(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 702 044**

(51) Int. CI.:

G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.11.2003 PCT/IB2003/005725**

(87) Fecha y número de publicación internacional: **15.07.2004 WO04059451**

(96) Fecha de presentación y número de la solicitud europea: **21.11.2003 E 03775710 (1)**

(97) Fecha y número de publicación de la concesión europea: **17.10.2018 EP 1581849**

(54) Título: **Derechos divididos en dominio autorizado**

(30) Prioridad:

30.12.2002 EP 02080568

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.02.2019

(73) Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
High Tech Campus 5
5656 AE Eindhoven, NL

(72) Inventor/es:

KAMPERMAN, FRANCISCUS, L., A., J.;
SCHRIJEN, GEERT, J. y
VAN DEN HEUVEL, SEBASTIAAN, A., F., A.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Derechos divididos en dominio autorizado

La invención se refiere a un método para controlar el acceso a un elemento de contenido en un sistema que comprende un conjunto de dispositivos, comprendiendo el método una etapa de asociar al menos un derecho de uso con el elemento de contenido.

La invención se refiere además a un sistema cliente que comprende un conjunto de dispositivos, estando dispuesto el sistema cliente para realizar el control de acceso a un elemento de contenido, con medios de manejo para un derecho de uso asociado con el elemento de contenido.

La invención se refiere además a un sistema de servidor que está dispuesto para realizar el control de acceso a un elemento de contenido, el sistema de servidor además asocia al menos un derecho de uso con el elemento de contenido.

La invención también se refiere a una señal para llevar derechos de uso.

La invención también se refiere a un dispositivo dispuesto para realizar el control de acceso a un elemento de contenido, pudiendo manejar un derecho de uso asociado con el elemento de contenido.

La televisión y otros contenidos se están volviendo cada vez más digitales. Además, el contenido digital puede transferirse fácilmente entre dispositivos que a menudo pueden comunicarse entre sí. Esto presenta al usuario final con un sistema fácil de usar, donde el acceso al contenido ya no se limita a un solo dispositivo, sino que se puede acceder al contenido desde cualquier dispositivo conectado a algún tipo de red (en casa).

También representa una amenaza para el propietario del contenido que su contenido se copie o transfiera de forma ilimitada. Un sistema (DRM) de gestión de derechos digitales está diseñado para proteger y regular el acceso al contenido. Para el propietario del contenido, que a menudo desea imponer reglas estrictas sobre la transferencia digital de contenido para evitar la copia digital ilimitada, la protección del contenido mediante un sistema DRM es una condición importante para la aceptación de la distribución de contenido digital a los hogares de los consumidores.

En varios foros, como CPTWG (Copy Protection Technical Working Group, http://www.cptwg.org), DVB (Digital Video Broadcasting, http://www.dvb.org), y TV-Anytime (http://www.tv-anytime.org) continúan las discusiones sobre cómo asegurarse de que los contenidos digitales de alto valor no puedan redistribuirse ilegalmente cuando los consumidores accedan a ellos en dispositivos conectados a su red interna.

En discusiones recientes dentro de DVB-CPT (Copy Protection Technical module) y TV-Anytime RMP (Rights Management and Protection), los problemas anteriores se abordan bajo el título de Dominio autorizado (AD). Un AD respeta tanto el interés del proveedor como del consumidor de contenido, en el sentido de que el consumidor tiene libertad para acceder y distribuir el contenido dentro del AD, mientras que al mismo tiempo se cubren los derechos de los propietarios de contenido y los proveedores de servicios mediante la introducción de una estricta importación y reglas de exportación para evitar la copia digital ilimitada del contenido a través de dominios.

El grupo DVB-CPT ha definido un AD como un conjunto de unidades funcionales compatibles con DVB-CPCM (Copy Protection and Copy Management), que controla el flujo de contenido y el formato del contenido. El AD representa un entorno de confianza para el uso autorizado de contenido con derechos de autor. El AD puede consistir en varios segmentos, potencialmente desconectados, de la red doméstica de un usuario. Esto incluye la conexión temporal de dispositivos móviles y la "conexión" virtual de diferentes segmentos de red (posiblemente operativos en tiempos no superpuestos) mediante medios portátiles.

Un AD ofrece a los consumidores un acceso sin restricciones y sin complicaciones al contenido adquirido legalmente dentro del AD. Los consumidores esperarán que puedan agregar dispositivos, derechos y contenido al dominio. Los consumidores también esperan que puedan acceder a su contenido en cualquier lugar, en cualquier momento y en cada uno de sus dispositivos. Además, esto también puede ser válido para dispositivos móviles o para terminales fuera de la casa, como un televisor en una habitación de hotel. Además, los usuarios pueden agregarse y eliminarse de un dominio, por ejemplo, porque cambian entre hogares. Otros usuarios también esperan tener acceso al contenido, por ejemplo, porque son amigos durante una visita o debido a disposiciones de uso legítimo.

Por otro lado, los proveedores de contenido requieren fuertes limitaciones en el intercambio de contenido, especialmente a través de la redistribución de Internet. Por lo tanto, los derechos de contenido deben estar claramente definidos y protegidos. Por ejemplo, en el dominio de los sistemas de TV, un derecho de contenido (también llamado ECM en el contexto de televisión de pago) describe lo que se permite con dicho contenido, y un derecho de uso (también llamado EMM en el contexto de televisión de pago) autoriza a una persona a usar un cierto derecho de contenido, y también puede describir lo que un usuario puede hacer con dicho contenido.

Los derechos de uso de ejemplo son un derecho para reproducir contenido, un derecho para hacer una copia de una generación, etc.

Tanto los derechos de contenido como los derechos de uso también pueden contener claves criptográficas.

Para una introducción más extensa en el uso de DRM en redes domésticas, véase F.L.A.J. Kamperman, S.A.F.A. van den Heuvel, M.H. Verberkt, Digital Rights Management in Home Networks, Philips Research, Países Bajos, publicación de la conferencia IBC 2001 vol. I, páginas 70-77.

Es obvio que los derechos de contenido y los derechos de uso representan una cierta cantidad de valor y deben protegerse contra la duplicación no deseada o la creación no autorizada. Esto podría hacerse utilizando comunicaciones seguras y cifradas y el almacenamiento seguro de estos derechos, que solo deben ser manejados por software y/o hardware a prueba de manipulaciones.

Los derechos de contenido no son personalizados y, por lo tanto, pueden transferirse junto con el contenido o ser ofrecidos por diferentes servidores.

Sin embargo, los derechos de uso son personalizados. Dependiendo del modelo de negocio o del esquema de protección, los derechos de uso se pueden vincular a un dispositivo, a un medio como un CD, a un AD o a una persona. El requisito de una manipulación resistente a la manipulación hace que sea difícil utilizar o transferir libremente el derecho de uso, por ejemplo, entre dispositivos o cuando se viaja.

Una mejor solución es proteger los derechos de uso con una firma digital. El derecho de uso está firmado por el proveedor de contenido o una fuente autorizada diferente utilizando una tecnología de firma de clave pública bien conocida. En tal solución, el proveedor de contenido tiene un par de claves privada/pública. La clave privada se requiere en el proceso de agregar una firma al derecho público. La clave privada se mantiene completamente secreta por el proveedor de contenido. La validez de la firma, que protege la integridad del derecho público, se puede verificar utilizando la clave pública correspondiente. Debido a que el derecho de uso está protegido por la firma digital, se puede permitir fuera del entorno a prueba de manipulaciones.

Para evitar el acceso ilegal al contenido, el certificado de derecho de uso solo debe ser aceptado por un dispositivo (compatible) si puede verificarse (utilizando su clave pública) que se origina desde una fuente autorizada. Además, se pueden verificar otras condiciones antes de aceptar un certificado, tal como si el certificado pertenece al AD, el derecho está destinado o, en el caso de un AD basado en una persona, si la persona asociada está presente.

