puede emplear a menos que se emplee la información de validación en la misma para validar la firma en la porción de autorización,
en el que la firma digital de la porción de autorización conduce de nuevo a la autoridad de confianza de raíz identificada en la porción de descifrado, la autoridad de confianza de raíz tiene un par de claves pública / privada particular (PU-ROOT, PR-ROOT), la firma digital se basa en (PR-ROOT) o incluye una cadena de certificados que conducen de nuevo a un último certificado con una firma basada en (PR-ROOT), y la identificación de la autoridad de confianza de raíz tal como se expone en la porción de descifrado comprende (PU-ROOT), y en el que (PU-ROOT) se aplica a la firma digital para validar la misma o bien directamente o bien por medio de la cadena de certificados, y
en el que la porción de descifrado está cifrada en una forma que puede ser descifrada por el usuario a quien se emite la licencia y que está vinculada a dicho usuario,
en el que no es necesario que la licencia esté vinculada a autoridad de confianza de raíz particular alguna.

2. El medio de la reivindicación 1, en el que la porción de descifrado está separada de la porción de autorización.

3. El medio de la reivindicación 1, en el que la porción de autorización de la licencia especifica al menos un usuario o tipo de usuario particular que puede usar dicha porción de autorización y, para cada usuario / tipo de usuario especificado, las condiciones que se han de satisfacer en relación con el uso de la licencia.

4. El medio de la reivindicación 1, en el que la porción de descifrado tiene unas condiciones que se han de satisfacer, incluyendo una condición de que los derechos concedidos en la porción de autorización solo se pueden ejercer si se satisfacen las condiciones expuestas en la porción de autorización.

5. El medio de la reivindicación 1, en el que la porción de descifrado está cifrada, al menos parcialmente, de acuerdo con un secreto compartido conocido por el usuario a quien se emite la licencia.

6. El medio de la reivindicación 1, en el que el usuario en el que se usa la licencia tiene un par de claves pública / privada (PU-USER, PR-USER), la porción de descifrado está cifrada, al menos parcialmente, de acuerdo con (PU-USER), y (PR-USER) se aplica a la porción de descifrado cifrada para descifrar la misma.

7. Un procedimiento para presentar un fragmento de contenido digital en un dispositivo informático, estando el contenido en una forma cifrada y pudiendo descifrarse de acuerdo con una clave de descifrado (KD), comprendiendo el procedimiento:

obtener una licencia digital que se corresponde con el contenido, emitiéndose la licencia digital a un usuario y comprendiendo:

una porción de descifrado a la que puede acceder solo el usuario a quien se emite la licencia y que tiene una clave de descifrado (KD) y que valida una información que incluye una identificación de una autoridad de confianza de raíz; y
una porción de autorización que expone unos derechos concedidos en relación con el contenido digital y unas condiciones que se han de satisfacer para ejercer los derechos concedidos, teniendo la porción de autorización una firma digital que se valida de acuerdo con la autoridad de confianza de raíz identificada en la porción de descifrado;
acceder a la porción de descifrado;
obtener la clave de descifrado (KD) y la información de validación en la porción de descifrado a la que se ha accedido;
validar la firma digital de la porción de autorización con la información de validación obtenida; y

ejercer los derechos en la porción de autorización solo si la firma digital de la misma se valida y las condiciones en la porción de autorización así lo permiten, ejerciéndose los derechos mediante el descifrado del contenido cifrado con la clave de descifrado (KD) obtenida y la presentación del contenido descifrado,
en el que no es necesario que la licencia esté vinculada a autoridad de confianza de raíz particular alguna,
en el que la firma digital de la porción de autorización conduce de nuevo a la autoridad de confianza de raíz identificada en la porción de descifrado, la autoridad de confianza de raíz tiene un par de claves pública / privada particular (PU-ROOT, PR-ROOT), la firma digital se basa en (PR-ROOT) o incluye una cadena de certificados que conducen de nuevo a un último certificado con una firma basada en (PR-ROOT) y la identificación de la autoridad de confianza de raíz tal como se expone en la porción de descifrado comprende (PU-ROOT), comprendiendo el procedimiento la aplicación de (PU-ROOT) a la firma digital para validar la misma, o bien directamente o bien por medio de la cadena de certificados,
en el que la porción de descifrado está cifrada en una forma que puede ser descifrada por el usuario a quien se emite la licencia y que está vinculada a dicho usuario, comprendiendo el procedimiento el acceso a la porción de descifrado mediante el descifrado de la misma.

