(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 982 303**

(51) Int. Cl.:

G06F 21/10 (2013.01)

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.04.2018 PCT/EP2018/058628**

(87) Fecha y número de publicación internacional: **11.10.2018 WO18185174**

(96) Fecha de presentación y número de la solicitud europea: **04.04.2018 E 18713994 (4)**

(97) Fecha y número de publicación de la concesión europea: **28.02.2024 EP 3607751**

(54) Título: **Seguridad de medios de vigilancia**

(30) Prioridad:

04.04.2017 EP 17164869

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.10.2024

(73) Titular/es:

NAGRAVISION SÀRL (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

ANGEL, MICHEL;
RETAUREAU, HERVÉ y
CELLETTI, ANTONY

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Seguridad de medios de vigilancia

Campo

La presente divulgación se refiere a la seguridad de los medios generados por el dispositivo de medios, tal como un dispositivo de vigilancia. En particular, pero no exclusivamente, se refiere a garantizar la confidencialidad de los medios generados por una cámara de vigilancia.

Antecedentes

Muchos sistemas de videovigilancia protegen contenido de medios de vigilancia generado durante el transporte entre elementos del sistema. Por ejemplo, cuando una cámara genera un flujo de medios para su visualización en un dispositivo remoto, la confidencialidad de los medios se aplica en el transporte del flujo de medios entre elementos del sistema, tal como entre la cámara, el dispositivo remoto y cualquier dispositivo intermedio a través del que se transporta el flujo de medios.

Como consecuencia, fuera de las fases de comunicación segura entre elementos del sistema, a menudo no hay aplicación de protección y el contenido de medios está realmente desprotegido, es vulnerable y puede divulgarse. El control de acceso con una gestión de políticas adecuada no siempre se implementa o se implementa débilmente en uno o más elementos del sistema, lo que significa que: se puede acceder a contenido de medios desprotegido sin autorización en elementos sin control de acceso o monitorización efectivos; el contenido de medios está desprotegido y es vulnerable cuando el control de acceso o la monitorización en cualquier elemento se piratea o se elude de otra manera.

Breve descripción de los dibujos

La Figura 1 es una ilustración esquemática de un sistema para implementar una realización preferida;
La Figura 2 es la ilustración esquemática de la Figura 1 con información adicional que representa etapas de procesamiento en cada entidad;
La Figura 3 es un diagrama de proceso que muestra el proceso de una realización preferida; y
La Figura 4 muestra una infraestructura de hardware para implementar una realización preferida.

El documento US 2015/0235011 A1 divulga la reproducción segura de contenido multimedia protegido en una consola de juegos usando una aplicación sin secreto. Se puede usar un modelo de SSO para la autenticación de cliente en un servidor de claves, lo que elimina la necesidad de almacenar o usar cualquier información secreta en la aplicación cliente. Además, una clave de contenido cifrada generada por un empaquetador de contenido que usa una clave pública puede implementarse en el URI de clave de un archivo de lista de reproducción, que se envía al servidor de claves.

El documento US 7.508.941 B1 divulga que se proporciona una señal de control a un sistema de adquisición de datos de vídeo que genera datos de vídeo. En respuesta a recibir la señal de control, el sistema de adquisición de datos de vídeo modifica al menos una porción de los datos de vídeo para producir una señal de salida. La autenticidad de la señal de salida del sistema de adquisición de datos de vídeo se verifica comprobando que los datos de vídeo incluyen modificaciones de acuerdo con la señal de control.

Sumario

Aunque la invención se define en las reivindicaciones independientes, se exponen aspectos adicionales de la invención en las reivindicaciones adjuntas, los dibujos y la siguiente descripción.

Descripción detallada de los dibujos

En resumen, un método de acuerdo con la divulgación comprende asegurar los medios generados por un dispositivo de medios con una clave de medios y proteger la clave de medios con una clave de dominio para formar un testigo de medios cifrado. Cuando una entidad de recepción desea acceder a los medios, un proveedor de servicios confiable puede autenticar la entidad de recepción y descifrar el testigo de medios cifrado para recuperar la clave de medios para su uso por la entidad de recepción para descifrar los medios. De esta manera, los medios pueden protegerse por el dispositivo de medios que los genera sin descifrarse posteriormente hasta que estén presentes en una entidad de recepción autorizada. No se requiere que las entidades intermedias tengan acceso a los medios descifrados. La divulgación proporciona además un medio legible por ordenador y un sistema configurado para llevar a cabo este método.

En algunos aspectos de la divulgación se proporciona un método para asegurar contenido de medios en una red que comprende las siguientes etapas: Un dispositivo de medios recibe una clave de dominio de un proveedor de servicios.

El dispositivo de medios cifra además los medios con una clave de medios y cifra la clave de medios con la clave de dominio para formar un testigo de medios cifrado: la clave de medios protegida se encapsula en un testigo de medios cifrado. El proveedor de servicios a continuación recibe el testigo de medios cifrado y uno o más identificadores de entidad de recepción relacionados con una entidad de recepción y determina si la entidad de recepción está autorizada a acceder a medios desde el dispositivo de medios. Si la entidad de recepción está autorizada a acceder a los medios desde el dispositivo de medios, el proveedor de servicios descifra el testigo de medios criptográficos usando la clave de dominio para obtener la clave de medios y proporcionar la clave de medios a la entidad de recepción. Como tal, una entidad de recepción autenticada puede obtener la clave de medios necesaria para descifrar los medios. Además, no existe ningún requisito para que ninguna entidad intermedia tenga un acceso similar y, por lo tanto, el cifrado proporcionado por la clave de medios está en su lugar a través de todo el transporte de los medios desde el dispositivo de medios a la entidad de recepción.