Algunos derechos de uso digital pueden ser utilizados solo un número limitado de veces, por ejemplo, un derecho para reproducir un fragmento de contenido tres veces, o un derecho para transferir el contenido a un dominio diferente dos veces. Esto requiere que el derecho de uso en sí mismo contenga un mecanismo de conteo o revocación de algún tipo que se active cada vez que se use el derecho. Sin embargo, cualquier cambio debido a la implementación del mecanismo de conteo en el derecho de uso invalida la firma. La firma solo puede ser calculada por un tercero de confianza, lo que es claramente una desventaja.

Además, el derecho de uso también puede contener el derecho de transferir contenido una sola vez a un dominio o usuario diferente. Dicho derecho de transferencia debe ser revocado después de haber sido utilizado. La revocación o eliminación de dicho derecho de transferencia también invalida la firma del derecho de uso restante.

El documento WO 01/63387 A divulga el suministro de un archivo que contiene una pluralidad de campos de control que pueden comprender un derecho de acceso. Cada uno de los campos de control está codificado y puede compartirse con otra entidad.

El documento EP 0930556 A divulga el uso de una lista de revocaciones en la que cada elemento está firmado y luego toda la lista también está firmada.

Un objeto de la presente invención es proporcionar un método, un sistema cliente y un dispositivo que permita que el derecho de uso se pueda manejar sin invalidar la firma digital. De este modo, este objeto se realiza al menos al descomponer el derecho de uso en un conjunto de derechos parciales y, subsecuentemente, firmar por separado cada uno de los conjuntos de derechos parciales, lo que da como resultado una firma correspondiente.

Este método tiene la ventaja de que un derecho de uso ahora está firmado en piezas elementales, en lugar de como un todo. Por ejemplo, el derecho a transferir el contenido a un dominio diferente y el derecho a reproducir el contenido una vez en un AD particular, están firmados individualmente. Cuando se utiliza o transfiere un derecho parcial, aún está firmado digitalmente, y también lo son los derechos restantes.

Los dispositivos en el sistema pueden acceder a dicho derecho parcial firmado y verificar su validez, sin requerir acceso al derecho de uso completo. Subsecuentemente, el derecho puede ser ejercido después de la validación exitosa.

Algunos derechos parciales solo se pueden ejercer un número limitado de veces, lo que permite controlar el número de veces que se puede acceder al elemento de contenido. Si un derecho solo puede ejercerse una sola vez, tiene la ventaja de que puede revocarse, eliminarse o marcarse inmediatamente por separado como de haber sido utilizado.

El dispositivo puede verificar la revocación de un derecho antes de ejercerlo, lo que aumenta la robustez frente al uso de derechos obsoletos.

Esta verificación, en la que se puede consultar un dispositivo a prueba de manipulaciones dentro del dominio, permite la revocación confiable de los derechos.

El sistema de dispositivos puede constituir un dominio, por ejemplo, como se describió anteriormente, de, por ejemplo, dispositivos que pertenecen a miembros de un solo hogar, o que tienen alguna otra relación entre los dispositivos o sus propietarios. Las personas pueden entrar y salir de un dominio. Los usuarios pueden ser identificados, por ejemplo, por una tarjeta inteligente personal.

Al menos un dispositivo en el dominio puede agregar su firma a la combinación de uno de los derechos parciales e información que contiene al menos la identificación de sí mismo y/o un dispositivo o dominio diferente, información de validez (longitud, tipo) y, subsecuentemente, para transferir este derecho a un dispositivo diferente, posiblemente sea parte de o represente un dominio diferente.

Esto tiene la ventaja de que es posible rastrear el historial, el canal de redistribución y el emisor original de un derecho transferido.

De manera similar, se podría permitir que un dispositivo se limite a firmar solo el derecho parcial.

Se puede requerir que el dispositivo que transfiere el derecho verifique el cumplimiento del dispositivo que recibe el derecho. También puede verificar con un tercero si el dispositivo receptor no ha sido revocado. El dispositivo receptor puede realizar verificaciones similares en el dispositivo de origen.

El dispositivo que transfiere el derecho a un dispositivo diferente puede revocar o eliminar localmente el derecho parcial.

Se introduce un tipo de derecho de uso, llamado derecho de oferta, que representa una oferta de un proveedor de contenido. El derecho de oferta puede contener la promesa de transferir, previa solicitud, un derecho de uso firmado del proveedor de contenido directamente a un tercero para que se especifique en una etapa posterior. Esto le permite al propietario del derecho de oferta "transferir" un derecho de uso en una etapa posterior, mientras que le permite al proveedor de contenido la verificación del uso del derecho. Se pueden introducir restricciones adicionales, tal como un retraso mínimo o máximo entre el derecho de oferta y el momento de transferir.

El tercero puede ser un dominio diferente, pero también podría ser uno de los dispositivos de propiedad del usuario que no es o no siempre parte del dominio. El tercero también puede ser un dispositivo propiedad de otra persona, pero el propietario de la transferencia lo utiliza en la actualidad, por ejemplo, durante una visita, mientras viaja, o en una habitación de hotel.

La invención se define únicamente por el alcance de las reivindicaciones adjuntas.

Estos y otros aspectos de la invención se describirán adicionalmente a modo de ejemplo y con referencia al dibujo, en el cual:

La Fig. 1 muestra esquemáticamente un sistema que comprende dispositivos interconectados a través de una red,

La Fig. 2 es un derecho firmado digitalmente de acuerdo con el estado de la técnica,

La Fig. 3 es un conjunto de derechos parciales que están firmados individualmente de acuerdo con la presente invención,

La Fig. 4 es un derecho que ha sido transferido y firmado por el emisor de acuerdo con la presente invención.

La Fig. 5 muestra la transferencia de dicho derecho entre dos dominios,

La Fig. 6 muestra un campo asociado con cada derecho para indicar el nivel de protección requerido,

La Fig. 7 muestra la comunicación de un derecho firmado individualmente a una ubicación fuera de la red doméstica, y

La Fig. 8 muestra un derecho de oferta que es utilizado para solicitar la transferencia de un derecho de uso de un proveedor a una ubicación fuera de la red doméstica.

A lo largo de las figuras, los mismos numerales de referencia indican características similares o correspondientes. Algunas de las características indicadas en los dibujos se implementan normalmente en software, y como tal representan entidades de software, como módulos de software u objetos.

La figura 1 muestra esquemáticamente un sistema 100 de red doméstica. Un sistema de este tipo normalmente incluye un número de dispositivos, por ejemplo, un receptor de radio, un sintonizador/decodificador, un reproductor de CD, un par de parlantes, un televisor, una videograbadora, una grabadora, un ordenador personal, etc. Estos dispositivos generalmente están interconectados para permitir un dispositivo, por ejemplo, la televisión, para controlar a otro, por ejemplo, la videograbadora. Un dispositivo, como por ejemplo un sintonizador/decodificador o un decodificador (STB), generalmente es el dispositivo central, que proporciona un control central sobre los demás.

El contenido 130, que normalmente comprende cosas como música, canciones, películas, programas de TV, imágenes, información de la guía de programación y similares, se recibe, por ejemplo, a través de una PC 106 o una puerta de enlace residencial o un decodificador 101. La fuente podría ser una conexión a una red de cable de banda ancha, una conexión a Internet, un enlace descendente de satélite, etc. El decodificador 101, o cualquier otro dispositivo en el sistema 100, puede comprender un medio de almacenamiento S1 tal como un disco duro adecuadamente grande, que permita la grabación y la reproducción posterior del contenido recibido. El almacenamiento S1 podría ser una grabadora (PDR) digital personal de algún tipo, por ejemplo, una grabadora de DVD + RW, a la que está conectado el decodificador 101. El contenido también se puede proporcionar al sistema 100 almacenado en un portador 120 como un Disco Compacto (CD) o un Disco Versátil Digital (DVD). El contenido puede luego transferirse a través de la red 110 a un receptor para representación.

