(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 837**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04N 21/258 (2011.01)
H04N 21/472 (2011.01)
H04N 21/462 (2011.01)
G06F 21/10 (2013.01)
H04N 21/254 (2011.01)
H04N 21/835 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.01.2013 PCT/EP2013/051256**

(87) Fecha y número de publicación internacional: **01.08.2013 WO13110669**

(96) Fecha de presentación y número de la solicitud europea: **23.01.2013 E 13707116 (3)**

(97) Fecha y número de publicación de la concesión europea: **22.01.2020 EP 2807810**

(54) Título: **Método y sistema de autorización en un sistema de provisión de contenido**

(30) Prioridad:

23.01.2012 GB 201201063

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.07.2020

(73) Titular/es:

YOUVIEW TV LTD (100.0%)
3rd Floor 10 Lower Thames Street
London EC3R 6YT, GB

(72) Inventor/es:

ROY, ANDRE;
HUNTER, JEFFREY;
POOLE, CHRISTOPHER y
EARNSHAW, NIGEL

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Método y sistema de autorización en un sistema de provisión de contenido

La presente invención se refiere a un sistema de autorización, específicamente, un sistema de autorización para su uso en un sistema de provisión de contenido. Esta invención también se refiere a un método de autorización y a un receptor/decodificador.

En el campo de la transferencia electrónica de datos, ha habido mucha investigación sobre la seguridad y la fiabilidad de la transmisión de datos. Es una propiedad intrínseca (y útil) de los datos electrónicos que se pueden copiar y retransmitir. Se han ideado muchos métodos para superar los aspectos negativos de esta propiedad.

La presente invención se refiere principalmente a la situación en la que los datos están en forma de contenido de audio/vídeo (A/V). En este caso, la seguridad de los datos es importante ya que pueden aplicarse cargos y suscripciones a cierto contenido, y los proveedores de contenido pueden desear mantener el control sobre su contenido y/o asegurarse de que su contenido solo se envíe a un usuario autorizado o a un dispositivo que tenga sido autorizado.

Hay una multitud de proveedores de contenido que utilizan diversos métodos de entrega para transferir datos, tales como la Televisión Digital Terrestre (TDT), Televisión de Protocolo por Internet (IPTV) y Vídeo Bajo Demanda (VOD). Cada uno tiene su propio conjunto de requisitos al autorizar a un usuario, y diferentes requisitos sobre el uso de datos. Por ejemplo, VOD puede tener un límite de tiempo relacionado con cuándo se puede ver, y puede que no sea posible grabar IPTV. Esto crea una red compleja de 'emparejamientos' de confianza entre dispositivos de usuario y proveedores de servicios o contenido.

En sistemas de transmisión de audio/vídeo y provisión de contenido, es deseable autenticar tanto a los usuarios del sistema como al sistema mismo ante los usuarios. En un ejemplo de un sistema de autorización de la técnica anterior, cada dispositivo receptor de contenido separado (por ejemplo, decodificador) producido por un fabricante diferente tiene una relación de confianza independiente con cada proveedor de contenido disponible.

Para que funcione un sistema de provisión de contenido efectivo y eficiente, los proveedores de contenido idealmente tienen una relación de confianza con los dispositivos de consumo y viceversa. Esto es para que los proveedores de contenido sepan que el dispositivo al que suministran contenido es un dispositivo autorizado que, por ejemplo, tiene la suscripción necesaria o el software de Gestión de Derechos Digitales (DRM). Esta relación de confianza también debe funcionar a la inversa; idealmente, el dispositivo del consumidor puede confiar en que los datos que recibe provienen de un proveedor autorizado, para reducir las posibilidades de descarga de software malicioso, por ejemplo. Una solución actual es que cada proveedor de contenido tenga una relación de confianza individual con cada dispositivo (y, por lo tanto, con el usuario). Esto se vuelve ineficiente cuando hay una gran cantidad de proveedores y/o usuarios de contenido. La presente invención tiene como objetivo aliviar al menos algunos de estos problemas.

El documento "Digital Video Broadcasting (DVB); Multimedia Home Platform (MHP) Specification 1.0.3; Draft ES 201 812", 1 de agosto de 2001 (01-08-2001), IEEE, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, XP055080469, vol. V1.1.1, divulga la solución DVB para Plataformas Multimedia Domésticas (MHP). Las MHP ejecutan aplicaciones de software que implementan servicios interactivos. En general, de acuerdo con la presente invención, se proporciona un sistema y un método adaptados para implementar un sistema de autorización de modo que una multitud de consumidores o dispositivos de consumo puedan recibir datos de una multitud de proveedores de contenido de una manera segura y eficiente a través de una autoridad de confianza.

El sistema y el método están adaptados para que los proveedores de contenido y los dispositivos de consumo puedan ser autorizados independientemente como parte de un ecosistema en donde los dispositivos de consumo y los proveedores de contenido puedan reconocerse mutuamente como partes autorizadas dentro del ecosistema.

De acuerdo con un aspecto de la invención, se proporciona un método de acuerdo con la reivindicación 1.

El término "receptor/decodificador", como se usa en el presente documento, puede connotar un receptor para recibir señales codificadas o no codificadas, por ejemplo, señales de televisión y/o radio, que pueden ser difundidas, emitidas, descargadas o transmitidas por algún otro medio. El término también puede connotar un decodificador para decodificar señales recibidas. Las realizaciones de tales receptores/decodificadores pueden incluir un decodificador integral con el receptor para decodificar las señales recibidas, por ejemplo, en un "decodificador", funcionando tal decodificador en combinación con un receptor físicamente separado, o incluyendo tal decodificador funciones adicionales, tal como un navegador web, una grabadora de vídeo o un televisor.

Se contempla que el sistema tal como se describe en el presente documento se pueda implementar completamente en un servidor central, o un conjunto de servidores interconectados, que es/son conectables a una pluralidad de dispositivos de clientes remotos. Como alternativa, los aspectos del sistema pueden implementarse, al menos en

parte, sobre el o cada dispositivo (remoto) cliente/usuario.

Se contempla que los aspectos del sistema, del dispositivo y/o el método de usuario descritos en el presente documento pueden implementarse en un software que se ejecuta en un ordenador, tal como un ordenador personal o un receptor/decodificador (que puede conectarse directamente a un monitor o a un televisor u otro medio de visualización), y debe tenerse en cuenta que los aspectos inventivos pueden residir en el software que se ejecuta en tales dispositivos.

Otros aspectos de este sistema, el dispositivo y/o el método de usuario pueden implementarse en software que se ejecuta en diversos servidores interconectados, y debe apreciarse que los aspectos inventivos pueden residir en el software que se ejecuta en tales servidores.

Otras características de la invención se caracterizan por las reivindicaciones independientes y dependientes.

Cualquier característica del aparato como se describe en el presente documento también se puede proporcionar como una característica del método, y viceversa. Como se usa en el presente documento, los medios más las características funcionales pueden expresarse alternativamente en términos de su estructura correspondiente, tal como un procesador adecuadamente programado y memoria asociada.

Además, las características implementadas en hardware generalmente pueden implementarse en software, y viceversa. Cualquier referencia a las características de software y hardware en el presente documento debe interpretarse en consecuencia.