En algunas realizaciones, la clave de medios se genera en el dispositivo de medios. Como alternativa, la clave de medios puede recibirse por el dispositivo de medios desde una fuente externa, tal como el proveedor de servicios. Por ejemplo, la clave de medios puede generarse aleatoriamente.

Opcionalmente, la clave de dominio está asociada con un dominio que define uno o más dispositivos de medios dentro de la red. Por tanto, la clave de dominio puede ser común a más de un dispositivo de medios. Un dispositivo de medios dado puede añadirse o eliminarse de un dominio a lo largo del tiempo, permitiendo el control sobre el acceso a los medios desde ese dispositivo de medios a través del proceso de autenticación de una entidad de recepción. La entidad de recepción puede autenticarse antes de la etapa de determinar si la entidad de recepción está autorizada a acceder a medios desde dispositivos de medios dentro del dominio asociado con la clave de dominio.

El dispositivo de medios recibe la clave de dominio del proveedor de servicios en una forma cifrada usando uno o más identificadores de dispositivo de medios. De esta manera, el proveedor de servicios puede garantizar la seguridad de la transmisión de la clave de dominio al dispositivo de medios.

El testigo de medios cifrado puede comprender metadatos asociados con la clave de dominio. La clave de medios protegida se encapsula en ese caso en el testigo de medios cifrado con metadatos. Por ejemplo, estos metadatos pueden identificar el dominio con el que está asociada la clave de dominio o pueden permitir de alguna otra manera que se identifique la clave de dominio. Esto puede ayudar al proveedor de servicios a localizar la clave de dominio que va a usarse para descifrar el testigo de medios cifrado.

En algunas realizaciones, el dispositivo de medios transmite el testigo de medios cifrado a la entidad de recepción y el proveedor de servicios recibe el testigo de medios cifrado de la entidad de recepción. Por ejemplo, el testigo de medios cifrado puede transmitirse a la entidad de recepción junto con los propios medios. En otros ejemplos, el testigo de medios cifrado puede transmitirse a la entidad de recepción en una comunicación fuera de banda, por ejemplo, por separado a los medios. El testigo de medios cifrado puede transmitirse directamente desde el dispositivo de medios a la entidad de recepción o puede transmitirse a través de una o más entidades intermedias.

El proveedor de servicios puede recibir el testigo de medios cifrado en una forma cifrada usando uno o más identificadores de dispositivo de recepción. Como alternativa, o, adicionalmente, el proveedor de servicios puede proporcionar la clave de medios a la entidad de recepción en una forma cifrada usando uno o más identificadores de dispositivo de recepción. Este enfoque puede ayudar a asegurar la comunicación entre la entidad de recepción y el proveedor de servicios.

Una o ambas de la clave de medios y la clave de dominio pueden cambiarse periódicamente. De esta manera, se puede aumentar la seguridad. Cambiar la clave de medios o la clave de dominio puede provocar la regeneración del testigo de medios cifrado. Por ejemplo, la secuencia de medios puede comprender paquetes de datos y cada paquete de datos puede cifrarse usando la clave de medios antes de la transmisión desde el dispositivo de medios. Si se cambia la clave de medios, por ejemplo, después de un tiempo de duración predeterminado o después de un número predeterminado de paquetes, a continuación, los paquetes posteriores del mismo flujo de medios se cifran usando la clave de medios actualizada.

Los medios pueden comprender contenido de audio y/o visual. El contenido visual puede comprender vídeo o una o más imágenes fijas. Los medios pueden comprender además metadatos. Tales metadatos podrían incluir, por ejemplo, una indicación de alarma diseñada para alertar a un usuario. Los medios pueden ser medios de envío por flujo continuo. Los medios pueden generarse en tiempo real por el dispositivo de medios. El dispositivo de medios puede comprender una cámara. Por ejemplo, el dispositivo de medios puede ser una cámara de vigilancia tal como una cámara de vigilancia móvil. El dispositivo de medios puede ser un dron, robot o cámara llevable, por ejemplo. El dispositivo de medios puede ser, pero sin limitación, cualquier otro dispositivo que pueda procesar o generar medios.

En algunos aspectos de la divulgación, se proporciona un medio legible por ordenador que comprende instrucciones ejecutables por ordenador para llevar a cabo el método de los aspectos descritos anteriormente. Además, aspectos adicionales de la divulgación proporcionan un sistema configurado para llevar a cabo estos métodos.

En algunos aspectos de la divulgación se proporciona un sistema para asegurar contenido de medios en una red que comprende un dispositivo de medios y un proveedor de servicios. El dispositivo de medios está configurado para: recibir una clave de dominio del proveedor de servicios; y cifrar medios con una clave de medios y cifrar la clave de medios con la clave de dominio para formar un testigo de medios cifrado. El proveedor de servicios está configurado para recibir el testigo de medios cifrado y uno o más identificadores de entidad de recepción relacionados con una entidad de recepción; determinar si la entidad de recepción está autorizada a acceder a los medios desde el dispositivo de medios; y, si la entidad de recepción está autorizada a acceder a los medios desde el dispositivo de medios, descifrar el testigo de medios cifrado usando la clave de dominio para obtener la clave de medios y proporcionar la clave de medios a la entidad de recepción. Las características opcionales del método también pueden aplicarse al sistema. El sistema puede comprender además la entidad de recepción. La entidad de recepción puede configurarse para descifrar los medios usando la clave de medios recibida del proveedor de servicios.

Se describen ahora algunas realizaciones específicas a modo de ilustración con referencia a los dibujos adjuntos.

Con referencia a la Figura 1, se ilustra un sistema que comprende un dispositivo de cámara 11, uno o más dispositivos intermedios 20 y una entidad de recepción 30. El dispositivo de cámara es un dispositivo de medios que puede generar medios a recibir por la entidad de recepción 30. Los medios generados por la cámara 11 pueden transmitirse a la entidad de recepción 30 a través de la una o más entidades intermedias 20.