Un receptor puede ser, por ejemplo, la pantalla 102 de televisión, el dispositivo 103 de pantalla portátil, el teléfono 104 móvil y/o el dispositivo 105 de reproducción de audio. La forma exacta en que se representa un elemento de contenido depende del tipo de dispositivo y del tipo de contenido. Por ejemplo, en un receptor de radio, la representación comprende generar señales de audio y enviarlas a los altavoces. Para un receptor de televisión, la representación generalmente comprende generar señales de audio y video y enviarlas a una pantalla de visualización y altavoces. Para otros tipos de contenido se debe tomar una acción apropiada similar. La representación también puede incluir operaciones como desencriptar o descifrar una señal recibida, sincronizar señales de audio y video, etc.

Bajo ciertas condiciones, un ordenador106 personal también podría funcionar como fuente, medio de almacenamiento y/o receptor.

El dispositivo 103 de pantalla portátil y el teléfono 104 móvil están conectados de manera inalámbrica a la red 110 utilizando una estación 111 base, por ejemplo, utilizando Bluetooth o IEEE 802.11b. Los otros dispositivos están conectados mediante una conexión por cable convencional. Para permitir que los dispositivos 101-106 interactúen, hay varios estándares de interoperabilidad disponibles, que permiten que diferentes dispositivos intercambien mensajes e información y se controlen entre sí. Un estándar bien conocido es el estándar de Interoperabilidad de audio/video en el hogar (HAVi), cuya versión 1.0 se publicó en enero de 2000 y está disponible en Internet en la dirección http://www.havi.org. Otros estándares bien conocidos son el estándar de bus (D2B) digital doméstico, un protocolo de comunicaciones descrito en IEC 1030 y Universal Plug and Play (http://www.upnp.org).

A menudo es importante asegurarse de que los dispositivos 101-106 en la red doméstica no hagan copias no autorizadas del contenido. Para hacer esto, es necesario un marco de seguridad, generalmente denominado sistema (DRM) de gestión de derechos digitales. Tal sistema normalmente usa derechos. Diferentes tipos de derechos son derechos de contenido y derechos de uso.

Un derecho de contenido describe lo que se permite con dicho contenido, y un derecho de uso autoriza a una persona a usar un cierto derecho de contenido y también puede describir lo que un usuario puede hacer con dicho contenido.

Los derechos de uso de ejemplo son un derecho para reproducir contenido, un derecho para hacer una copia de una generación, etc.

Tanto los derechos de contenido como los derechos de uso también pueden contener claves criptográficas.

El procesamiento seguro y el almacenamiento de derechos se pueden realizar en un módulo 108 resistente a la manipulación indebida que se puede ubicar, por ejemplo, en el controlador 101 central.

La figura 2 muestra cómo se puede firmar un derecho de uso de acuerdo con la técnica anterior. El derecho de uso podría comprender, por ejemplo, un derecho de representación, un derecho de transferencia, un derecho de trabajo derivado o un derecho de utilidad. Algunos derechos pueden tener una validez limitada en el tiempo o en el número de veces. En este ejemplo, un derecho 201 de uso podría contener un derecho 202 de representación que especifique que un usuario tiene derechos de reproducción para una cierta pieza de contenido, y un derecho 203 de transferencia

que especifica que el usuario tiene derecho a transferir una cierta cantidad de contenido a un dominio diferente exactamente dos veces. El proceso de firma utiliza un cifrado de clave pública bien conocido que se basa en la existencia de un par de claves, una privada y una pública. La clave privada se mantiene secreta por la parte que firma y autentica un mensaje usando esta clave privada, y la clave pública correspondiente puede ser distribuida y utilizada por cualquier tercero para verificar que el mensaje haya sido firmado y no haya cambiado desde que fue firmado por la parte de origen.

En este ejemplo, un generador 210 de par de claves privada/pública ha generado un par de una clave 211 privada y una clave 212 pública para el emisor de los derechos de uso, que puede ser el proveedor de contenido mismo a quien llamamos P. P usa su clave 211 privada durante el proceso 213 de firma del derecho 201 de uso y calcula una firma 204. La combinación del derecho 201 de uso y la firma 204 constituye el derecho 205 de uso firmado que puede almacenarse y transmitirse sin riesgo de manipulación indebida. Cualquier tercero puede realizar un procedimiento 214 de verificación si el mensaje 205 es auténtico usando la clave 212 pública. La respuesta está disponible como salida 215.

Sin embargo, como solo el emisor de los derechos puede firmar dicho derecho 201 de uso, un derecho de este conjunto no puede eliminarse ni manejarse por separado, ya que esto invalidaría la firma 204. Los derechos parciales que han estado disponibles fuera de la protección de entornos seguros tampoco pueden ser revocados de manera confiable, ya que no hay control sobre copias (ilegales) de dicho derecho parcial.

La presente invención hace posible que el derecho de uso se pueda manejar sin invalidar la firma digital.

En un primer ejemplo de la invención, el derecho 201 de uso se descompone en derechos parciales, que subsecuentemente se firman individualmente.

La figura 3 muestra un conjunto de derechos 330 parciales firmados individualmente de acuerdo con la presente invención. Contiene un número de ejemplos de derechos 301, 311, 321 parciales y posiblemente más. En el sistema 350 bajo control de P, se firman derechos parciales. La clave 351 privada de P se usa nuevamente en el proceso 353 para firmar el derecho 301 parcial con el fin de calcular la firma 302. El mismo proceso 356 de firma se utiliza para calcular la firma 312 de P del derecho 311 parcial, y así sucesivamente. Estos derechos firmados junto con otros derechos firmados opcionalmente forman un nuevo conjunto de derechos 330 parciales firmados individualmente. Cada derecho parcial ahora se puede verificar individualmente en el sistema 345 como en el proceso 354, 357 y 360 de verificación para calcular si las firmas son válidas (salida 355, 358 y 361, respectivamente). Esta verificación puede ser realizada por cualquier dispositivo en el dominio que tenga acceso a un derecho parcial. Dicho dispositivo puede verificar si el emisor no ha revocado el derecho o si el emisor en sí no ha sido revocado.

Al tratar los derechos parciales como un conjunto, la comunicación se minimiza en tamaño y número de transacciones, y se mantiene la relación conceptual entre el derecho de uso y el elemento de contenido.

Opcionalmente, el conjunto completo de derechos 330 parciales firmados individualmente puede firmarse en el proceso 373 en su totalidad para poder verificar la integridad del conjunto de derechos. La firma se puede hacer nuevamente en un sistema 369 por el proveedor del servicio, pero también, como se muestra en la Fig. 3, por un tercero T de confianza diferente con su propio par 371/372 de clave privada/pública generado por el generador 370 de pares de clave. La verificación 374 produce la respuesta 375 de salida si el conjunto firmado de derechos 340 está completo.

Una ventaja del primer ejemplo de la invención es que los derechos parciales están protegidos individualmente por una firma y, por lo tanto, pueden fluir libre e independientemente dentro del dominio. Ahora se pueden procesar individualmente, por ejemplo, Revocado

En una variación del primer ejemplo, el conjunto completo de derechos parciales firmados individualmente se puede firmar en el proceso 373 mediante el par 371/372 de claves privada/pública del receptor del conjunto de derechos (por ejemplo, el propio usuario). El resultado se puede enviar de nuevo, por ejemplo, al emisor del conjunto de derechos. Esto puede ser parte de una transacción, para que el emisor pueda probar que el conjunto completo de derechos ha llegado al receptor deseado.

En un segundo ejemplo de la invención, algunos o todos los derechos parciales firmados pueden transferirse desde un dominio (el dominio de origen) a un dominio diferente (el dominio de recepción).

La Fig. 4 muestra cómo un derecho parcial, tal como se describe en la Fig. 3, se complementa con información y firmas adicionales y, subsecuentemente, se firma para formar un derecho de transferencia, que también se denomina un derecho transferible. El derecho transferible se compone preferiblemente desde el mencionado módulo a prueba de manipulaciones, como el módulo 108 en la Fig. 1. Contiene el derecho 311 parcial, además contiene la firma 312 original y aún válida creada por el proceso 356 de firma por P. Además, se agregan los metadatos 411 que contienen información sobre, pero no se limitan a, un identificador para el dominio de origen, un identificador para el dominio de recepción, la razón o el propósito de la transferencia, el tiempo de transferencia y la duración de la validez. Para el

identificador del dominio de origen y de recepción, es preferible utilizar sus claves públicas respectivas. El derecho 311 parcial, la firma 312 correspondiente y la información 411 adicional están compuestas juntas en la información 430 y subsecuentemente firmadas por el dominio de origen en el proceso 463 con su propia clave 461 privada para formar la firma 431. El derecho 440 transferible contiene tanto la información 430 como la firma 431, y cualquier tercero puede verificar en el proceso 464 su validez y autenticidad al usar la clave 462 pública del dominio de origen.