8. El procedimiento de la reivindicación 7, en el que la porción de descifrado está cifrada, al menos parcialmente, de acuerdo con un secreto compartido conocido por el usuario a quien se emite la licencia, comprendiendo el procedimiento el acceso a la porción de descifrado mediante el descifrado de la misma de acuerdo con el secreto compartido.

9. El procedimiento de la reivindicación 7, en el que el usuario en el que se usa la licencia tiene un par de claves pública / privada (PU-USER, PR-USER), la porción de descifrado está cifrada, al menos parcialmente, de acuerdo con (PU-USER), comprendiendo el procedimiento el acceso a la porción de descifrado mediante la aplicación de (PR-USER) a esta para descifrar la misma.

10. El procedimiento de la reivindicación 7, en el que la porción de descifrado tiene unas condiciones que se han de satisfacer, comprendiendo además el procedimiento la revisión de las condiciones expuestas en la porción de descifrado y la determinación de que se satisfacen dichas condiciones.

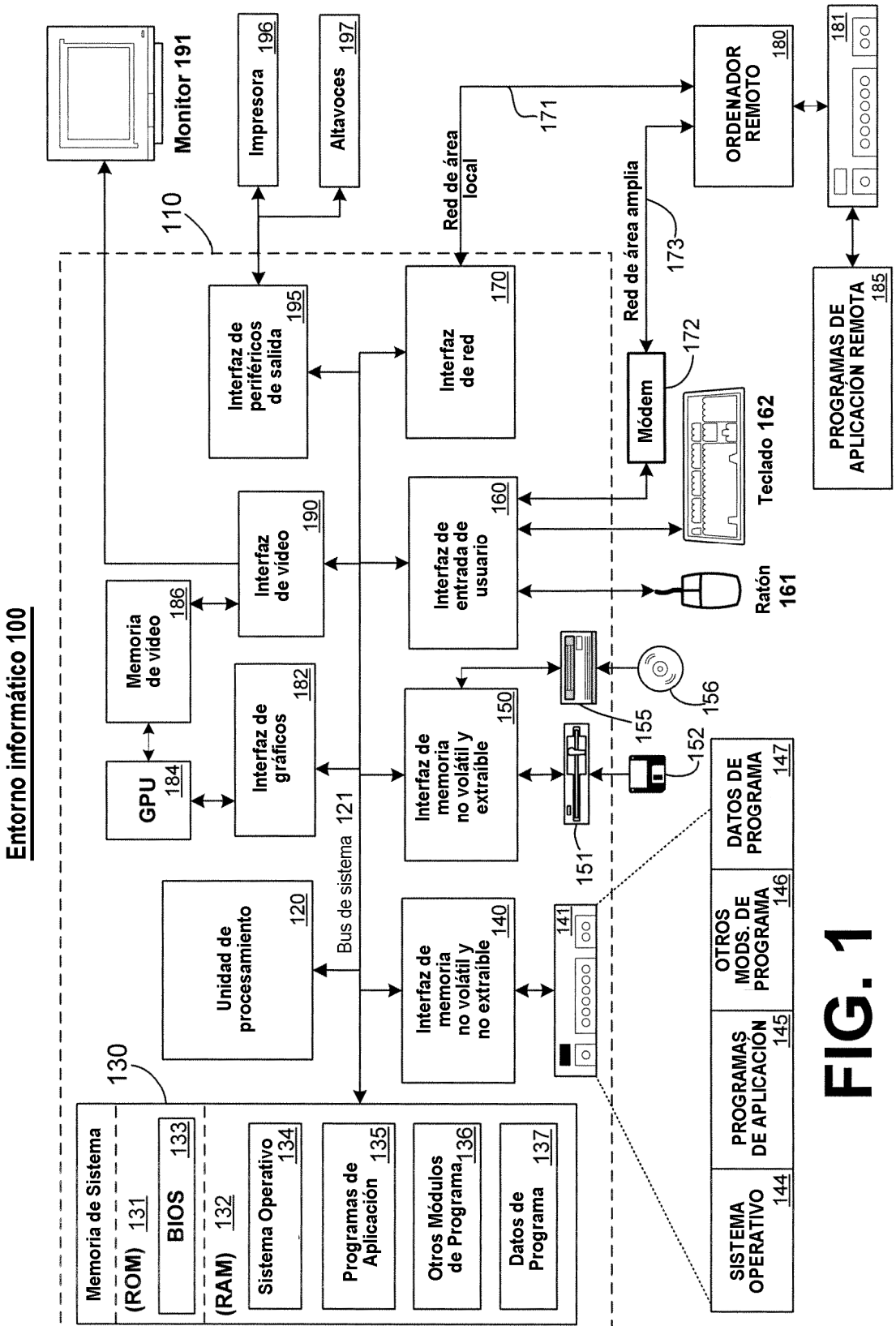
Entorno informático 100
110
Monitor 191
Impresora 196
Altavoces 197
Red de área local
171
ORDENADOR REMOTO 180
181
Red de área amplia
173
PROGRAMAS DE APLICACIÓN REMOTA 185
Interfaz de periféricos de salida 195
Interfaz de red 170
Módem 172
Interfaz de vídeo 190
Interfaz de entrada de usuario 160
Teclado 162
Ratón 161
Memoria de vídeo 186
GPU 184
Interfaz de gráficos 182
Interfaz de memoria no volátil y extraíble 150
155
156
152
151
Bus de sistema 121
Unidad de procesamiento 120
Interfaz de memoria no volátil y no extraíble 140
141
130
Memoria de Sistema
(ROM) 131
BIOS 133
(RAM) 132
Sistema Operativo 134
Programas de Aplicación 135
Otros Módulos de Programa 136
Datos de Programa 137
SISTEMA OPERATIVO 144
PROGRAMAS DE APLICACIÓN 145
OTROS MODS. DE PROGRAMA 146
DATOS DE PROGRAMA 147