El dispositivo de cámara 11 puede ser parte de cualquier sistema de vigilancia fijo o móvil, tal como un dron, robot o dispositivo llevable. En general, puede ser cualquier dispositivo que pueda procesar o generar contenido de medios. Las entidades intermedias 20 pueden ser cualquier elemento de red que pueda pasar tráfico de red, mientras que la entidad de recepción 30 podría ser cualquier dispositivo adecuado para la reproducción o procesamiento de medios. La entidad de recepción 30 puede ubicarse en una sala de control de vigilancia o en cualquier otra ubicación deseada, y puede ser fija o portátil. Por ejemplo, la entidad de recepción 30 puede ser un dispositivo de usuario final habilitado para red, tal como un ordenador portátil, un ordenador personal, ordenador de tipo tableta, teléfono inteligente o similar.

También se muestra como parte del sistema de la Figura 1 un servicio de aprovisionamiento de licencias 40. Este actúa como un proveedor de servicios y puede comunicarse con un gestor de políticas 50. También se muestra un servicio de aprovisionamiento de secretos 60, que puede proporcionarse opcionalmente para comunicarse con el dispositivo de cámara 11 y la entidad de recepción 30.

El servicio de aprovisionamiento de licencias 40, el gestor de políticas 50 y el servicio de aprovisionamiento de secretos 60 pueden actuar conjuntamente como un proveedor de servicios. Cada uno de ellos puede implementarse como un servicio basado en la nube o puede implementarse en dispositivos físicos definidos, tal como un servidor.

En general, cada uno de los elementos ilustrados en la Figura 1 puede implementarse en uno o más dispositivos informáticos, cuyos detalles adicionales se exponen a continuación con referencia a la Figura 4.

La operación del sistema de la Figura 1 puede entenderse con referencia a las Figuras 2 y 3. La Figura 2 muestra el sistema de la Figura 1 con números de referencia adicionales que identifican la comunicación dentro o entre elementos del sistema asociados con las etapas de proceso descritas a continuación. Esta numeración en la Figura 2 está asociada con los números de párrafo "1" a "10" a continuación. La Figura 3 es un diagrama de proceso que proporciona una exposición adicional de ciertas etapas de proceso e ilustra estas en un posible orden secuencial.

1 - En la etapa s31, la cámara 11 está configurada con secretos únicos de dispositivo. Hay uno o más identificadores asociados con la cámara 11. Esos secretos pueden estar basados en software o hardware. Pueden aprovisionarse previamente en el momento de la fabricación o a través de la comunicación como se muestra en la Figura 2, la opción 1d del servicio de aprovisionamiento de secreto 60.

2 - La cámara está asociada con un dominio. Este dominio puede conectar o asociar la cámara con el área que cubre. En la etapa s32, el servicio de aprovisionamiento de licencias 40 puede generar una clave de dominio para el dominio. En la etapa s34, que puede ocurrir durante la instalación de la cámara 11, la clave de dominio única se suministra en el transcurso de la comunicación desde el servicio de aprovisionamiento de licencias 40. Esta clave de dominio se protege de forma segura cuando se transmite a la cámara 11 usando secretos únicos de dispositivo disponibles. Cuando la cámara se instala en un área nueva o el área existente se divide en un nuevo dominio, se suministra una nueva clave de dominio única a la cámara.

3 - La cámara 11 puede generar una clave de medios en la etapa s35 usada para cifrar medios generados por la cámara en la etapa s36. En la etapa s37, esta clave de medios se protege usando la clave de dominio única y se genera un testigo de medios cifrado. El testigo de medios cifrado comprende la clave de medios protegida y metadatos adicionales. Cualquier información relevante puede registrarse en los metadatos, tal como información que identifica el dominio asociado con la cámara 11. Dado que los medios están cifrados dentro de la cámara 11, están protegidos cuando salen de la cámara 11 para transmitirse a cualquier otro sitio. Por ejemplo, en la etapa s38, los medios cifrados por la clave de medios se transmiten a la entidad de recepción 30. Como puede observarse en la Figura 2, esta transmisión puede tener lugar a través de una o más entidades intermedias 20. En la etapa

s29, el testigo de medios cifrado también se transmite a la entidad de recepción 30. Dependiendo del formato de envío por flujo continuo, el testigo de medios cifrado puede transmitirse embebido en el contenido de medios de cámara protegido o con un canal fuera de banda.

4 - La entidad de recepción 30 puede configurarse con secretos únicos de entidad en la etapa s33. Estos actúan como uno o más identificadores asociados con la entidad de recepción. Los secretos pueden estar basados en software o hardware. Pueden aprovisionarse previamente en el momento de la fabricación o a través de la comunicación como se ilustra en la Figura 1, la opción 4d del servicio de aprovisionamiento de secreto 60.

5 - Después de la etapa s39 descrita anteriormente, la entidad de recepción ha recibido el testigo de medios cifrado de la cámara 11. Si es necesario, puede extraer este testigo del flujo de medios. En algunas alternativas, lo obtendrá de un canal fuera de banda. La entidad de recepción 30 a continuación proporciona el testigo de medios cifrado al servicio de aprovisionamiento de licencias 40 en la etapa s40. Esto se proporciona en forma de un desafío criptográfico asegurado con secretos únicos de entidad. Este desafío criptográfico se usa para autenticar la entidad de recepción 30.