La Fig. 5 muestra dos dominios 500 y 550, ambos similares al sistema 100 en la Fig. 1. Muestra un derecho 440 transferible que se está transfiriendo en el proceso 540 fuera del dominio 500, posiblemente utilizando una comunicación segura, a un dominio 550 diferente, preferiblemente después de que los dispositivos 101 y 501 de comunicación en los respectivos dominios se hayan verificado mutuamente para ser compatibles y no revocados. El dominio 500 de origen puede revocar o eliminar localmente el derecho transferido.

Este ejemplo de la invención tiene la ventaja adicional de que tanto el dominio de origen como el dominio de destino de un derecho transferido pueden recuperarse de manera confiable de los metadatos y firmas contenidos en el derecho transferible. Esto permite el seguimiento del contenido.

En un tercer ejemplo de la invención, se hace una distinción entre diferentes niveles de protección para diferentes tipos de derechos y su manejo.

Algunos de los derechos parciales se pueden usar libremente dentro de un dominio, incluso fuera de la protección de la transmisión encriptada o el almacenamiento seguro, como el derecho local para reproducir una determinada pieza de contenido. Estos derechos serán llamados "derechos seguros". Los derechos seguros pueden fluir libremente dentro del dominio autorizado (AD). Otros derechos, tal como el derecho a transferir una pieza de contenido exactamente una vez, deben ser revocados o eliminados inmediatamente después de haber sido utilizados. Estos derechos serán llamados "derechos débiles". Los derechos débiles necesitan protección contra la duplicación y manipulación no autorizadas, y para hacer cumplir, por ejemplo, que solo pueden emitirse un número limitado de veces. Esta protección se puede proporcionar, por ejemplo, al no permitir derechos débiles fuera de la protección de un entorno seguro, por ejemplo, en un módulo a prueba de manipulaciones (posiblemente en un controlador central) que también se encarga de la transferencia de derechos a un dominio diferente. Por supuesto, también es posible definir más de dos niveles de protección.

Un método potencial para indicar el nivel de protección mínimo requerido para un cierto derecho, es agregar un campo con dicha información. La figura 6 muestra un conjunto modificado de derechos 640, similar al conjunto firmado de derechos 340 parciales firmados individualmente en la figura 3. En su forma más simple, un campo 601/611 de un solo bit indica si los derechos 301/311 tienen que estar restringidos en un almacenamiento seguro. Por ejemplo, el derecho 301 podría ser un derecho de reproducción que no requiere almacenamiento seguro (el contenido de ejemplo en el campo 601 de bits es 0), mientras que el derecho 311 requiere almacenamiento seguro (el contenido de ejemplo en el campo 611 de bits es 1). Los métodos alternativos para indicar el nivel de protección mínimo requerido incluyen, entre otros: un dispositivo toma una decisión sobre el nivel de protección adquirido según el tipo de derecho, o un dispositivo tiene una lista (actualizable) que indica para cada derecho el nivel de protección requerida.

El nivel de protección mínimo requerido se puede usar para determinar cómo se debe manejar el derecho parcial.

En un cuarto ejemplo de la invención, se describe la transferencia de un derecho fuera del dominio, con el fin de (quizás temporalmente) extender la red doméstica con un dispositivo ubicado cerca del usuario/propietario. La extensión también puede ser un dispositivo de un propietario diferente que tenga derecho a acceder a dicho contenido, como se especifica en el derecho parcial o por otras razones (como el uso legítimo).

En la solicitud de patente europea con el número de solicitud 02079390.7 (registro de abogados NL021063) se describe una extensión de la infraestructura AD que le permite a una persona ver o usar su contenido personal de forma remota fuera de la definición original de la red doméstica, por ejemplo, cuando viaja. En dicha aplicación, la seguridad se obtiene mediante el cifrado del contenido, el almacenamiento seguro de las claves de descifrado correspondientes y los derechos de uso personalizados que están protegidos por una firma creada por un tercero de confianza.

En tal situación es ventajoso poder comunicar solo partes del derecho de uso, lo que es posible utilizando las firmas individuales de acuerdo con la presente invención. La figura 7 ilustra el proceso 730 de transferencia de un derecho 731 transferible desde un sistema 100 (como se muestra en la figura 1), a un sistema 770 de televisión remota del hotel a través de una puerta 751 de enlace a, por ejemplo, un conjunto 753 de audio o un televisor 752 ubicado cerca del usuario autorizado. Estos dispositivos pueden ubicarse en una habitación de hotel, salón, etc.

En un quinto ejemplo de la invención, los derechos de transferencia se mantienen en el proveedor del servicio y el propietario se comunica con el proveedor del servicio para que el derecho se transfiera a otra persona o dominio.

Para indicar la existencia de los derechos de transferencia, el derecho de oferta se ha introducido en el texto de esta solicitud.

En este caso, no se requiere almacenamiento seguro para evitar la duplicación no autorizada, ya que el proveedor del servicio puede supervisar que solo se puede hacer un número permitido de copias.

La figura 8 muestra el uso de un derecho de oferta por parte de un sistema 100 de red doméstica. Durante un proceso 820 de comunicación, un derecho 821 de oferta se envía a un proveedor 810 para solicitar la transferencia 830 de un derecho 831 de uso a un sistema 550 fuera de la red doméstica. El proveedor del servicio puede mantener los derechos de transferencia en el almacenamiento 811 o generarlos con un generador 812 cuando sea necesario.

Las alternativas son posibles. En la descripción anterior, "que comprende" no excluye otros elementos o pasos, "un" o "una" no excluye una pluralidad, y un solo procesador u otra unidad también puede cumplir las funciones de varios medios enumerados en las reivindicaciones.

REIVINDICACIONES

1. Un método para controlar el acceso a un elemento de contenido en un sistema que comprende un conjunto de dispositivos, constituyendo el conjunto de dispositivos un primer dominio que comprende dispositivos que están relacionados con un hogar o un grupo limitado de consumidores,

comprendiendo el método una etapa de asociar al menos un derecho de uso con el elemento de contenido, en donde el método comprende además descomponer el derecho de uso en un conjunto de derechos parciales,

subsecuentemente, firmar por separado cada uno de los conjuntos de derechos parciales, lo que da como resultado una firma correspondiente, y

agrupar los derechos parciales firmados individualmente en un conjunto de derechos parciales firmados individualmente, el método comprende, además

permitir al menos un dispositivo en el sistema, para identificar un dispositivo diferente que represente un dominio diferente, para subsecuentemente firmar información que comprende una combinación de

- al menos un derecho parcial y su correspondiente firma,

- una identificación del primer dominio, y

- una identificación del dominio diferente,

y para subsecuentemente transferir esta combinación firmada al dispositivo diferente.

2. El método de la reivindicación 1, en donde al menos un dispositivo en el sistema puede acceder y ejercer al menos uno de los derechos parciales después de la verificación de la firma correspondiente.

3. El método de la reivindicación 1, en donde uno de los derechos parciales asociados con el elemento de contenido comprende uno de un derecho de representación, un derecho de transferencia, un derecho de oferta, un derecho de trabajo derivado y un derecho de utilidad.

4. El método de la reivindicación 1, en donde al menos uno de los derechos parciales solo se puede ejercer un número limitado de veces.

5. El método de la reivindicación 1, en donde el método comprende además una etapa en la que un dispositivo del conjunto de dispositivos verifica si el derecho parcial y el emisor del mismo no han sido revocados antes de ejercer el derecho parcial.

6. El método de la reivindicación 1, en donde se indica un nivel de protección mínimo requerido de al menos un derecho parcial junto con el derecho parcial.