FIG. 1

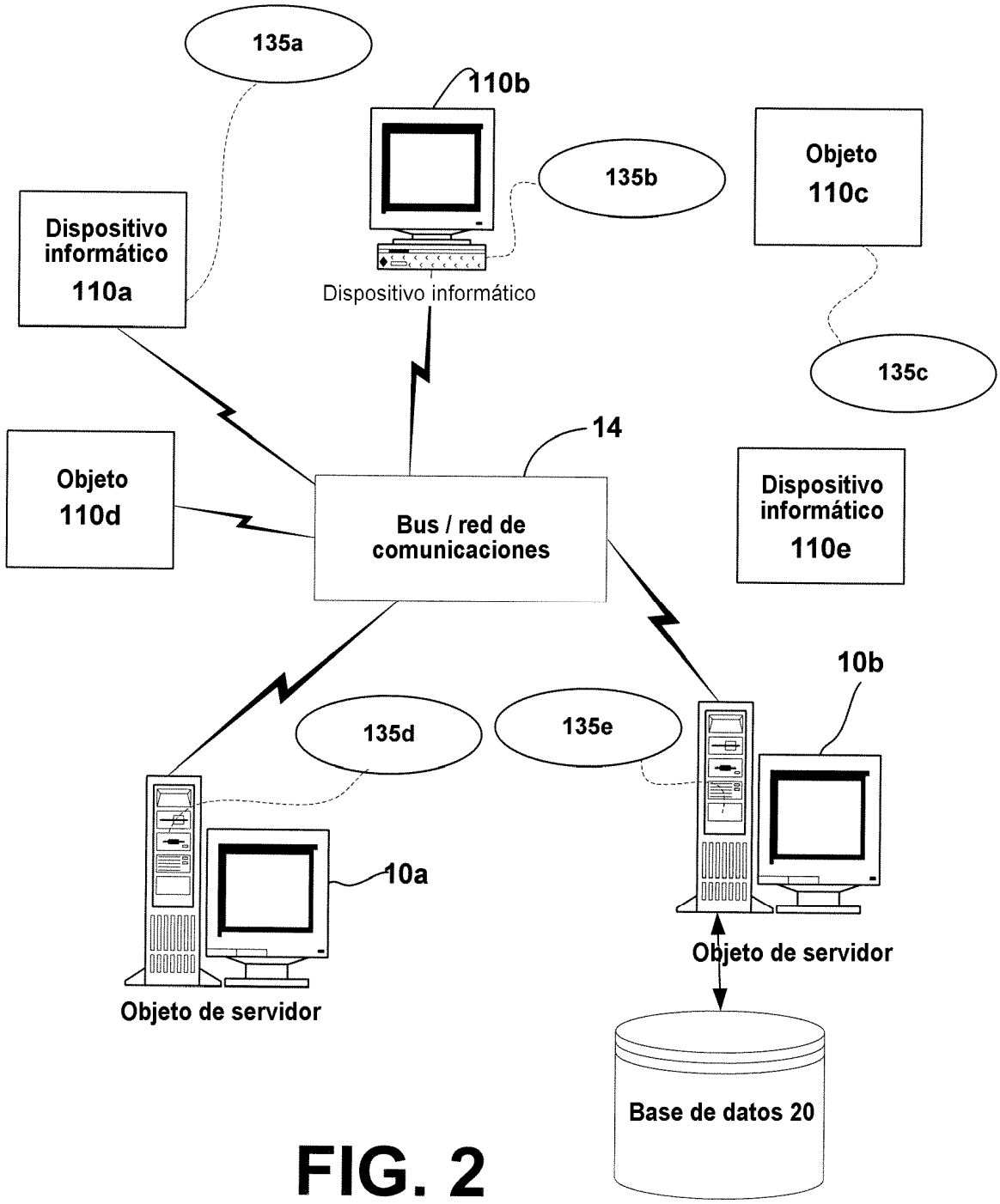
135a
110b
135b
Objeto
110c
Dispositivo
informático
110a
Dispositivo informático
135c
14
Objeto
110d
Bus / red de
comunicaciones
Dispositivo
informático
110e
10b
135d
135e
10a
Objeto de servidor
Objeto de servidor
Base de datos 20