6 - El servicio de aprovisionamiento de licencias 40 verifica el desafío criptográfico que autenticó la entidad de recepción 30 en la etapa anterior 5, y extrae el testigo de medios cifrado. El servicio de aprovisionamiento de licencias 40 identifica el dominio a partir de los metadatos encapsulados en el testigo de medios cifrado. A continuación, puede confirmar si la entidad de recepción está autorizada a acceder a los medios desde la cámara 11. Si la entidad de recepción 30 está autorizada a acceder a este dominio por el gestor de políticas 50, el servicio de aprovisionamiento de licencias 40 extrae la clave de medios del testigo de medios cifrado usando la clave de dominio en la etapa s41. El servicio de aprovisionamiento de licencias 40 genera a continuación un testigo de entidad cifrado que encapsula la clave de medios con reglas de uso relevantes. El testigo de entidad cifrado se protege usando los secretos únicos de entidad conocidos por la entidad de recepción 30, en lugar de la clave de dominio no conocida por la entidad de recepción 30, y que se proporciona de vuelta a la entidad de recepción 30 en la etapa s42.

7 - La entidad de recepción 30 verifica a continuación el testigo de entidad cifrado recibido del servicio de aprovisionamiento de licencias 40. La entidad de recepción 30 puede extraer a continuación la clave de medios y, por lo tanto, puede descifrar el contenido de medios de cámara protegido de acuerdo con las reglas de uso relacionadas en la etapa s43. El contenido de medios de cámara no protegido resultante puede accederse y/o procesarse por la entidad de recepción.

8 - Como opción y para mejorar la protección del contenido multimedia de la cámara, la clave de medios se puede cambiar periódicamente. Por ejemplo, la secuencia de medios puede comprender paquetes de datos y cada paquete de datos se cifra usando la clave de medios antes de la transmisión desde la cámara 11. Si se cambia la clave de medios, por ejemplo, después de un tiempo de duración predeterminado o después de un número predeterminado de paquetes, a continuación, los paquetes posteriores del mismo flujo de medios se cifran usando la clave de medios actualizada. En ese caso, el testigo de medios cifrado debe regenerarse para cada cambio de clave de medios y transmitirse de nuevo a la entidad de recepción 30. Este enfoque puede ayudar a asegurar la comunicación entre una entidad de recepción y el proveedor de servicios, incluso si la entidad de recepción está autorizada inicialmente para descifrar un flujo de medios, requiriendo la reautenticación de la entidad de recepción usando el testigo de medios cifrado regenerado.

9 - De manera similar y por la misma razón, la clave de dominio se puede cambiar periódicamente. En ese caso, debe generarse una nueva clave de medios y un nuevo testigo de medios cifrado para cada cambio de clave de dominio y transmitirse de nuevo a la entidad de recepción 30.

10 - Como el esquema de protección de contenido de medios de cámara propuesto conserva las propiedades del formato de contenido, cualquier entidad intermedia que no esté autorizada a acceder al contenido de medios de cámara no protegido aún puede grabar el contenido de medios de cámara protegido sin problema de privacidad. Este contenido de medios de cámara grabado puede duplicarse en cualquier lugar sin problema de privacidad; Permanece protegido y acceder a él requiere autenticar la entidad que necesita acceder o procesar el contenido de medios de cámara y verificaciones por el servicio de aprovisionamiento de licencias 40 como se describe en 5, 6 y 7.

El proceso puede proteger de manera única contenido de la cámara 11 u otro dispositivo de medios y proporciona protección de los medios independientemente del número de dispositivos tales como dispositivos intermedios 20 implicados en una cadena de procesamiento.

La Figura 4 ilustra un diagrama de bloques de una implementación de un dispositivo informático 300 dentro del que puede ejecutarse un conjunto de instrucciones, para hacer que el dispositivo informático realice una cualquiera o más de las metodologías analizadas en el presente documento. El dispositivo informático 300 puede usarse para elementos del sistema mostrado en las Figuras 1 y 2. En implementaciones alternativas, el dispositivo informático puede estar conectado (por ejemplo, en red) a otras máquinas en una red de área local (LAN), una intranet, una extranet o Internet.

El dispositivo informático puede operar en la capacidad de un servidor o una máquina cliente en un entorno de red cliente-servidor, o como una máquina de pares en un entorno de red entre pares (o distribuido). El dispositivo informático puede ser un ordenador personal (PC), un ordenador de tableta, un decodificador de salón (STB), un asistente personal digital (PDA), un teléfono celular, un dispositivo web, un servidor, un enrutador de red, conmutador o puente, o cualquier máquina que pueda ejecutar un conjunto de instrucciones (secuenciales o de otro tipo) que especifican acciones a realizar por esa máquina. Además, mientras que únicamente se ilustra un único dispositivo informático, la expresión "dispositivo informático" también se considerará que incluye cualquier colección de máquinas (por ejemplo, ordenadores) que ejecutan individual o conjuntamente un conjunto (o múltiples conjuntos) de instrucciones para realizar una cualquiera o más de las metodologías analizadas en el presente documento.

El dispositivo informático 300 de ejemplo incluye un dispositivo de procesamiento 302, una memoria principal 304 (por ejemplo, memoria de solo lectura (ROM), memoria flash, memoria de acceso aleatorio dinámica (DRAM) tal como DRAM síncrona (SDRAM) o DRAM Rambus (RDRAM), etc.), una memoria estática 306 (por ejemplo, memoria flash, una estática de acceso aleatorio memoria (SRAM), etc.), y una memoria secundaria (por ejemplo, un dispositivo de almacenamiento de datos 318), que se comunican entre sí a través de un bus 330.

El dispositivo de procesamiento 302 representa uno o más procesadores de propósito general, tales como un microprocesador, unidad central de procesamiento, o similares. Más particularmente, el dispositivo de procesamiento 302 puede ser un microprocesador de cálculo de conjunto de instrucciones complejo (CISC), microprocesadores de cálculo de conjunto de instrucciones reducido (RISC), microprocesador de palabra de instrucción muy larga (VLIW), procesador que implementa otros conjuntos de instrucciones, o procesadores que implementan una combinación de conjuntos de instrucciones. El dispositivo de procesamiento 302 también puede ser uno o más dispositivos de procesamiento de propósito especial, tales como un circuito integrado específico de la aplicación (ASIC), una matriz de puertas programables en campo (FPGA), un procesador de señales digitales (DSP), procesador de red o similar. El dispositivo de procesamiento 302 está configurado para ejecutar la lógica de procesamiento (instrucciones 322) para realizar las operaciones y etapas analizadas en el presente documento.