7. El método de la reivindicación 1, en donde un nivel de protección mínimo requerido de al menos un derecho parcial se deriva implícitamente del tipo del derecho parcial.

8. El método de la reivindicación 1, en donde se permite que la transferencia al dispositivo diferente ocurra solo después de que al menos uno de los dispositivos y el dispositivo diferente han sido verificados por el otro dispositivo para que sea al menos uno que cumpla con las normas y no esté revocado.

9. El método de la reivindicación 1, donde el derecho parcial está revocado o eliminado por el dispositivo que transfiere el derecho al dispositivo diferente.

10. El método de la reivindicación 1,

en donde el método comprende además permitir al menos un dispositivo en el sistema,

en donde el derecho de uso está asociado con el elemento de contenido por un proveedor de contenido,

en donde el derecho de uso comprende un derecho de oferta (para un derecho específico),

comprendiendo el método además solicitar al proveedor de contenido ejecutar el derecho de oferta y entregar el derecho específico a un tercero especificado,

sobre el cual el proveedor de contenido, después de verificar las condiciones que pueden aplicarse, entrega el derecho específico directamente al tercero especificado.

11. El método de la reivindicación 1, que comprende la firma de los derechos parciales firmados individualmente en su totalidad para poder verificar la integridad del conjunto de derechos.

12. Un sistema cliente que comprende un conjunto de dispositivos, el conjunto de dispositivos que constituye un primer dominio que comprende dispositivos que están relacionados con un hogar o un grupo limitado de consumidores, el sistema cliente está dispuesto para realizar el control de acceso a un elemento de contenido, con medios de manejo para un derecho de uso asociado con el elemento de contenido, en donde el derecho de uso es un conjunto de derechos parciales firmados individualmente, y el sistema cliente está dispuesto para verificar individualmente y manejar individualmente los derechos parciales, estando el sistema cliente dispuesto además para

permitir que al menos un dispositivo en el sistema identifique un dispositivo diferente que represente un dominio diferente, para subsecuentemente firmar información que comprende una combinación de

- al menos un derecho parcial y su correspondiente firma,

- una identificación del primer dominio, y

- una identificación de los diferentes dispositivos,

y subsecuentemente transferir esta combinación firmada a los diferentes dispositivos.

13. Un dispositivo dispuesto para realizar el control de acceso a un elemento de contenido, siendo el dispositivo parte de un conjunto de dispositivos, conformando el conjunto de dispositivos un primer dominio que comprende dispositivos que están relacionados con un hogar o un grupo limitado de consumidores, pudiendo el dispositivo manejar un derecho de uso asociado con el elemento de contenido, en donde el dispositivo está dispuesto además para manejar el derecho de uso que se ha dividido en derechos parciales, teniendo cada uno de los derechos parciales una firma digital, estando dispuesto el dispositivo de manera adicional para

- identificar un dispositivo diferente que represente un dominio diferente, para subsecuentemente firmar información que incluya una combinación de

- al menos un derecho parcial y su correspondiente firma,

- una identificación del primer dominio, y

- una identificación de los diferentes dispositivos,

y subsecuentemente transferir esta combinación firmada al dispositivo diferente.