Las características de esta descripción y/o ventajas de la invención incluyen:

- Un sistema adaptado para permitir que un proveedor de contenido confíe en un dispositivo y un dispositivo para confiar en un proveedor de contenido, sin tener relaciones de confianza individuales, incluida la utilización de una infraestructura de clave pública para este propósito.
- Confianza bidireccional, los proveedores de contenido confían en los dispositivos, los dispositivos confían en los proveedores de contenido.
- Medios para asegurar que un dispositivo (y, por lo tanto, un usuario) tenga los certificados necesarios para el contenido requerido y para proporcionar el contenido de forma segura e intransferible.
- Poner una clave en un dispositivo, donde la clave puede ser conocida o desconocida por el Fabricante del Equipo Original (OEM). Esta clave solo es accesible por el Sistema En Chip (SoC) del dispositivo.
- Una autoridad central que pasa por alto las relaciones de confianza.
- El uso de Infraestructura de Clave Pública (PKI): con una clave segura (Maestra) asociada con el dispositivo.
- Cada dispositivo tiene una identidad única para la protección del contenido y para ayudar con la gestión y la supervisión.
- Claves aprovisionadas para que el dispositivo sea renovable/revocable.
- La Clave Maestra (MK) en el dispositivo no es accesible por el software en el dispositivo que no sea a través del procesador seguro del SoC.
- La Clave Maestra puede derivarse de un secreto que está vinculado permanentemente en el SoC.
- Si el MK es una clave desconocida, se utiliza una clave alternativa para la provisión de claves.
- La Clave Maestra está enraizada y vinculada al SoC.
- Al menos dos 'niveles' de claves: (i) una MK: nada puede cambiar esto, seguro al dispositivo; y (ii) una Clave Operativa (OK): utilizada para las operaciones diarias, y que es renovable/revocable.
- La manera en que se deriva la clave depende de la implementación y puede usar escaleras de claves.
- Las claves pueden tomar la forma de claves privadas asimétricas con certificados de clave pública asociados.
- El dispositivo almacena el certificado de clave pública que corresponde a cada una de las claves privadas mantenidas de forma segura por el dispositivo. A diferencia de los certificados que se utilizan como anclas de confianza, no es necesario mantener estos certificados de forma segura.
- Además de las anclas de confianza, el dispositivo maneja certificados de clave pública que acompañan a documentos y/o datos protegidos por firmas de clave privada para afirmar la autoridad de tales firmas.
- Una autoridad muy confiable, que técnicamente se manifiesta como un certificado X.509 autofirmado.
- El dispositivo tiene la capacidad de administrar de manera segura material de clave confidencial.
- El dispositivo evita la manipulación de los buses de memoria flash, o es robusto contra tal manipulación. Esto típicamente se logra al cargar el código en la Memoria de Acceso Aleatorio Dinámico Sincrónico (SDRAM) antes de la verificación y ejecución, o por medios físicos.
- El dispositivo protege contra la alteración o el reemplazo de todos los cargadores de arranque, el kernel de Linux, el sistema de archivos raíz de Linux y todos los demás sistemas de archivos dentro del dispositivo desde el cual se puede ejecutar el código o se almacenan las anclas de confianza.
- El dispositivo verifica el software de la plataforma en cada arranque.
- Los niveles posteriores de un arranque pueden verificarse mediante firmas utilizando claves aseguradas en niveles anteriores.

Se puede encontrar más información en los siguientes documentos:

- [CMS] - Cryptographic Message Syntax (CMS) - RFC 3852 - Julio de 2004
- [PKIX] - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile - RFC 5280 - mayo de 2008
- [RFC 2585] - Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP - RFC 2585 - mayo de 1999
- [RFC 3279] - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile - abril de 2002
- [TR-069] - CPE WAN Management Protocol v1.1 - diciembre de 2007

Además, se hace referencia al número de solicitud de patente del Reino Unido GB1020290.1, en nombre de You-View TV Ltd.

La invención se describe ahora, puramente a modo de ejemplo, con referencia a las figuras adjuntas, en los que:

La figura 1 muestra una visión general esquemática de un sistema de autorización;
la figura 2 muestra un diagrama esquemático más detallado de una porción del sistema de autorización de la figura 1;
la figura 3 muestra un ejemplo del sistema de autorización de la figura 2 en uso;
La figura 4 muestra un diagrama de las etapas de procesamiento realizados por el sistema de la figura 2 en operación;
la figura 5 muestra detalles de las formas en que las claves se almacenan y utilizan en un dispositivo de usuario del sistema de la figura 2; y
la Figura 6 muestra un ejemplo de una Jerarquía de Confianza. Visión general

La figura 1 muestra una visión general esquemática de un sistema de autorización 10 para un sistema de provisión de contenido. El sistema de autorización 10 incluye una Autoridad de Confianza/Operador del sistema 226 que está adaptado para examinar y autorizar una pluralidad de dispositivos de usuario 56, siendo cada uno opcionalmente proporcionado por un fabricante diferente, así como una pluralidad de proveedores de contenido independientes y/o separados 52, cada uno adaptado para proporcionar artículos de contenido de datos a los usuarios, a través de dichos dispositivos de usuario 56. La autoridad de confianza/operador del sistema 226 también se denomina en el presente documento como la autoridad más confiable, o la autoridad del certificado raíz, dependiendo del contexto.

El sistema de suministro de contenido se utiliza para la provisión de contenido a los usuarios, típicamente en forma de contenido multimedia de audio/vídeo, tal como contenido de difusión. En este caso, los dispositivos de usuario 56 tienen forma de decodificadores (STB), o similares, conectables a pantallas tal como unidades de pantalla visual (VDU), televisores o monitores.

El sistema de autorización 10 utiliza Infraestructura de Clave Pública (PKI) que implica el uso de claves y certificados públicos y privados para implementar un modelo de confianza entre el operador del sistema 226, la pluralidad de dispositivos de usuario 56, y cada uno de los proveedores de contenido 52 para asegurar que todas las entidades en el sistema 10 estén autenticadas y autorizadas apropiadamente.

El Operador del Sistema 226 actúa como una autoridad de certificación raíz, emitiendo y verificando certificados de las otras entidades en el sistema 10 (como se tratará con más detalle a continuación).

Por lo tanto, el operador del sistema 226 determina qué dispositivos de usuario 56 y proveedores de contenido 52 están autorizados a formar parte del sistema 10.

Este sistema de autenticación 10 da como resultado un modelo de confianza 'horizontal' en el que numerosos fabricantes de dispositivos pueden usar el mismo modelo de confianza para permitir que sus dispositivos reciban datos de múltiples proveedores de contenido diferentes. Esto es opuesto a un modelo 'vertical' en el que diferentes fabricantes deben tener relaciones de confianza separadas con cada proveedor de contenido.