FIG. 2

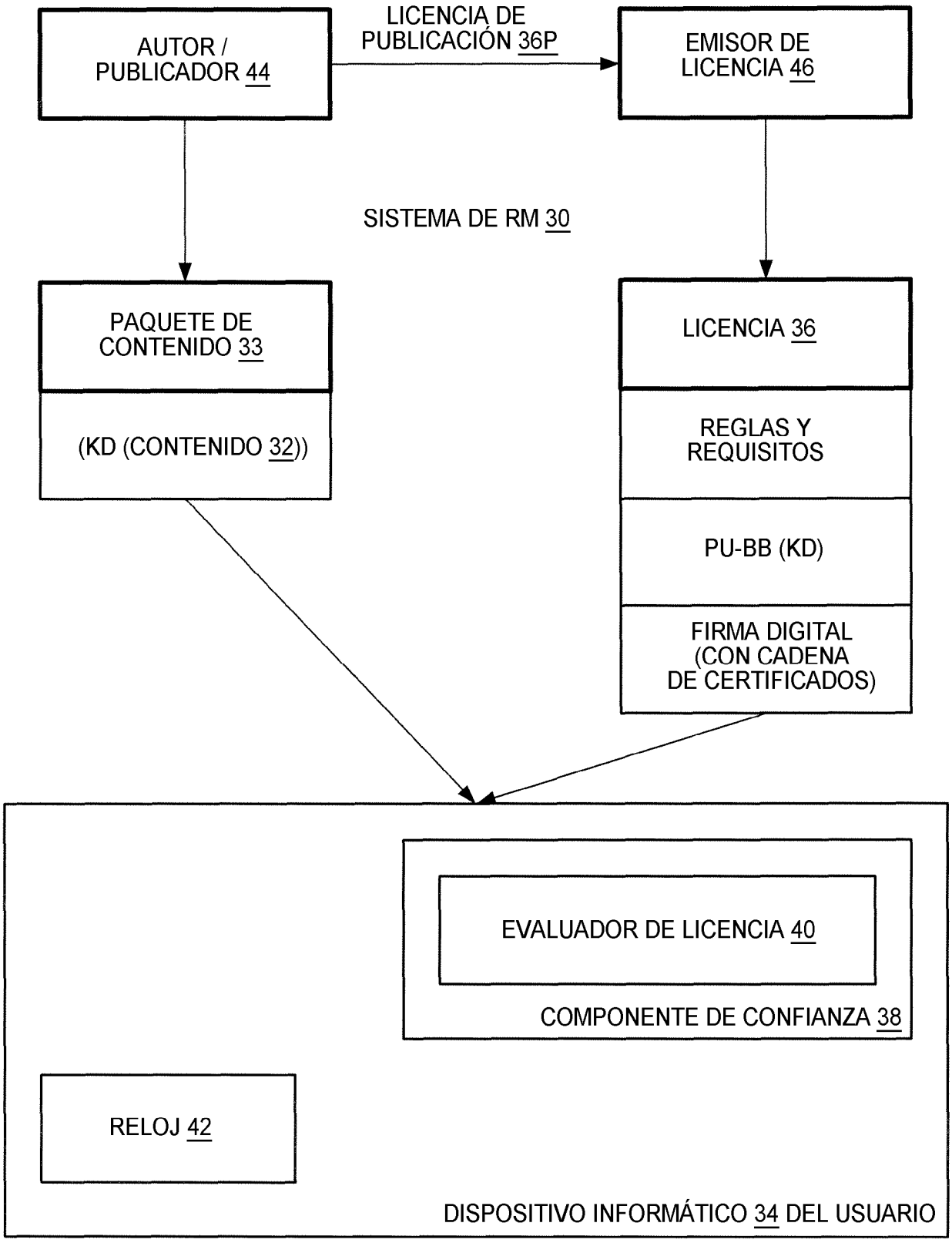
AUTOR / PUBLICADOR 44
LICENCIA DE PUBLICACIÓN 36P
EMISOR DE LICENCIA 46
SISTEMA DE RM 30
PAQUETE DE CONTENIDO 33
(KD (CONTENIDO 32))
LICENCIA 36
REGLAS Y REQUISITOS
PU-BB (KD)
FIRMA DIGITAL (CON CADENA DE CERTIFICADOS)
EVALUADOR DE LICENCIA 40
COMPONENTE DE CONFIANZA 38
RELOJ 42
DISPOSITIVO INFORMÁTICO 34 DEL USUARIO