El dispositivo informático 300 puede incluir además un dispositivo de interfaz de red 308. El dispositivo informático 300 también puede incluir una unidad de visualización de vídeo 310 (por ejemplo, una pantalla de cristal líquido (LCD) o un tubo de rayos catódicos (CRT)), un dispositivo de entrada alfanumérica 312 (por ejemplo, un teclado o pantalla táctil), un dispositivo de control de cursor 314 (por ejemplo, un ratón o pantalla táctil) y un dispositivo de audio 316 (por ejemplo, un altavoz).

El dispositivo de almacenamiento de datos 318 puede incluir uno o más medios de almacenamiento legibles por máquina (o más específicamente uno o más medios de almacenamiento legibles por ordenador no transitorios) 328 en los que se almacenan uno o más conjuntos de instrucciones 322 que incorporan una cualquiera o más de las metodologías o funciones descritas en el presente documento. Las instrucciones 322 también pueden residir, total o al menos parcialmente, dentro de la memoria principal 304 y/o dentro del dispositivo de procesamiento 302 durante su ejecución por el dispositivo informático 300, constituyendo también la memoria principal 304 y el dispositivo de procesamiento 302 medios de almacenamiento legibles por ordenador.

Los diversos métodos descritos anteriormente pueden implementarse mediante un programa informático. El programa informático puede incluir código informático dispuesto para dar instrucciones a un ordenador para realizar las funciones de uno o más de los diversos métodos descritos anteriormente. El programa informático y/o el código para realizar tales métodos pueden proporcionarse a un aparato, tal como un ordenador, en uno o más medios legibles por ordenador o, más en general, un producto de programa informático. Los medios legibles por ordenador pueden ser transitorios o no transitorios. El uno o más medios legibles por ordenador podrían ser, por ejemplo, un sistema electrónico, magnético, óptico, electromagnético, infrarrojo, o semiconductor, o un medio de propagación para la transmisión de datos, por ejemplo, para descargar el código a través de Internet. Como alternativa, el uno o más medios legibles por ordenador podrían tomar la forma de uno o más medios legibles por ordenador físicos, tales como memoria de semiconductores o de estado sólido, cinta magnética, un disquete informático extraíble, una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), un disco magnético rígido y un disco óptico, tal como un CD-ROM, CD-R/W o DVD.

En una implementación, los módulos, componentes y otras características descritas en el presente documento (por ejemplo, la unidad de control 310 en relación con la Figura 4) pueden implementarse como componentes discretos o integrarse en la funcionalidad de componentes de hardware tales como ASICS, FPGA, DSP o dispositivos similares como parte de un servidor de individualización.

Un "componente de hardware" es un componente físico tangible (por ejemplo, no transitorio) (por ejemplo, un conjunto de uno o más procesadores) que puede de realizar ciertas operaciones y puede configurarse o disponerse de una cierta manera física. Un componente de hardware puede incluir circuitería o lógica especializados que están configurados permanentemente para realizar ciertas operaciones. Un componente de hardware puede ser o incluir un procesador de propósito especial, tal como una matriz de puertas programables en campo (FPGA) o un ASIC. Un componente de hardware también puede incluir circuitería o lógica programable que están configurados temporalmente por software para realizar ciertas operaciones.

En consecuencia, la expresión "componente de hardware" debe entenderse que abarca una entidad tangible que puede estar construida físicamente, configurada permanentemente (por ejemplo, cableada de manera permanente), o configurada temporalmente (por ejemplo, programada) para operar de cierta manera o para realizar ciertas operaciones descritas en el presente documento.

Además, los módulos y componentes pueden implementarse como firmware o circuitería funcional dentro de dispositivos de hardware. Además, los módulos y componentes pueden implementarse en cualquier combinación de dispositivos de hardware y componentes de software, o únicamente en software (por ejemplo, código almacenado o incorporado de otra manera en un medio legible por máquina o en un medio de transmisión).

A menos que se indique específicamente lo contrario, como es evidente a partir del siguiente análisis, se aprecia que, a través de toda la descripción, los análisis que utilizan términos tales como "recibir", "determinar", "comparar", "habilitar", "mantener", "identificar", "remplazar", o similares, se refieren a las acciones y procesos de un sistema informático o dispositivo informático electrónico similar, que manipula y transforma datos representados como cantidades físicas (electrónicas) dentro de los registros y memorias del sistema informático en otros datos representados de manera similar como cantidades físicas dentro de las memorias o registros de sistema informático u otros dispositivos de almacenamiento de información, transmisión o visualización de este tipo.