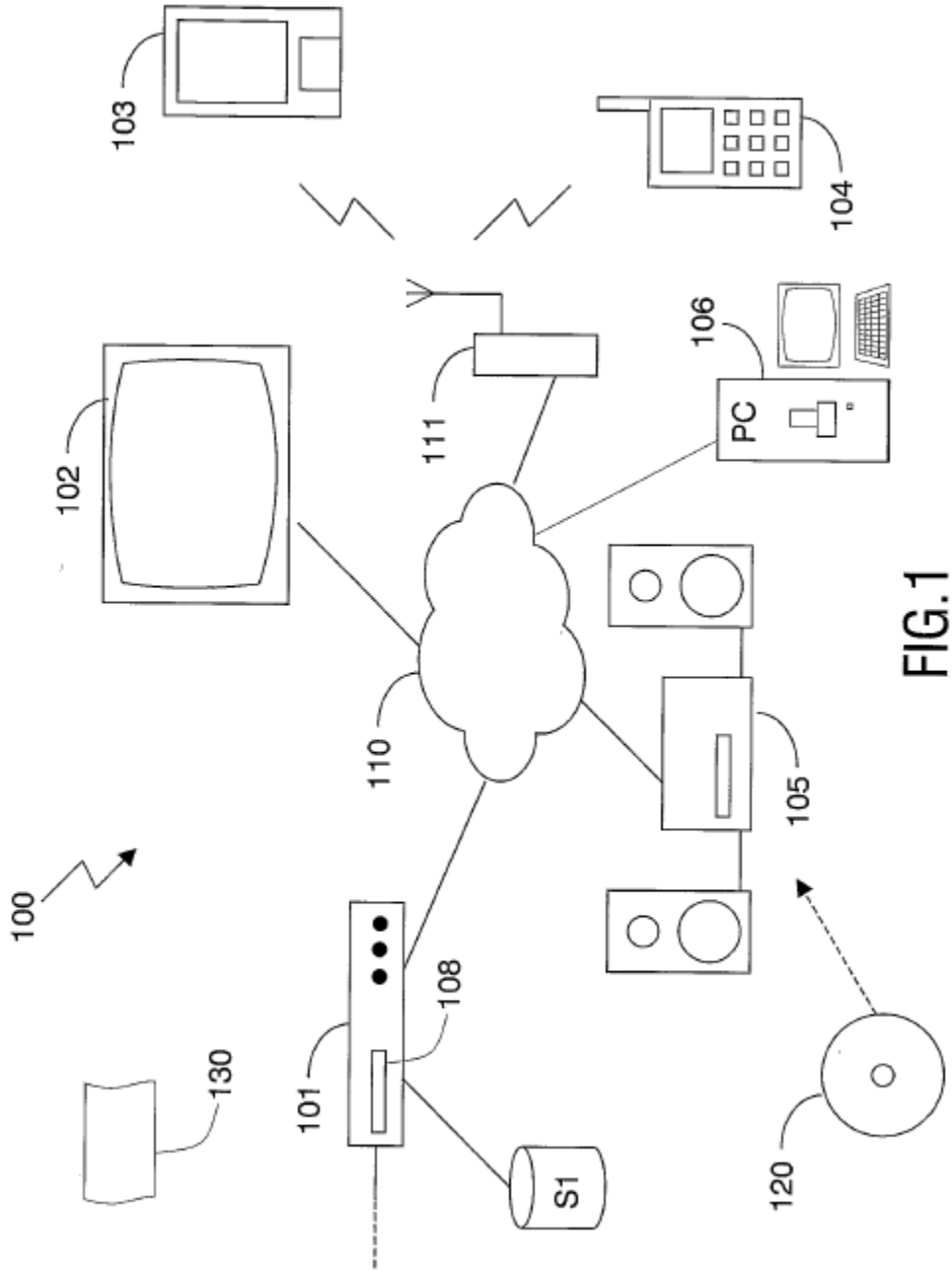

FIG.1

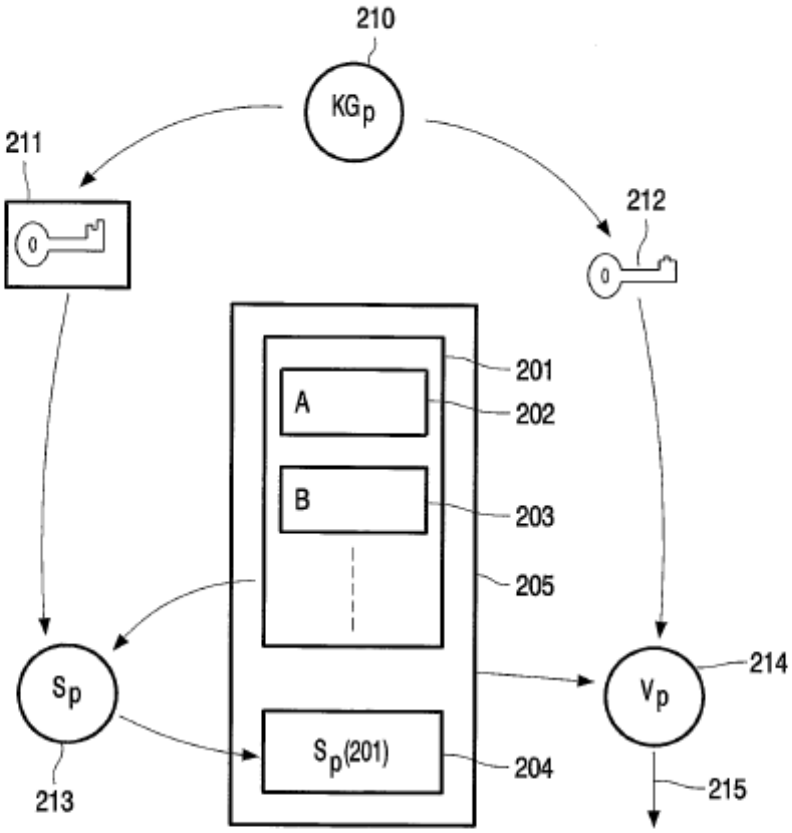

FIG. 2

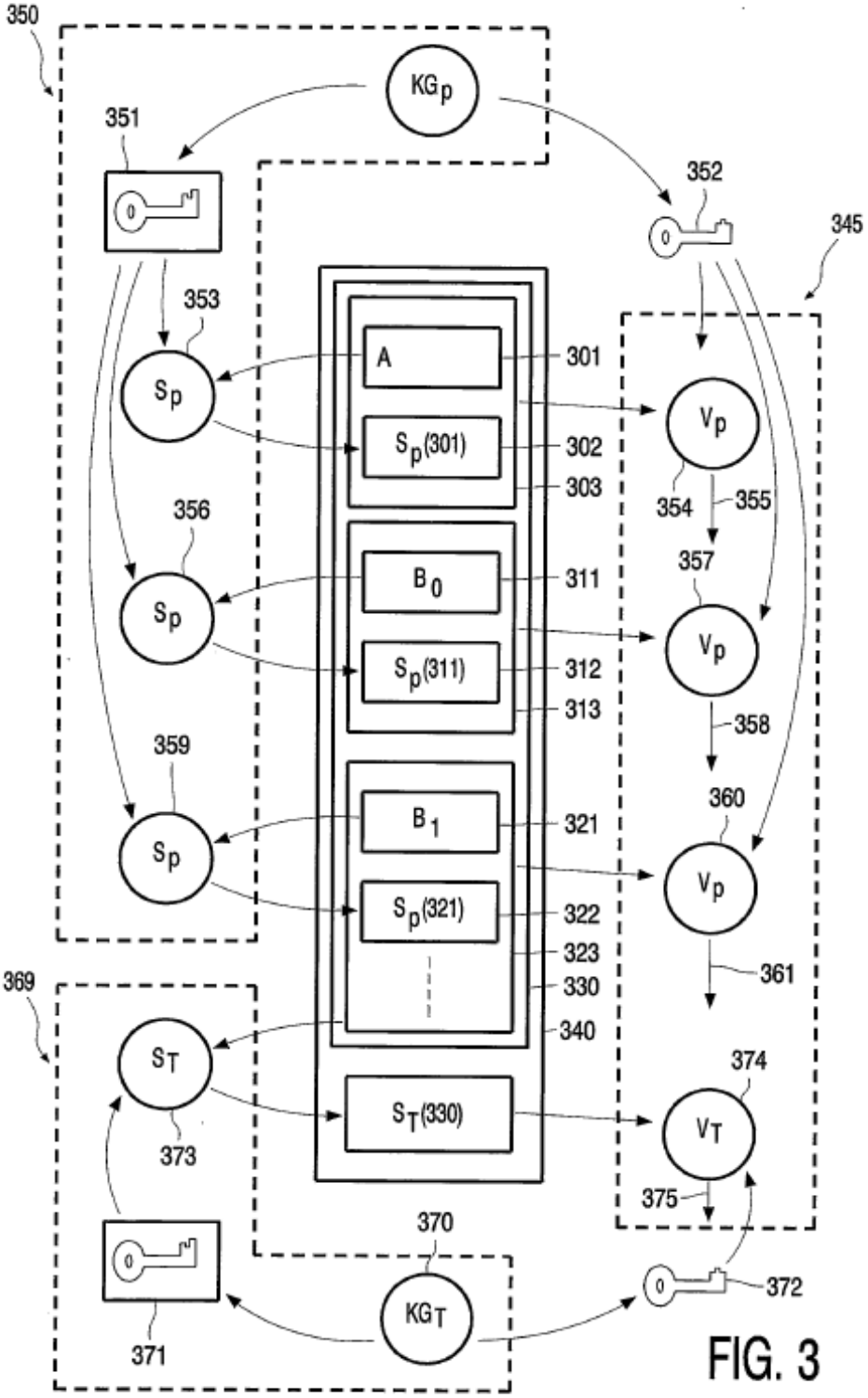
350
KGp
351
352
345
353
A
301
Sp
Vp
Sp(301)
302
303
354
355
356
357
B0
311
Sp
Vp
Sp(311)
312
313
358
359
360
B1
321
Sp
Vp
Sp(321)
322
323
361
369
330
340
ST
374
ST(330)
VT
373
375
370
372
KGT
371

FIG. 3

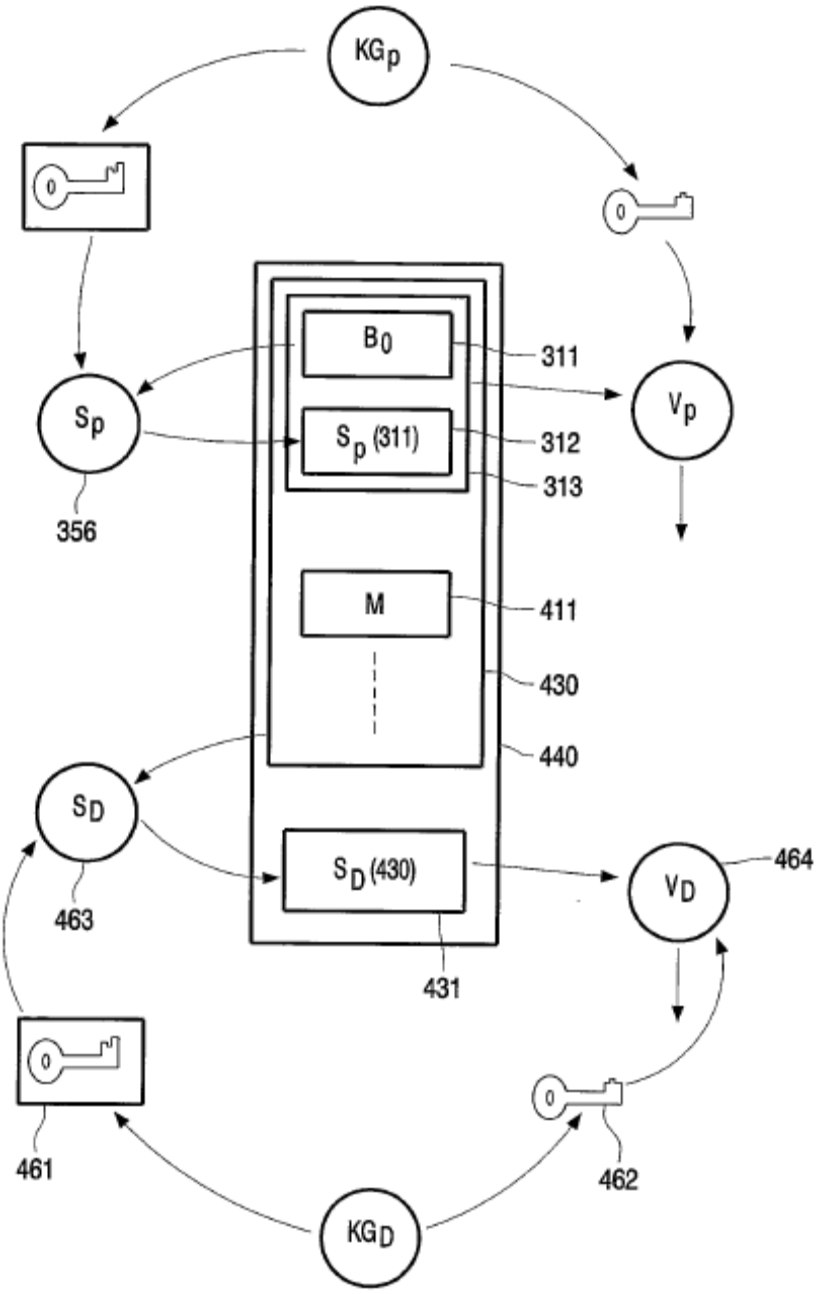
KGp
B0
311
Sp
Sp (311)
312
313
Vp
356
M
411
430
440
SD
SD (430)
VD
464
463
431
461
462
KGD