Fig. 3

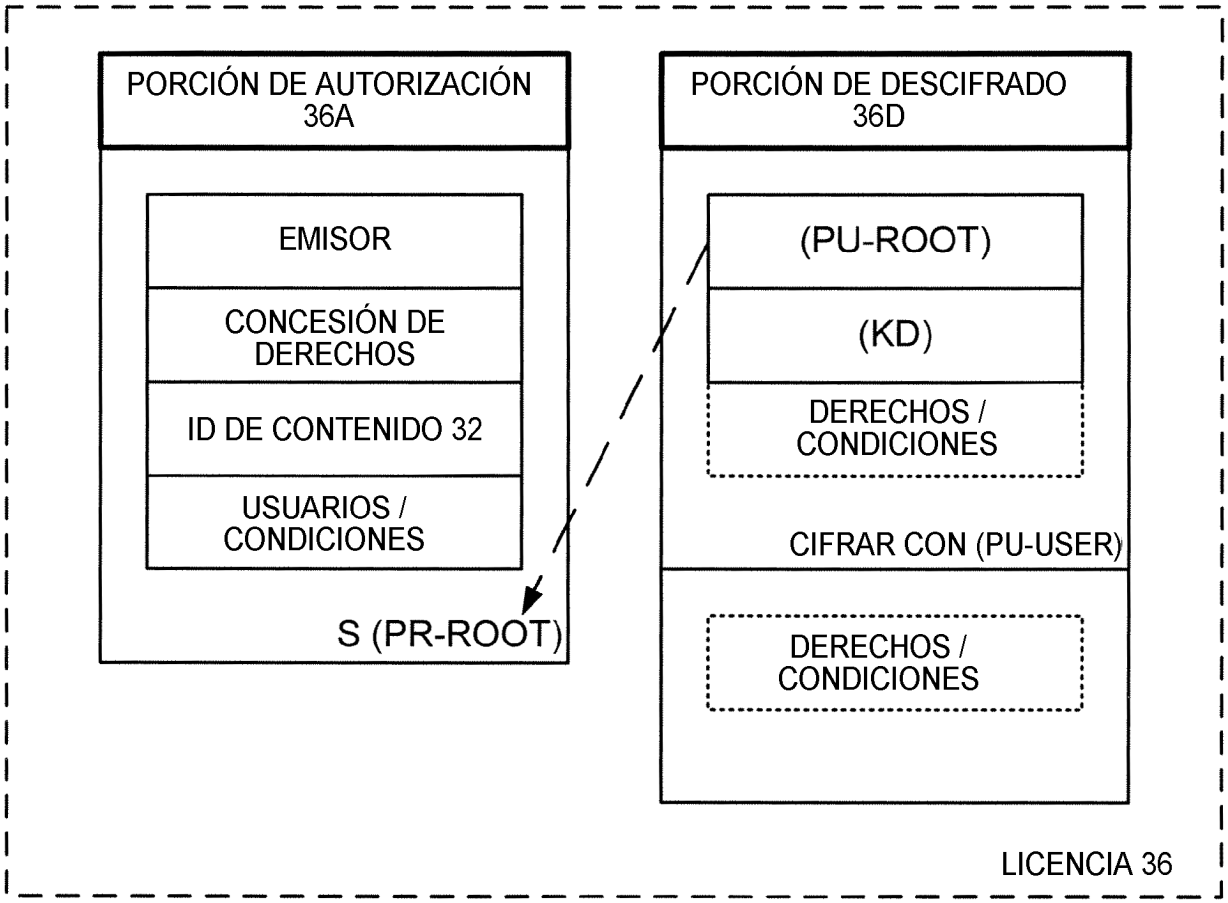
PORCIÓN DE AUTORIZACIÓN
36A
EMISOR
CONCESIÓN DE DERECHOS
ID DE CONTENIDO 32
USUARIOS / CONDICIONES
S (PR-ROOT)
PORCIÓN DE DESCIFRADO
36D
(PU-ROOT)
(KD)
DERECHOS / CONDICIONES
CIFRAR CON (PU-USER)
DERECHOS / CONDICIONES
LICENCIA 36