De esta manera, el número de 'emparejamientos' 222 de confianza requeridos (ver figura 1) entre un número p de proveedores de contenido 52 y un número m de dispositivos 56 se reduce de un p x m esperado a un p + m más eficiente. Las ganancias de eficiencia se vuelven cada vez más grandes a medida que se hacen más grandes p y m. Este sistema 10 también es mucho más fácil de agregar o modificar en una fase posterior. Por ejemplo, si hubiera otro proveedor de contenido 52 que desee unirse al sistema, solo se necesitaría un acuerdo de confianza adicional 222; previamente, sin el uso de Autoridad de Confianza 226, sería necesario establecer un nuevo acuerdo de confianza 222 para cada dispositivo 56, que podría volverse oneroso.

Como se muestra en las figuras 2 y 3, el operador del sistema 226 autoriza a los proveedores de contenido 52 y a los dispositivos 56 de la siguiente manera. El operador del sistema 226 proporciona un certificado raíz público TA1 100 (una "raíz de confianza") tanto para los dispositivos 56 como para los proveedores de contenido 52. La provisión de TA1 100 al dispositivo 56 permite al dispositivo 56 validar un certificado C5 120 que se presentará al dispositivo

56 junto con una aplicación de software específica (aplicación) 302 firmada con ese certificado C5. Esta aplicación es un complemento de software proporcionado por cada proveedor de contenido 52 y permite que el dispositivo 56 acceda al contenido de datos proporcionado por el proveedor de contenido 52, o facilita otros servicios proporcionados por el proveedor de contenido 52. El certificado C5 120 puede reconocerse como originario del operador del sistema 226, ya que se deriva o está enraizado en TA1 100 (ver la figura 2). TA1 100 es un certificado autofirmado típicamente basado en el estándar X.509.

Las aplicaciones 302 están autorizadas directamente por el operador del sistema 226 o por el proveedor de contenido 52 con el consentimiento del operador del sistema 226. De este modo, el dispositivo 56 puede reconocer la aplicación 302 como auténtica y confiar en la aplicación 302 para obtener contenido de un proveedor de contenido autorizado 52. Lo contrario también es cierto, el proveedor de contenido 52 puede ver que el dispositivo 56 está autorizado para usar la aplicación 302 para acceder al contenido (como se explica con más detalle a continuación).

Como se muestra en la figura 2, el operador del sistema 226 emite un certificado de clave pública operativa 108 (por ejemplo, OK2) a un dispositivo 56 que desea autenticarse. Esto puede seguir una etapa en el que el dispositivo 56 que solicita la autenticación transmite una porción pública de un par de claves criptográficas OK2 que posee al operador del sistema 226. En este caso, el operador del sistema 226 firma la porción pública de OK2 y emite el dispositivo 56 con el correspondiente certificado 108 de OK2. La provisión de este certificado de clave pública puede ocurrir a través de una autoridad de certificado intermedia 102. OK2 108 está enraizado en o derivado de, la raíz de confianza TA1 100 y puede ser reconocida como tal por cualquier entidad con conocimiento de TA1 100. De este modo, un proveedor de contenido 52 puede reconocer dispositivos autorizados 56 comparando el certificado OK2 108 con el certificado TA1 100 en poder del proveedor de contenido 52.

Como se ha mencionado anteriormente, cada proveedor de contenido 52 proporciona una aplicación 302 a un dispositivo de usuario 56 para permitirle comunicarse y/o interactuar con el proveedor de contenido 52 y, por lo tanto, recibir artículos de contenido y/o servicios del proveedor de contenido 52. El dispositivo 56 y el proveedor de contenido 52 se comunican usando esta aplicación 302. Cada aplicación 302 está asociada con un proveedor de contenido particular 52. Las aplicaciones 302 se utilizan para que cada proveedor de contenido 52 pueda implementar su propio método de comunicación con un dispositivo 56.

Cada aplicación 302 también está autenticada o autorizada para que los dispositivos 56 sepan que el contenido que reciben a través de la aplicación 302 es de un proveedor de contenido autorizado 52. Estas aplicaciones 302 se autorizan mediante su firma utilizando el certificado 120 de "firma de aplicaciones" C5, emitido por el operador del sistema 226 o por una entidad intermedia 106. El certificado C5 120 también está enraizado en TA1 100 para que otras entidades en el sistema 10 puedan confirmar la autenticidad de la aplicación 302. El proceso de firmar realmente las aplicaciones 302 con el certificado C5 120 puede ser manejado por los propios proveedores de contenido 52 o por el operador del sistema 226. El proveedor de contenido 52 puede proporcionar el certificado C5 120 junto con, o empaquetado en, la aplicación 302. La emisión del certificado C5 120 al proveedor de contenido 52 constituye efectivamente la autorización del proveedor de contenido 52. El certificado C5 120 puede basarse en una clave pública C5, que forma la mitad de un par de claves pública/privada asimétrica, originalmente en poder del proveedor de contenido 52, que es proporcionada por el proveedor de contenido 52 al operador del sistema 226 para que lo firme el operador del sistema 226.

Una vez que se hayan completado las etapas de autenticación anteriores, el sistema 10 comprende un proveedor de contenido confiable 52 con una aplicación firmada 302 y un dispositivo confiable 56 con un certificado de clave pública operacional OK2 108. La aplicación 302 se pasa luego al dispositivo 56, directamente por el operador del sistema, el proveedor de contenido 52, o por otros medios. Generalmente, cuando un dispositivo de usuario está encendido, las aplicaciones 302 correspondientes a proveedores de contenido 52 que han sido recientemente autorizadas por el operador del sistema 226 se descargan en el dispositivo de usuario 56 para que el usuario pueda acceder al contenido de los nuevos proveedores de contenido 52 utilizando estas nuevas aplicaciones 302. Este proceso ocurre repetidamente de modo que el dispositivo 56 posee una aplicación 302 para cada proveedor de contenido 52 al que tiene acceso.

Una vez que se hayan completado las etapas de anteriores, el operador del sistema 226 ya no necesita estar directamente involucrado en la comunicación posterior entre el dispositivo de usuario 56 y el proveedor de contenido 52. El operador del sistema 226 tampoco tiene un papel directo en la transferencia de contenido 76. Después de que los dispositivos 56 y los proveedores de contenido 52 hayan sido autorizados o autenticados, el operador del sistema 226 efectivamente "sale".

Cuando el dispositivo 56 solicita contenido de un determinado proveedor de contenido 52, se ejecuta la aplicación relevante 302. La aplicación 302 se comunica con el proveedor de contenido 52, pasar el certificado de clave pública OK2 108 al proveedor de contenido 52. El proveedor de contenido 52 puede verificar si el dispositivo de usuario 56 está autorizado verificando OK2 108 contra TA1 100. El dispositivo 56 lleva a cabo un procedimiento similar para autenticar la aplicación 302 comprobando C5 120, que se usó para firmar la aplicación 302, contra TA1 100. Una vez que estas etapas se hayan completado con éxito, el dispositivo 56 confía en el proveedor de contenido 52 y el proveedor de contenido 52 confía en el dispositivo 56. El contenido solicitado puede luego pasar del proveedor de

contenido 52 al dispositivo 56 utilizando un medio de comunicación, codificación y cifrado adecuado.

Los certificados OK2 108 y C5 120 son revocables. Esto es para que, si la suscripción de un dispositivo ha expirado, por ejemplo, ya no puede recibir cierto contenido. Esto podría lograrse agregando un límite de tiempo al certificado, o una lista de revocación de certificados (CRL) accesible para que los dispositivos 56 y los proveedores de contenido 52 puedan verificar si los certificados siguen siendo válidos.