FIG. 4

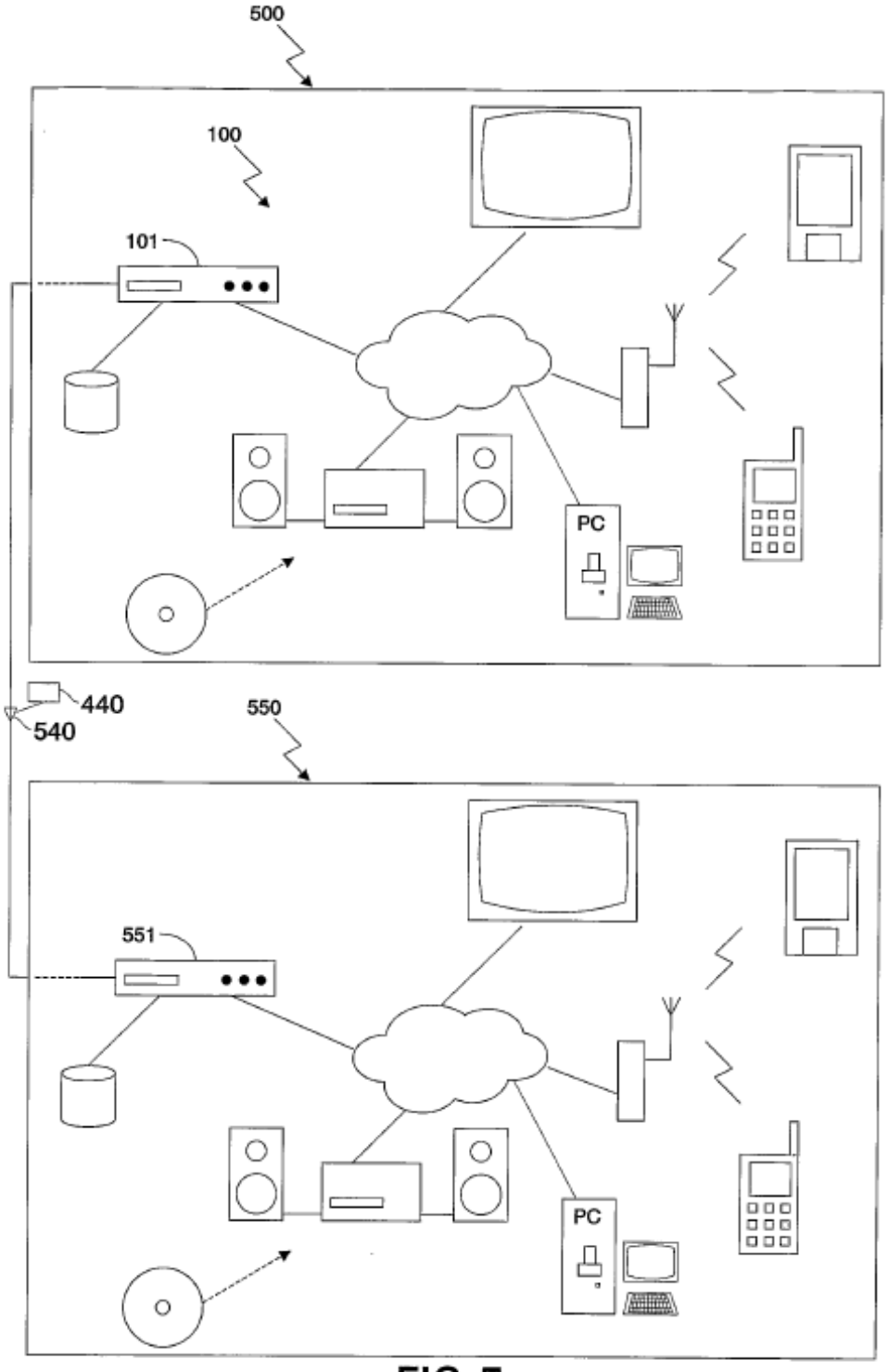

FIG.5

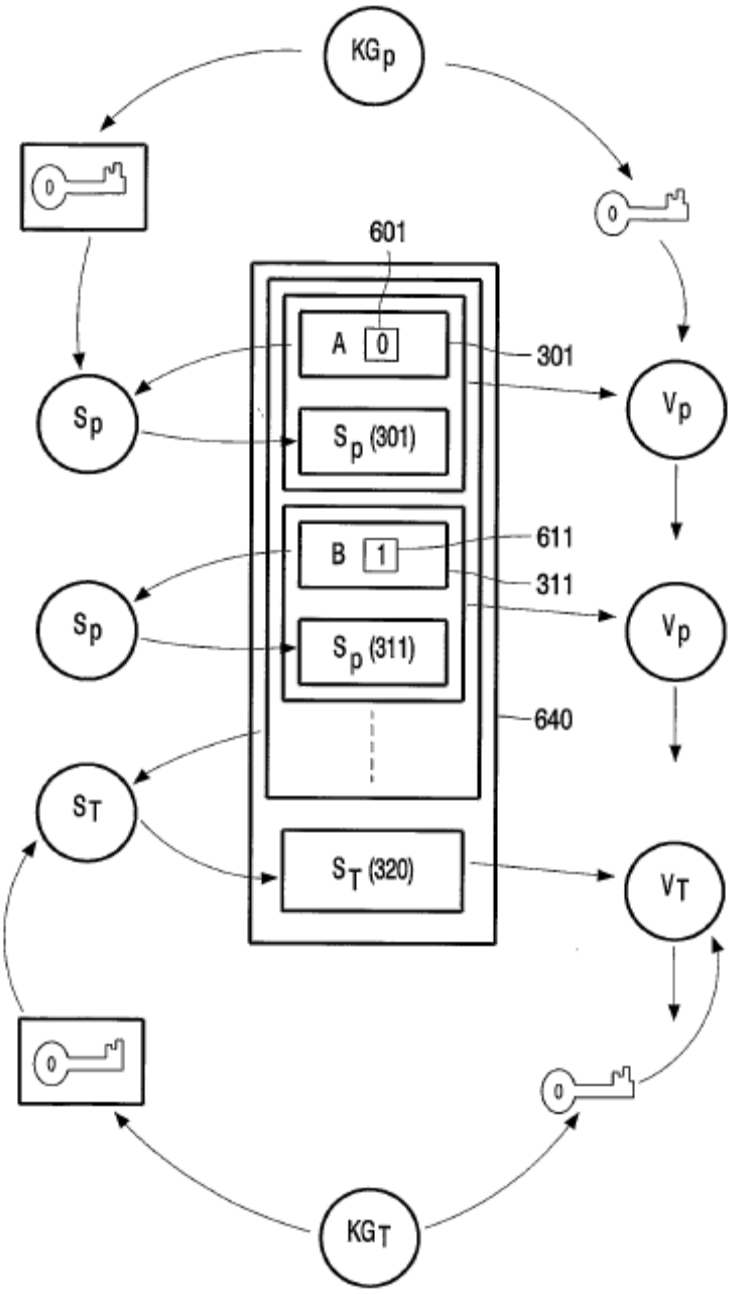
KGp
601
A 0
301
Sp
Sp (301)
Vp
B 1
611
311
Sp
Sp (311)
Vp
640
ST
ST (320)
VT
KGT