Debe entenderse que la descripción anterior pretende ser ilustrativa y no restrictiva. Muchas otras implementaciones resultarán evidentes para los expertos en la materia tras leer y comprender la descripción anterior. Aunque la presente divulgación se ha descrito con referencia a implementaciones de ejemplo específicas, se reconocerá que la divulgación no se limita a las implementaciones descritas, sino que puede ponerse en práctica con modificaciones y modificaciones dentro del alcance de las reivindicaciones adjuntas. En consecuencia, la memoria descriptiva y los dibujos han de considerarse en un sentido ilustrativo en lugar de restrictivo. El alcance de la invención debería, por lo tanto, determinarse con referencia a las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para asegurar contenido de medios en una red, comprendiendo el método, en un dispositivo de medios:

recibir una clave de dominio de un proveedor de servicios; y
cifrar medios generados por el dispositivo de medios con una clave de medios y cifrar la clave de medios con la clave de dominio para formar un testigo de medios cifrado;
comprendiendo el método, además, en el proveedor de servicios:

recibir el testigo de medios cifrado y uno o más identificadores de entidad de recepción relacionados con una entidad de recepción;
determinar si la entidad de recepción está autorizada a acceder a los medios desde el dispositivo de medios; y si la entidad de recepción está autorizada a acceder a los medios desde el dispositivo de medios, descifrar el testigo de medios cifrado usando la clave de dominio para obtener la clave de medios y proporcionar la clave de medios a la entidad de recepción; en donde uno o más identificadores de dispositivo de medios están asociados con el dispositivo de medios, y el dispositivo de medios recibe la clave de dominio en una forma cifrada usando uno o más identificadores de dispositivo de medios.

2. Un método de acuerdo con la reivindicación 1, que comprende además generar la clave de medios en el dispositivo de medios.

3. Un método de acuerdo con la reivindicación 1 o la reivindicación 2, en donde la clave de dominio está asociada con un dominio que define uno o más dispositivos de medios dentro de la red.

4. Un método de acuerdo con la reivindicación 3, en donde la etapa de autenticar la entidad de recepción comprende establecer que la entidad de recepción está autorizada a acceder a medios desde dispositivos de medios dentro del dominio asociado con la clave de dominio.

5. Un método de acuerdo con cualquier reivindicación anterior, en donde el testigo de medios cifrado comprende metadatos asociados con la clave de dominio.

6. Un método de acuerdo con cualquier reivindicación anterior, en donde el dispositivo de medios transmite el testigo de medios cifrado a la entidad de recepción y en donde el proveedor de servicios recibe el testigo de medios cifrado de la entidad de recepción.

7. Un método de acuerdo con cualquier reivindicación anterior, en donde el proveedor de servicios recibe el testigo de medios cifrado en una forma cifrada usando uno o más identificadores de dispositivo de recepción.

8. Un método de acuerdo con cualquier reivindicación anterior, en donde el proveedor de servicios proporciona la clave de medios a la entidad de recepción en una forma cifrada usando uno o más identificadores de dispositivo de recepción.

9. Un método de acuerdo con cualquier reivindicación anterior, en donde la clave de medios se cambia periódicamente.

10. Un método de acuerdo con cualquier reivindicación anterior, en donde la clave de dominio se cambia periódicamente.

11. Un método de acuerdo con cualquier reivindicación anterior, en donde los medios comprenden contenido de audio y/o visual.

12. Un método de acuerdo con cualquier reivindicación anterior, en donde el dispositivo de medios comprende una cámara.

13. Un medio legible por ordenador que comprende instrucciones ejecutables por ordenador que, cuando se ejecutan por un ordenador, hacen que el ordenador lleve a cabo el método de una cualquiera de las reivindicaciones anteriores.

14. Un sistema para asegurar contenido de medios en una red que comprende un dispositivo de medios y un proveedor de servicios, en donde:

el dispositivo de medios está configurado para:

recibir una clave de dominio del proveedor de servicios; y
cifrar medios generados por el dispositivo de medios con una clave de medios y cifrar la clave de medios con la clave de dominio para formar un testigo de medios cifrado;

y en donde el proveedor de servicios está configurado para:

recibir el testigo de medios cifrado y uno o más identificadores de entidad de recepción relacionados con una entidad de recepción;

determinar si la entidad de recepción está autorizada a acceder a los medios desde el dispositivo de medios; y si la entidad de recepción está autorizada a acceder a los medios desde el dispositivo de medios, descifrar el testigo de medios cifrado usando la clave de dominio para obtener la clave de medios y proporcionar la clave de medios a la entidad de recepción; en donde uno o más identificadores de dispositivo de medios están asociados con el dispositivo de medios, y el dispositivo de medios recibe la clave de dominio en una forma cifrada usando uno o más identificadores de dispositivo de medios.