Fig. 4

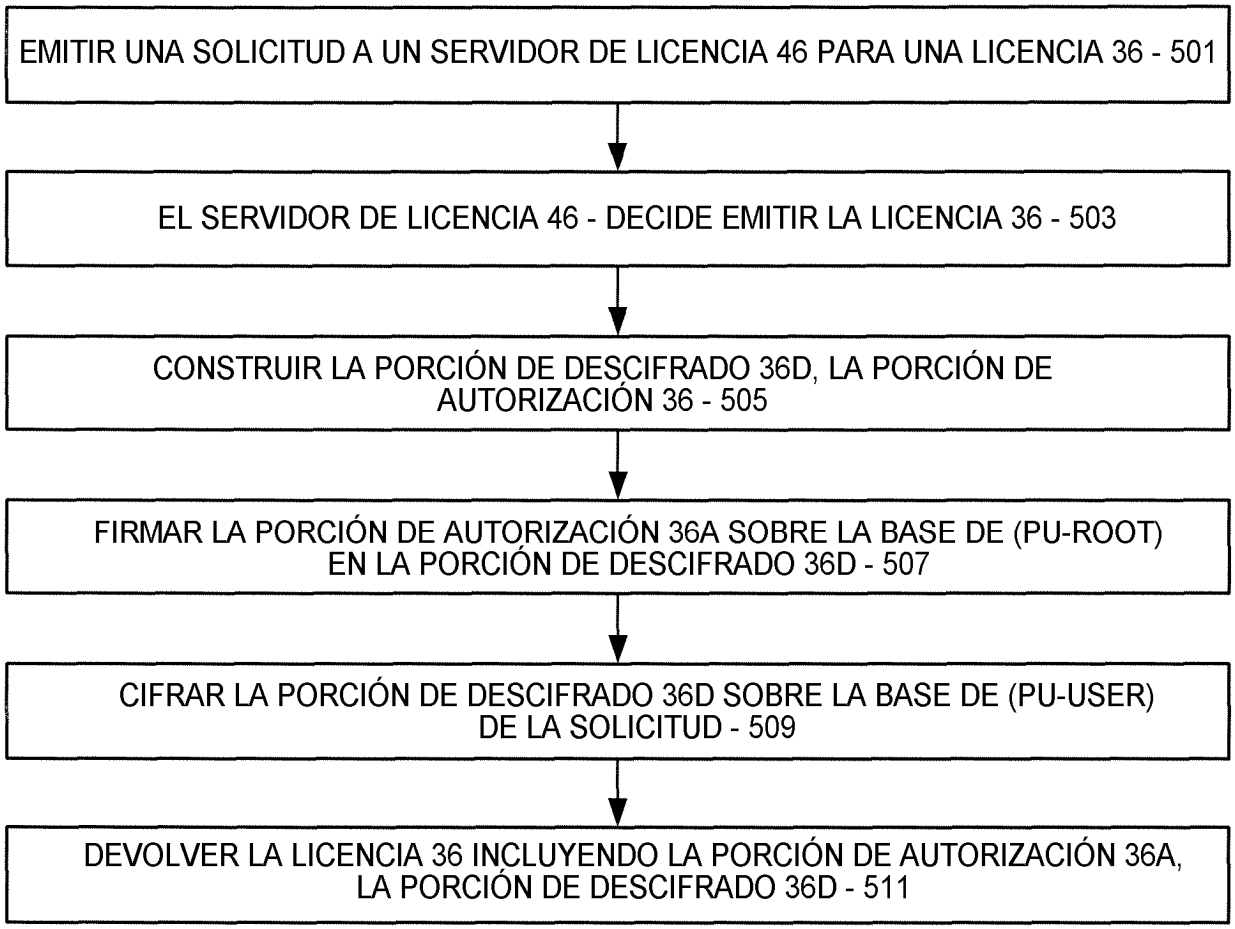
EMITIR UNA SOLICITUD A UN SERVIDOR DE LICENCIA 46 PARA UNA LICENCIA 36 - 501
EL SERVIDOR DE LICENCIA 46 - DECIDE EMITIR LA LICENCIA 36 - 503
CONSTRUIR LA PORCIÓN DE DESCIFRADO 36D, LA PORCIÓN DE AUTORIZACIÓN 36 - 505
FIRMAR LA PORCIÓN DE AUTORIZACIÓN 36A SOBRE LA BASE DE (PU-ROOT) EN LA PORCIÓN DE DESCIFRADO 36D - 507
CIFRAR LA PORCIÓN DE DESCIFRADO 36D SOBRE LA BASE DE (PU-USER) DE LA SOLICITUD - 509
DEVOLVER LA LICENCIA 36 INCLUYENDO LA PORCIÓN DE AUTORIZACIÓN 36A, LA PORCIÓN DE DESCIFRADO 36D - 511