FIG. 6

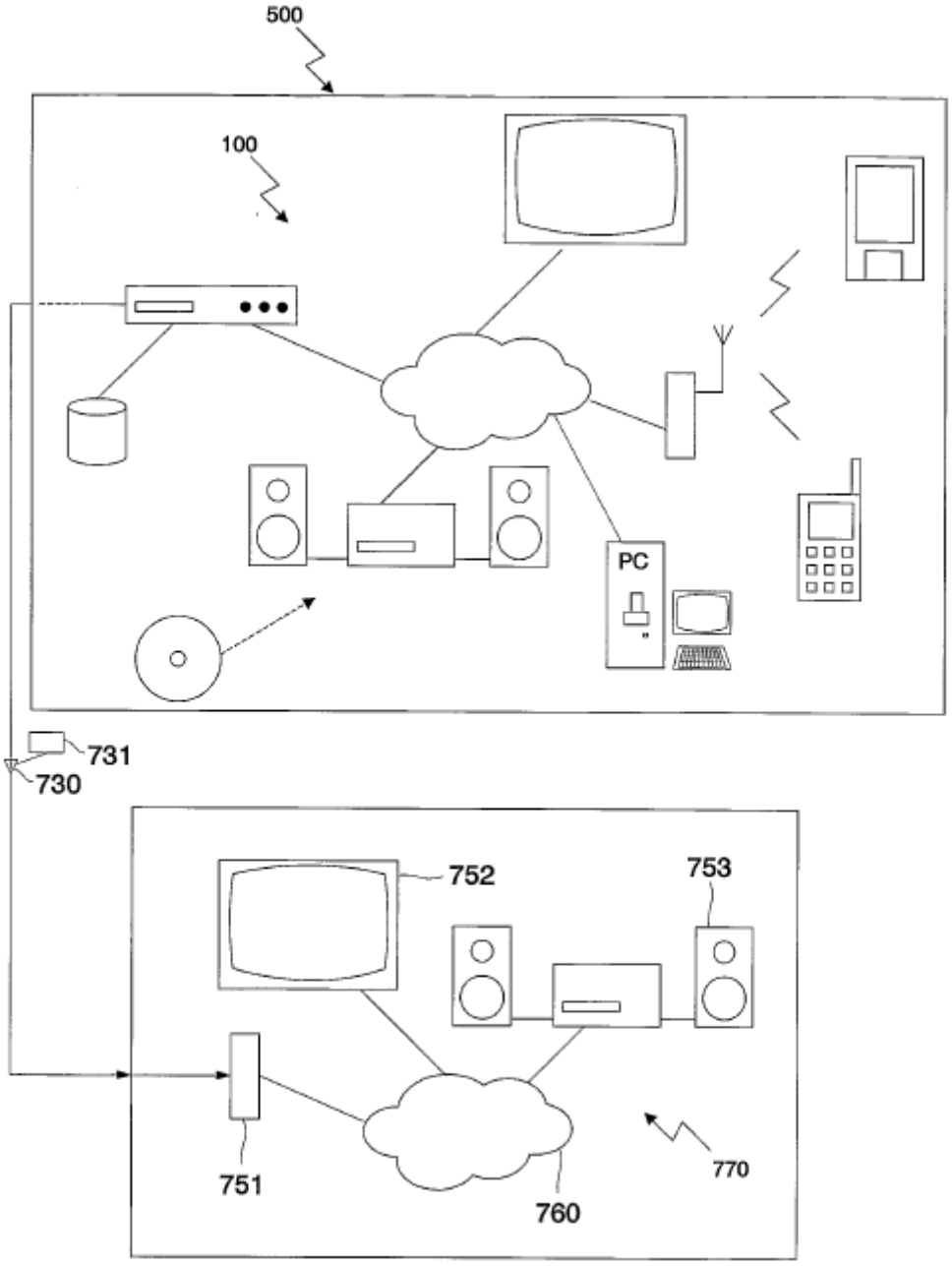

FIG.7

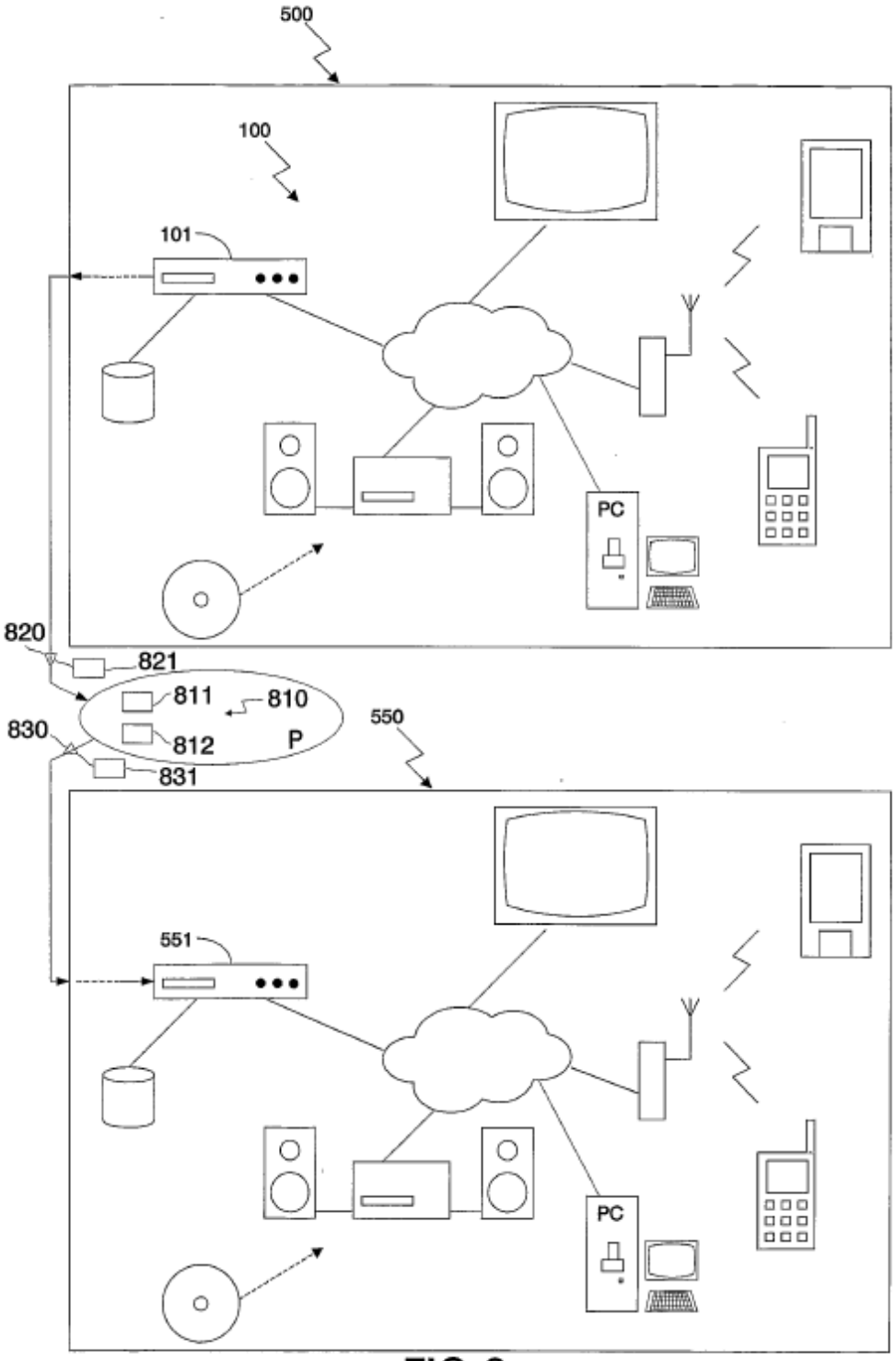

FIG.8