La figura 3 muestra el sistema descrito anteriormente en uso. El operador del sistema 226 autoriza a los proveedores de contenido 52 emitiendo los certificados C5 120. La aplicación 302 proporcionada por un proveedor de contenido 52 se firma utilizando el certificado C5 120, ya sea por el propio proveedor de contenido 52 o por el operador del sistema 226. El operador del sistema 226 también proporciona a los proveedores de contenido 52 TA1 100. El operador del sistema 226 autoriza el dispositivo 56 emitiendo OK2 108. El dispositivo 56 también está provisto de TA1 100. Como se ha mencionado anteriormente, las aplicaciones 302 correspondientes a cada proveedor de contenido 52 permiten la comunicación directa entre cada dispositivo 56 (uno de los cuales se muestra en la figura 3) y cada proveedor de contenido 52. Se muestra que el dispositivo 56 tiene otro software embebido tal como el software 402 de Gestión de Derechos Digitales (DRM) y una caja de claves 400 donde se pueden almacenar claves privadas. Una vez que los proveedores de contenido 52, las aplicaciones 302 y el dispositivo 56 han recibido sus certificados, como se describió anteriormente, el contenido 76 se puede transferir directamente entre ellos. Esto ocurre directamente entre el proveedor de contenido 52 y el dispositivo 56 usando la aplicación correspondiente 302.

La figura 4 muestra un proceso llevado a cabo por los diversos elementos del sistema 10 en uso. Generalmente, por supuesto, hay numerosos proveedores de contenido 52 y dispositivos de usuario 56, solo se muestra uno de cada uno para mayor claridad.

El proceso comienza con el operador del sistema 226 que proporciona un certificado de clave pública TA1 100 a un proveedor de contenido 52 en la etapa S1. TA1 100 es la raíz de confianza, o alternativamente un certificado derivado o enraizado, TA1 100. Este proceso puede ocurrir a través de una entidad intermedia 106 como se muestra en la figura 2. Este certificado raíz público TA1 100 permite que el proveedor de contenido 52 verifique si los dispositivos de usuario particulares 56 están autorizados o no.

El operador del sistema 226 autoriza entonces un dispositivo de usuario 56 en la etapa S2. El operador del sistema 226 proporciona un certificado de clave pública OK2 108, que tiene sus raíces en TA1 100, al dispositivo de usuario 56 junto con TA1 100. De nuevo, esto puede ocurrir a través de una entidad intermedia 102 como se muestra en la figura 2. La etapa adicional de enraizar OK2 108 en TA1 100, en lugar de usar TA1 100 directamente, se incluye para que el operador del sistema 226 pueda revocar la autorización de cualquier dispositivo de usuario 56 en cualquier momento sin tener que cambiar la raíz de confianza TA1 100.

La etapa final realizado por el operador del sistema 226 es autorizar una aplicación 302 proporcionada por un proveedor de contenido 52 en la etapa S3. En un ejemplo, un proveedor de contenido 52 presenta una aplicación 302 al operador del sistema 226 para su autorización. El operador del sistema 226 firma la aplicación 302 utilizando el certificado de firma de la aplicación C5 120, que lo identifica como una aplicación autorizada para todos los miembros del sistema 10. Como alternativa, el operador del sistema 226 emite el proveedor de contenido con el certificado C5 120 y el proveedor de contenido luego firma la aplicación 302 usando este certificado. En ciertos ejemplos, el certificado C5 puede ser proporcionado por una autoridad de certificado intermedia confiable 106. Las etapas S1-S3 pueden ocurrir en cualquier orden, o cuando el sistema lo requiera, por ejemplo, cuando se configura un nuevo proveedor de contenido 52.

Las etapas S4-S7 se realizan preferentemente independientemente del operador del sistema 226, con el proveedor de contenido 52 comunicándose directamente con el dispositivo de usuario 56. La aplicación autorizada/firmada 302 se envía al dispositivo de usuario 56, típicamente empaquetado junto con el certificado C5 120, y el certificado C5 120 y la aplicación firmada 302 son verificados en la etapa S4 por el dispositivo de usuario 56 para que el dispositivo de usuario 56 sepa que la aplicación ha sido autorizada. Esta verificación implica verificar el certificado C5 120 contra TA1 100, que posee el dispositivo 56 y que verifica la validez del certificado C5 120 (tal como su fecha de vencimiento y las políticas pertinentes).

El dispositivo de usuario 56 luego solicita contenido del proveedor de contenido 52, utilizando la aplicación del proveedor de contenido relevante 302. El proveedor de contenido 52 luego verifica la autenticidad del dispositivo de usuario 56 en la etapa S6 verificando OK2 contra TA1, que también posee el proveedor de contenido 52. La autenticidad del certificado C5 120 también puede ser verificada nuevamente en esta fase por el dispositivo 56 como se describe anteriormente; cuando corren/se ejecutan aplicaciones 302.

Una vez que la autorización ha sido confirmada mutuamente, la provisión de contenido puede tener lugar. Este proceso puede ocurrir en un canal exclusivo para el proveedor de contenido 52 y el dispositivo de usuario 56, y puede estar cifrado. El proveedor de contenido 52 luego envía el contenido en la etapa S7 a través de la aplicación 302.

La figura 5 muestra el uso y almacenamiento de claves en el dispositivo 56. En un ejemplo, una autoridad de aprovisionamiento 54 está autorizada por el Operador del Sistema 226 y suministra un dispositivo de usuario 56 con un conjunto de claves criptográficas. En un ejemplo, la autoridad de aprovisionamiento 54 es operada o administrada por el fabricante del equipo original (OEM) que produce los dispositivos de usuario 56.

El dispositivo de usuario 56 comprende un Sistema en un Chip (SoC) 60 en combinación con el almacenamiento local 58 y es típicamente un decodificador (STB), receptor-decodificador, o un ordenador personal (PC), o cualquier dispositivo adaptado para enviar y recibir datos, específicamente contenido de audio/vídeo. De manera similar, el proveedor de contenido 52 puede ser un proveedor de contenido de audio/vídeo, o cualquier entidad que proporcione datos.

En este ejemplo, el sistema emplea varios tipos generales de claves criptográficas:

- Una sola clave maestra (MK) 62
  MK 62 es la clave criptográfica de más alto nivel, y es la base (directa o indirectamente) para todos los demás certificados de clave pública y claves utilizadas por el dispositivo de usuario. MK 62 está típicamente codificado durante la fabricación del dispositivo 56 para que otras claves seguras se puedan derivar de forma segura. MK 62 no es accesible a ninguna parte del dispositivo 56 aparte del procesador seguro en el SoC 64. MK 62 es, o se deriva de, un secreto único del dispositivo que está vinculado en el SoC 60 durante la fabricación del dispositivo.