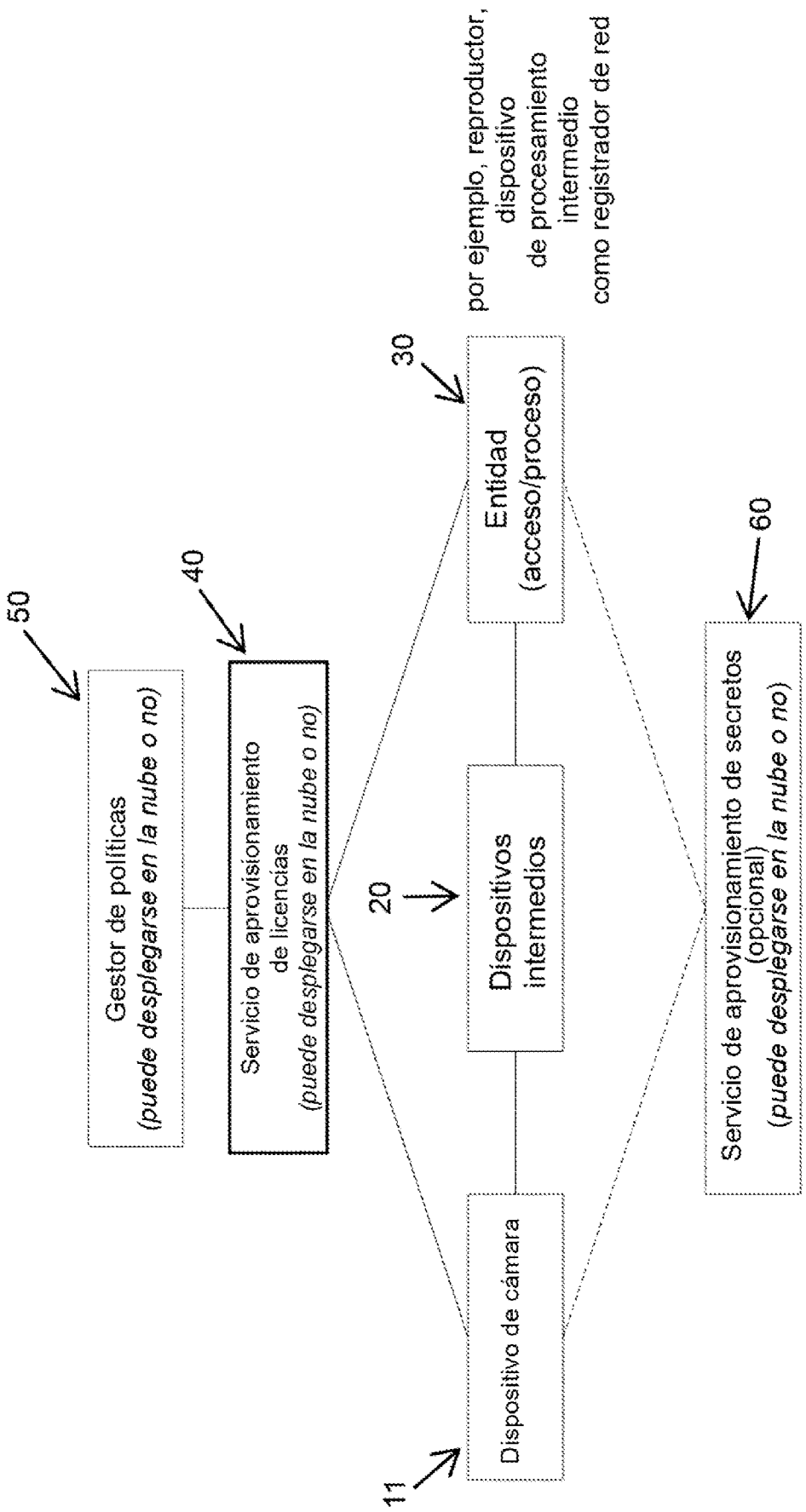
50
Gestor de políticas
(puede desplegarse en la nube o no)
40
Servicio de aprovisionamiento
de licencias
(puede desplegarse en la nube o no)
20
30
Entidad
(acceso/proceso)
por ejemplo, reproductor,
dispositivo
de procesamiento
intermedio
como registrador de red
Dispositivos
intermedios
60
Servicio de aprovisionamiento de secretos
(opcional)
(puede desplegarse en la nube o no)
11
Dispositivo de cámara

Fig. 1

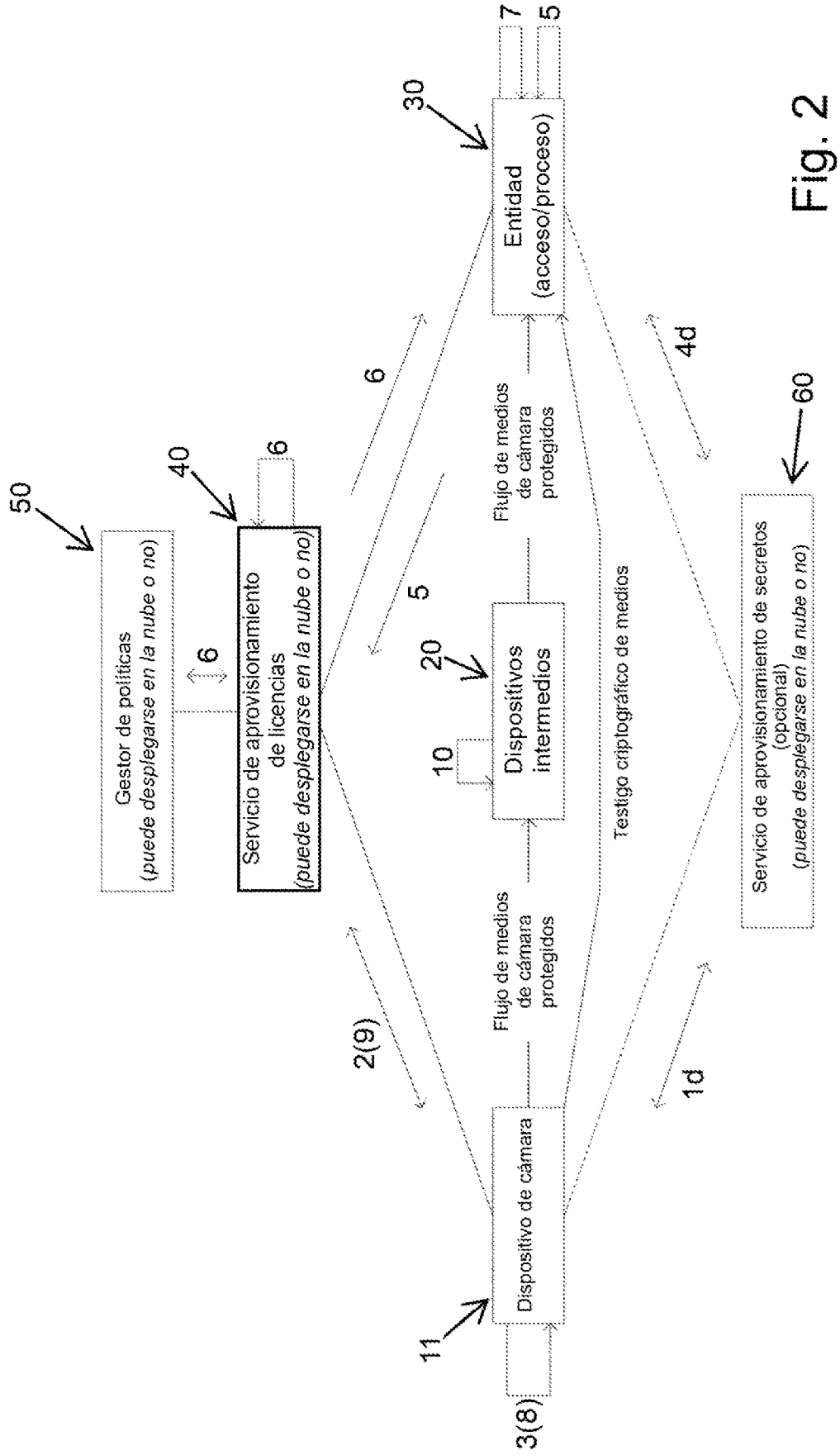
50
Gestor de políticas
(puede desplegarse en la nube o no)
6
40
Servicio de aprovisionamiento
de licencias
(puede desplegarse en la nube o no)
6
6
30
Entidad
(acceso/proceso)
7
5
4d
60
Servicio de aprovisionamiento de secretos
(opcional)
(puede desplegarse en la nube o no)
Flujo de medios
de cámara
protegidos
5
20
Dispositivos
intermedios
10
Flujo de medios
de cámara
protegidos
Testigo criptográfico de medios
2(9)
1d
11
Dispositivo de cámara
3(8)