Fig. 5

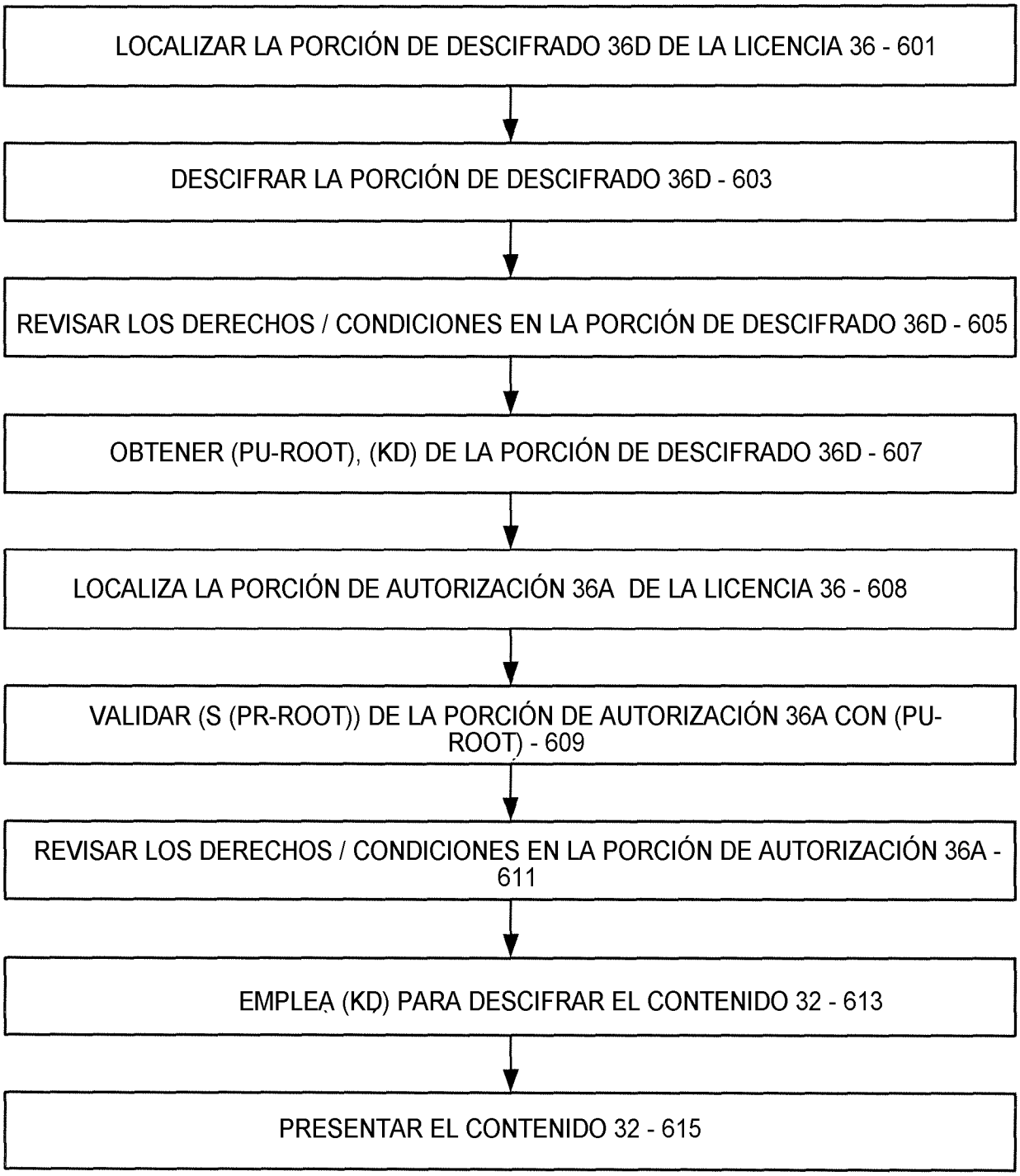
LOCALIZAR LA PORCIÓN DE DESCIFRADO 36D DE LA LICENCIA 36 - 601
DESCIFRAR LA PORCIÓN DE DESCIFRADO 36D - 603
REVISAR LOS DERECHOS / CONDICIONES EN LA PORCIÓN DE DESCIFRADO 36D - 605
OBTENER (PU-ROOT), (KD) DE LA PORCIÓN DE DESCIFRADO 36D - 607
LOCALIZA LA PORCIÓN DE AUTORIZACIÓN 36A DE LA LICENCIA 36 - 608
VALIDAR (S (PR-ROOT)) DE LA PORCIÓN DE AUTORIZACIÓN 36A CON (PU-ROOT) - 609
REVISAR LOS DERECHOS / CONDICIONES EN LA PORCIÓN DE AUTORIZACIÓN 36A - 611
EMPLEA (KD) PARA DESCIFRAR EL CONTENIDO 32 - 613
PRESENTAR EL CONTENIDO 32 - 615

Fig. 6