- Se utiliza un conjunto de certificados de clave pública operativa (OK) 68 OK 68 en la operación diaria del dispositivo 56, por ejemplo, durante la solicitud y recepción de contenido, y durante la ejecución y actualización de software. OK2 108 descrito anteriormente es un ejemplo de un certificado de clave pública operacional. Estos certificados pueden renovarse, cambiarse o revocarse por el Operador del Sistema 226. Estos certificados pueden ser proporcionados y renovados de acuerdo con las suscripciones de un usuario, o definidos por los Proveedores de Contenido 52 por ejemplo. En algunas realizaciones, estos certificados se proporcionan durante la fabricación.

Se muestra un solo OK 68, pero en la práctica hay varios de estos, así como otros tipos de claves, pero solo un único MK 62.

Ahora se proporcionan más detalles relacionados con el sistema de autorización 10.

El sistema de autorización y el modelo de confianza descritos proporcionan las siguientes ventajas y/o funciones:

- Protección de contenido de audio/vídeo (A/V) utilizando los mecanismos de protección de contenido definidos, incluida la Gestión de Derechos Digitales (DRM).
- Permitir a los proveedores de contenido verificar que su contenido vaya a un dispositivo compatible.
- Proteger la confidencialidad de los datos del usuario.
- Proporcionar un medio seguro para actualizar el software en los dispositivos.
- Proporcionar un medio para validar los datos de configuración.
- Controlar qué aplicaciones pueden ejecutarse en un dispositivo cliente y otorgar acceso apropiado a las Interfaces de Programación de Aplicaciones (API).
- Permitir la gestión remota segura de los dispositivos (donde sea compatible y donde el usuario lo permita).

Jerarquía de confianza de la plataforma

El Operador del Sistema (226, figura 1) es responsable de la Jerarquía de Confianza de Plataforma que se subdivide en varios niveles que forman una jerarquía, cada parte asociada con diferentes aspectos o áreas del sistema. La figura 6 muestra un ejemplo de una Jerarquía de Confianza de Plataforma formada por una pluralidad de activos confiables operativos, que comprende una Autoridad de Certificado Raíz 226 y tres Autoridades de Certificación (CA) intermedias para: Servicio e Identidad del Dispositivo 102, Gestión de Plataforma 104; y Gestión de Aplicaciones 106. Cabe señalar que la figura 6 muestra un ejemplo de una posible jerarquía y muchos otros ejemplos están dentro del alcance de la invención.

Se entenderá que la presente invención se ha descrito anteriormente únicamente a modo de ejemplo, y se pueden realizar modificaciones de detalle dentro del alcance de la invención.

Los números de referencia que aparecen en las reivindicaciones son solo a modo de ilustración y no tendrán efecto limitante sobre el alcance de las reivindicaciones.

REIVINDICACIONES

1. Un método para autorizar múltiples dispositivos de usuario (56) y múltiples proveedores de contenido (52) en un sistema de provisión de contenido (10), comprendiendo el método:

proporcionar a cada proveedor de contenido un certificado de autorización de proveedor de contenido (100);
proporcionar a cada dispositivo de usuario un certificado de autorización de dispositivo de usuario (100), en donde los certificados de autorización de proveedor de contenido para los múltiples proveedores de contenido y los certificados de autorización de dispositivo de usuario para los múltiples dispositivos de usuario se originan a partir de una fuente común; y determinar si cada proveedor de contenido (52) y cada dispositivo de usuario (56) está autorizado a participar en el sistema de provisión de contenido a través de un intercambio mutuo y comparación de dichos certificados entre proveedores de contenido y dispositivos de usuario respectivos;
en donde cada dispositivo de usuario está configurado para ejecutar una aplicación (302) proporcionada por cada proveedor de contenido respectivo para permitir que dicho dispositivo de usuario interactúe con dicho proveedor de contenido.

2. Un método de acuerdo con la reivindicación 1, que además comprende firmar dicha aplicación con el certificado de autorización de proveedor de contenido (100) para autenticar o autorizar dicha aplicación a los dispositivos de usuario.

3. Un método de acuerdo con la reivindicación 2, en donde la aplicación está firmada por una Autoridad de Certificado Raíz.

4. Un método de acuerdo con la reivindicación 3, en donde la aplicación está firmada por el proveedor de contenido.

5. Un método de acuerdo con cualquiera de las reivindicaciones 2 a 4, en donde la aplicación firmada se proporciona al dispositivo de usuario a través del proveedor de contenido y/o a través de un servidor central que forma parte del sistema de provisión de contenido.

6. Un método de acuerdo con la reivindicación 5, en donde la aplicación firmada está empaquetada junto con el certificado de autorización del proveedor de contenido.

7. Un método de acuerdo con la reivindicación 6, en donde el dispositivo de usuario verifica la autorización de la aplicación en una o más de las siguientes fases: la descarga de la aplicación al dispositivo de usuario; la instalación de la aplicación en el dispositivo de usuario; y la ejecución de la aplicación en el dispositivo de usuario.

8. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 7, en donde la aplicación permite a un proveedor de contenido transferir artículos de contenido, típicamente artículos de medios audio/visuales a un dispositivo de usuario.

9. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 8, en donde la aplicación permite la comunicación directa entre el proveedor de contenido y el dispositivo de usuario.

10. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 9, en donde la aplicación permite una comunicación cifrada entre el proveedor de contenido y el dispositivo de usuario.

11. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el dispositivo de usuario transmite su certificado a un proveedor de contenido junto con una solicitud de contenido y en donde el proveedor de contenido verifica la autorización del dispositivo de usuario para determinar de ese modo si el dispositivo de usuario es un dispositivo de usuario autorizado dentro del sistema de provisión de contenido.

12. Un sistema para autorizar múltiples dispositivos de usuario (56) y múltiples proveedores de contenido (52) en un sistema de provisión de contenido (10), comprendiendo el sistema:

múltiples dispositivos de usuario (56) y múltiples proveedores de contenido (52);
medios (226) para proporcionar a cada proveedor de contenido un certificado de autorización de proveedor de contenido (100);
medios (226) para proporcionar a cada dispositivo de usuario un certificado de autorización de dispositivo de usuario (100), en donde los certificados de autorización de proveedor de contenido para los múltiples proveedores de contenido y el certificado de autorización de dispositivo de usuario para los múltiples dispositivos de usuario se originan a partir de una fuente común; y
medios para determinar si cada proveedor de contenido y cada dispositivo de usuario está autorizado a participar en el sistema de provisión de contenido a través de un intercambio mutuo y comparación de dichos certificados entre proveedores de contenido y dispositivos de usuario respectivos.
en donde cada dispositivo de usuario está configurado para ejecutar una aplicación (302) proporcionada por cada proveedor de contenido respectivo para permitir que dicho dispositivo de usuario interactúe con dicho

proveedor de contenido.

13. Un sistema de acuerdo con la reivindicación 12, en donde el o cada dispositivo de usuario tiene la forma de un receptor/decodificador, por ejemplo, un decodificador, STB, preferentemente conectable a un medio de visualización tal como un televisor.

14. Un sistema de acuerdo con la reivindicación 13, en donde cada dispositivo de usuario y/o proveedor de contenido es conectable a una red de comunicación.

15. Un sistema de acuerdo con cualquiera de las reivindicaciones 12 a 14, que además comprende un servidor central que comprende medios para generar o firmar los certificados.

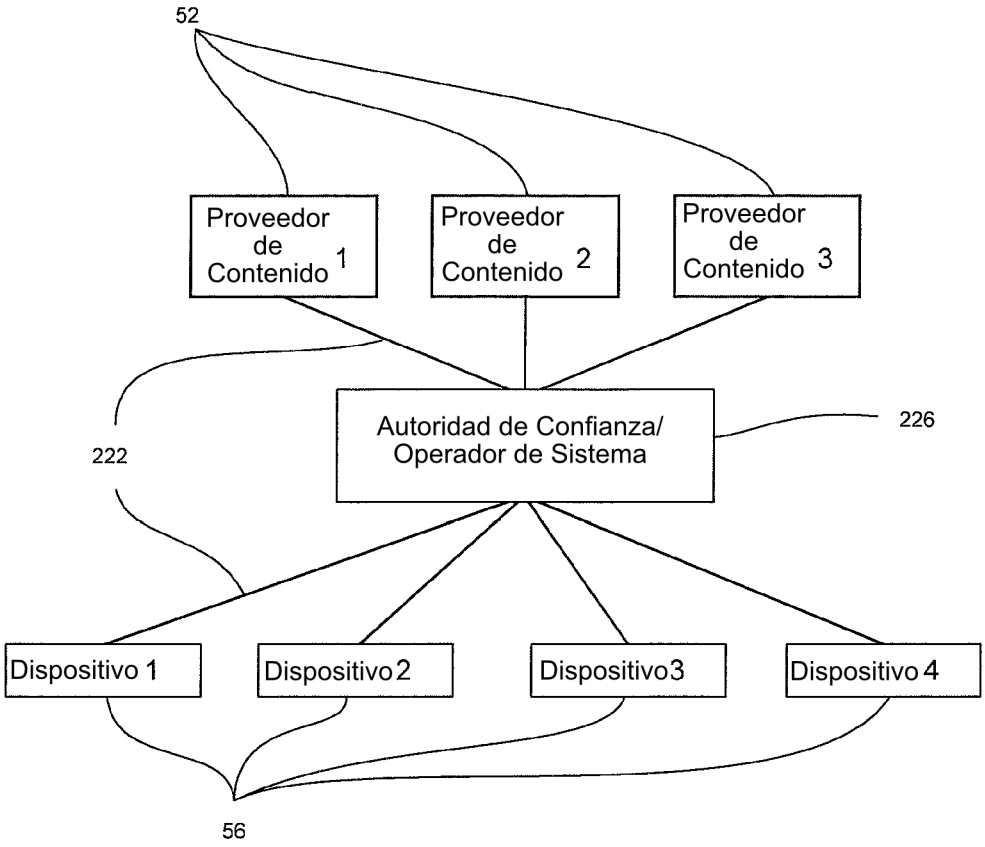
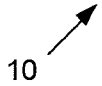

52
Proveedor de Contenido 1
Proveedor de Contenido 2
Proveedor de Contenido 3
222
Autoridad de Confianza/ Operador de Sistema
226
Dispositivo 1
Dispositivo 2
Dispositivo 3
Dispositivo 4
56

Figura 1


10

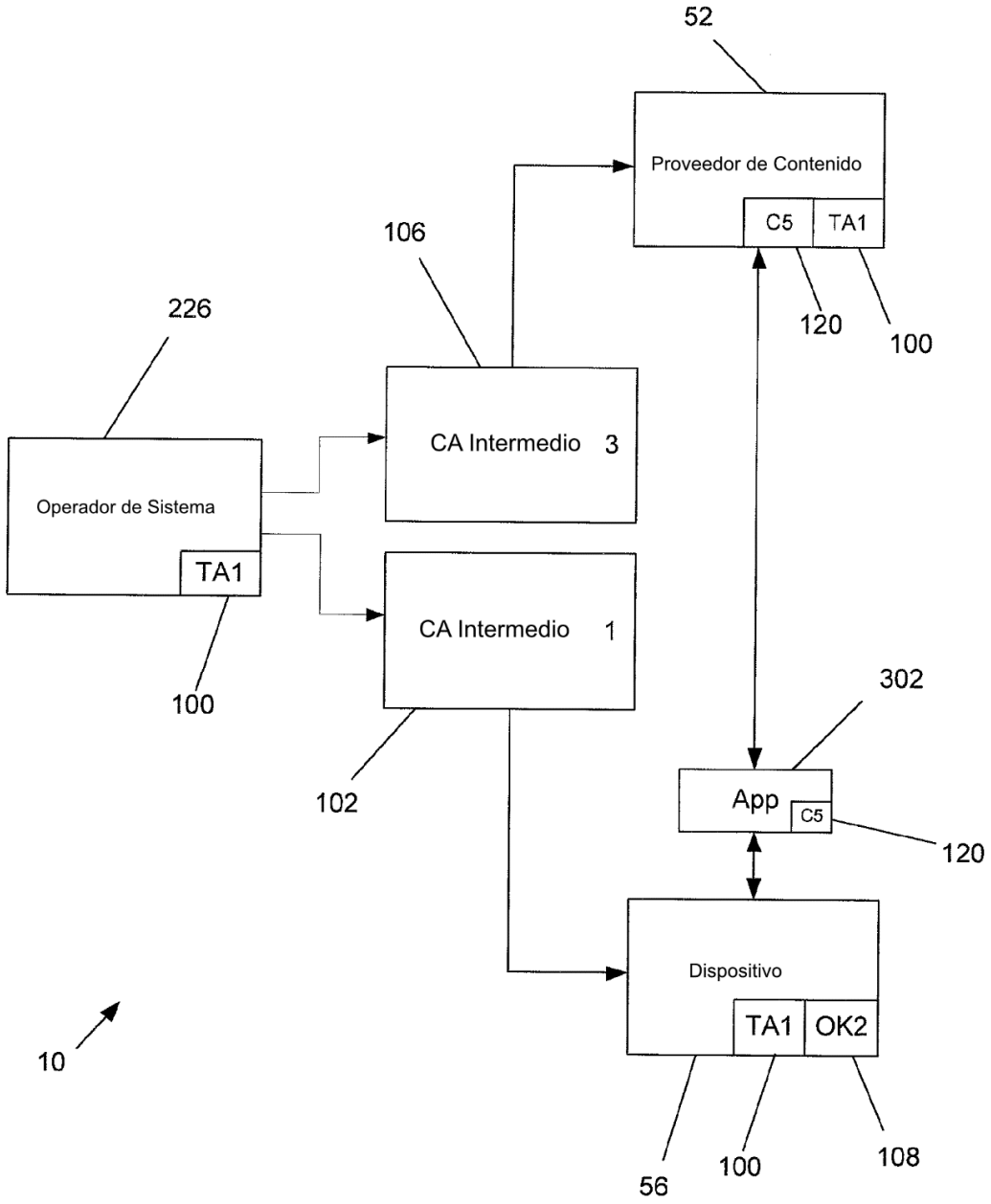

52
Proveedor de Contenido
C5
TA1
106
120
100
226
CA Intermedio 3
Operador de Sistema
TA1
CA Intermedio 1
100
102
302
App
C5
120
Dispositivo
TA1
OK2
10
56
100
108

Figura 2

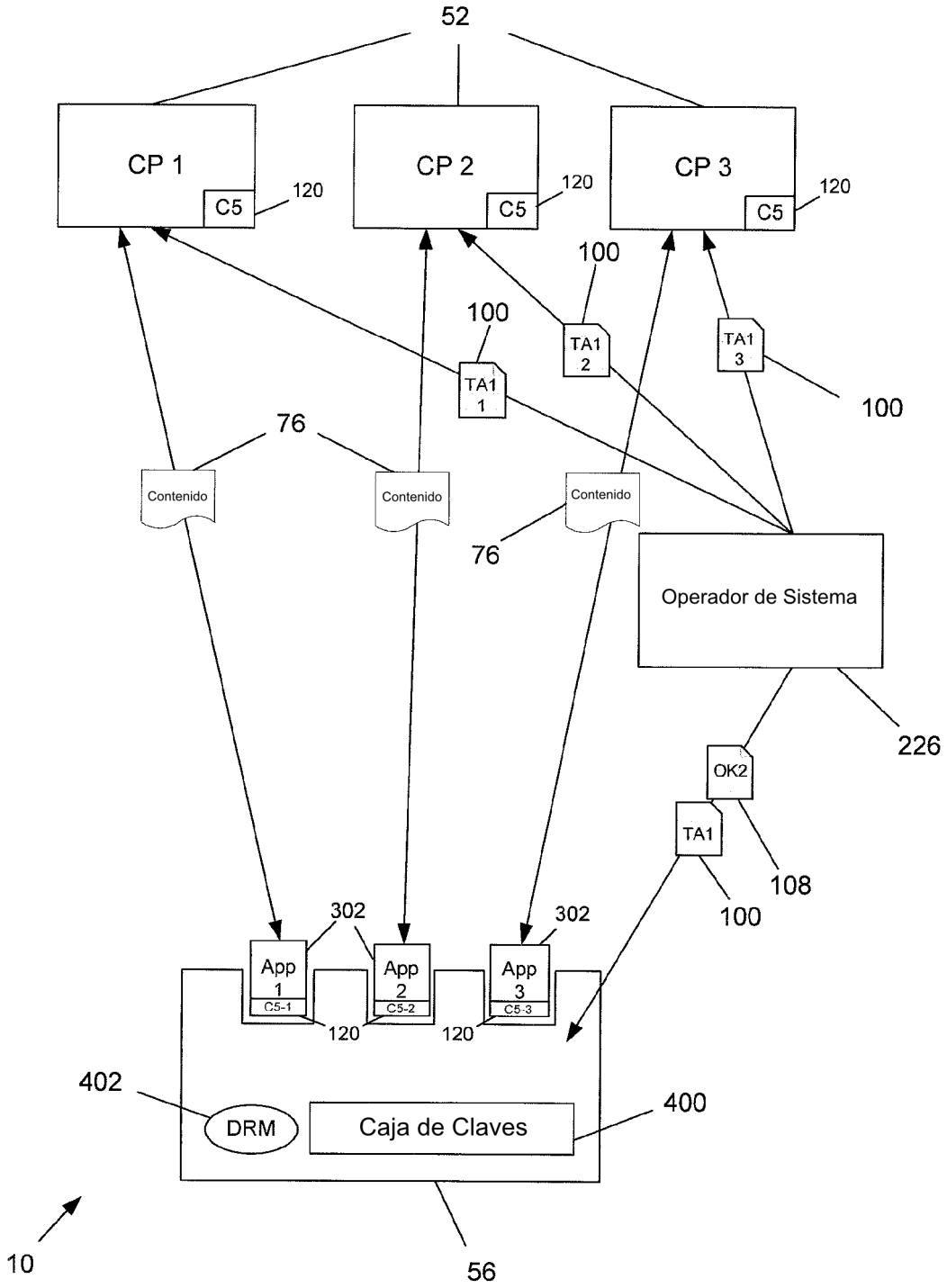

52
CP 1
C5
120
CP 2
C5
120
CP 3
C5
120
100
100
TA1
2
TA1
3
100
TA1
1
76
Contenido
Contenido
Contenido
76
Operador de Sistema
226
OK2
TA1
108
100
302
302
App
1
C5-1
App
2
C5-2
App
3
C5-3
120
120
402
DRM
Caja de Claves
400
10
56

Figura 3

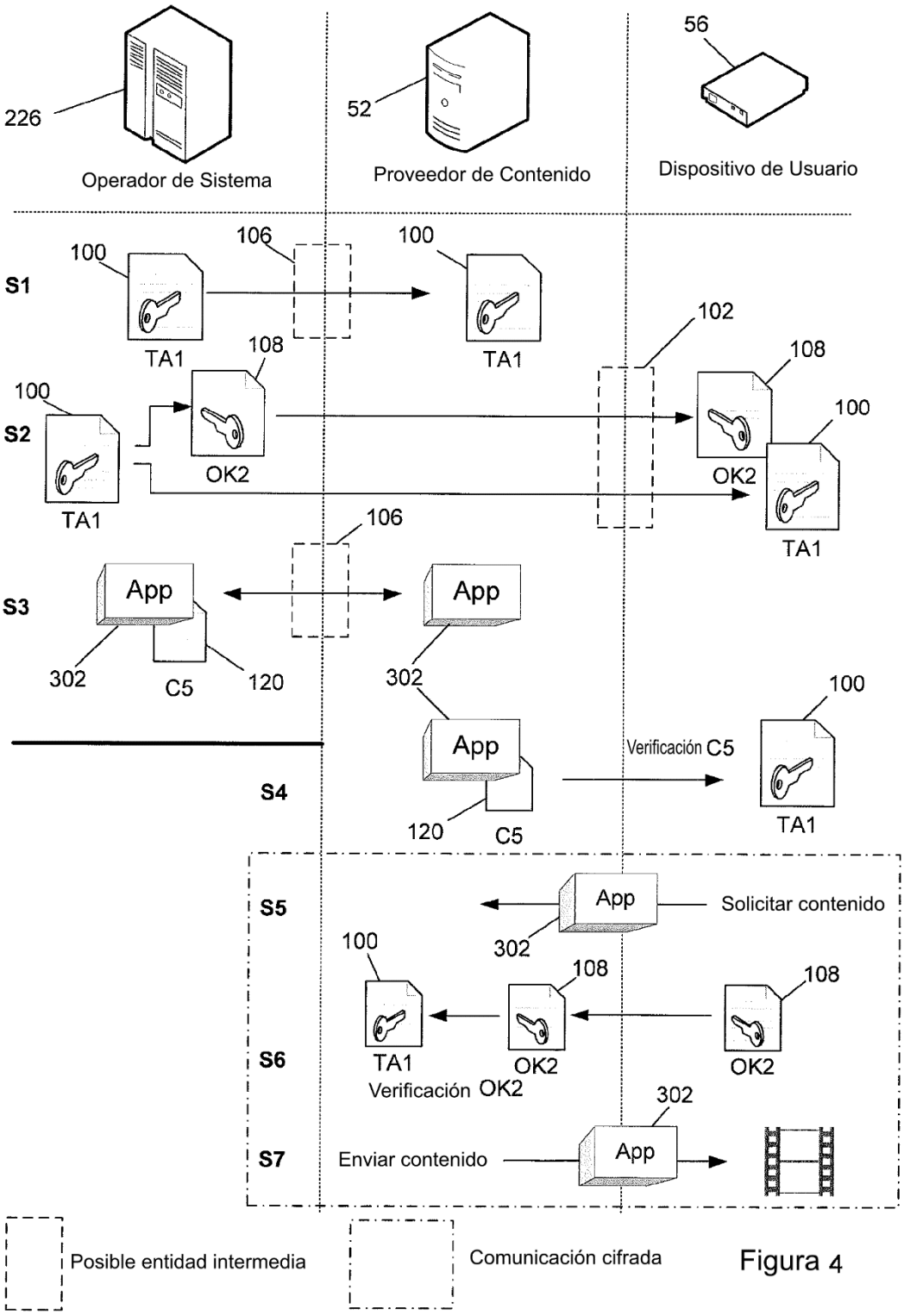

226
Operador de Sistema
52
Proveedor de Contenido
56
Dispositivo de Usuario
S1
100
106
100
TA1
TA1
102
108
S2
100
108
100
OK2
OK2
TA1
TA1
106
S3
App
App
302
C5
120
302
App
120
C5
Verificación C5
100
TA1
S4
S5
App
Solicitar contenido
302
100
108
108
S6
TA1
OK2
OK2
Verificación OK2
302
S7
Enviar contenido
App
Posible entidad intermedia
Comunicación cifrada

Figura 4

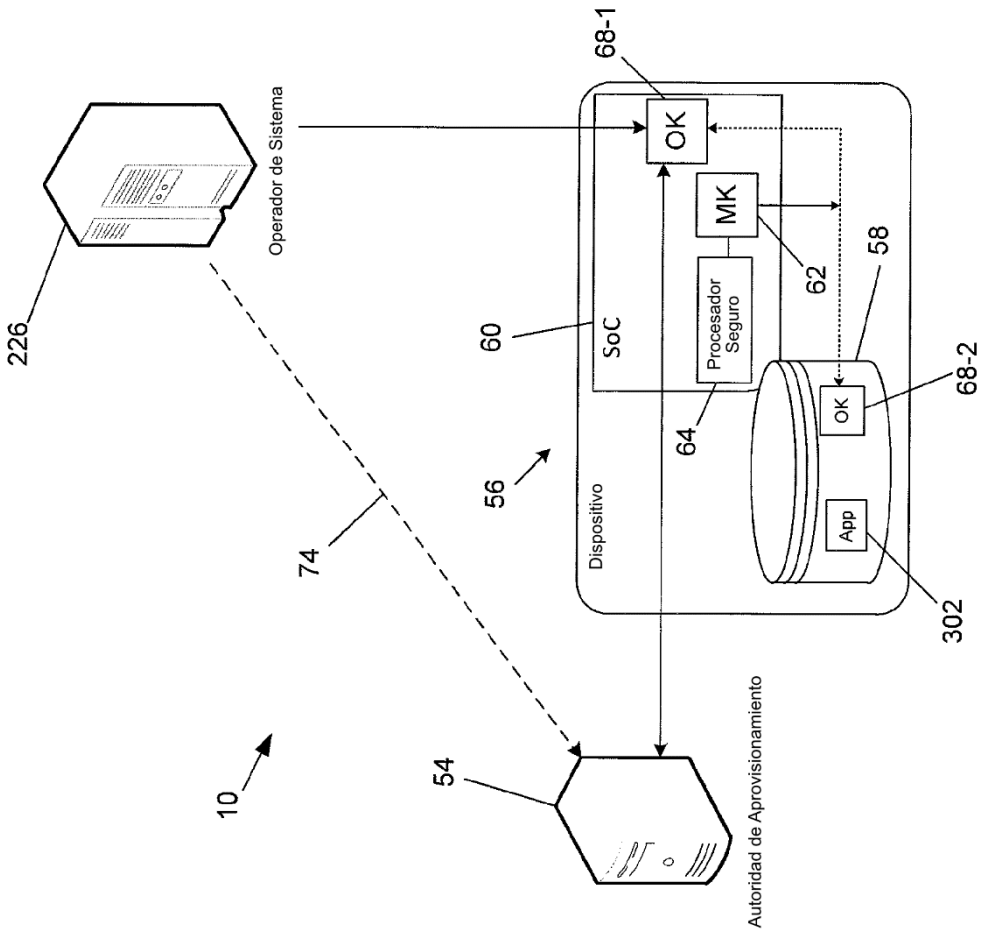

68-1
OK
MK
62
58
60
SoC
Procesador Seguro
64
68-2
OK
56
Dispositivo
App
302
74
226
Operador de Sistema
10
54
Autoridad de Aprovisionamiento

Figura 5

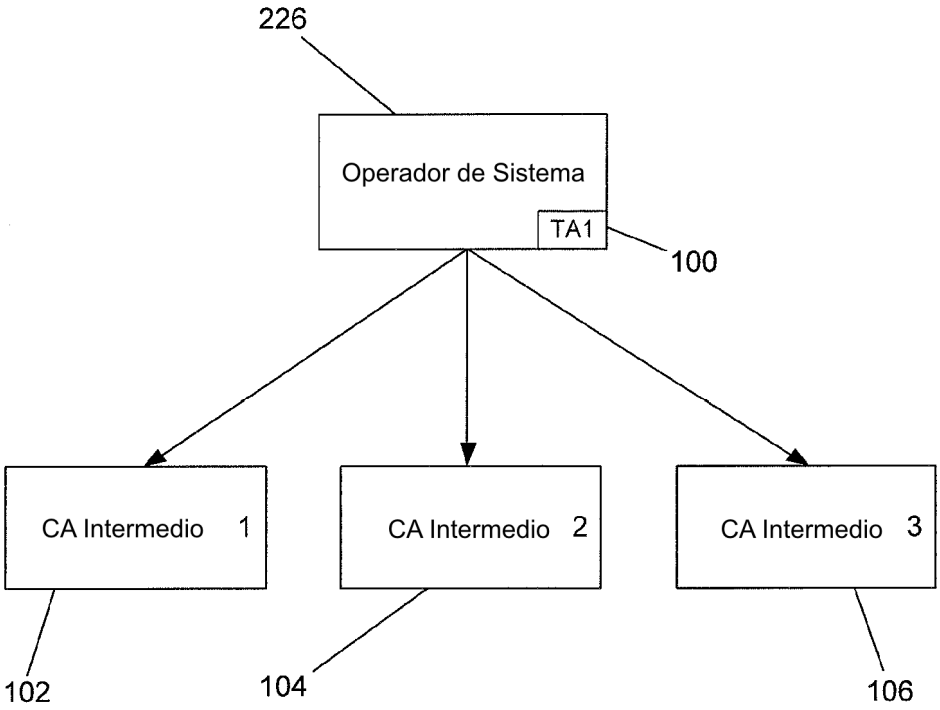

226
Operador de Sistema
TA1
100
CA Intermedio 1
CA Intermedio 2
CA Intermedio 3
102
104
106

Figura 6