Fig. 2

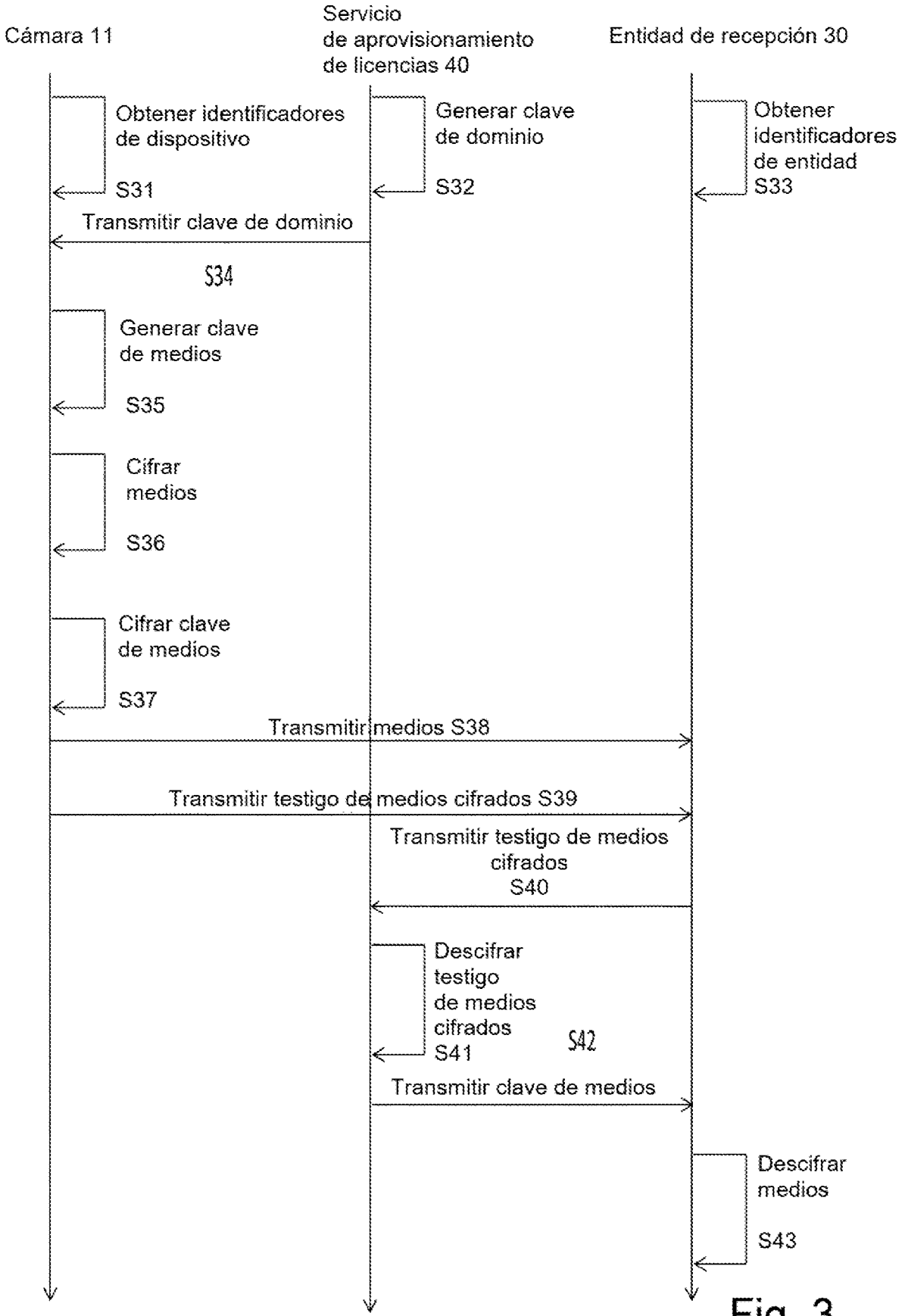
Cámara 11
Servicio de aprovisionamiento de licencias 40
Entidad de recepción 30
Obtener identificadores de dispositivo
S31
Generar clave de dominio
S32
Obtener identificadores de entidad
S33
Transmitir clave de dominio
S34
Generar clave de medios
S35
Cifrar medios
S36
Cifrar clave de medios
S37
Transmitir medios S38
Transmitir testigo de medios cifrados S39
Transmitir testigo de medios cifrados
S40
Descifrar testigo de medios cifrados
S41
S42
Transmitir clave de medios
Descifrar medios
S43

Fig. 3

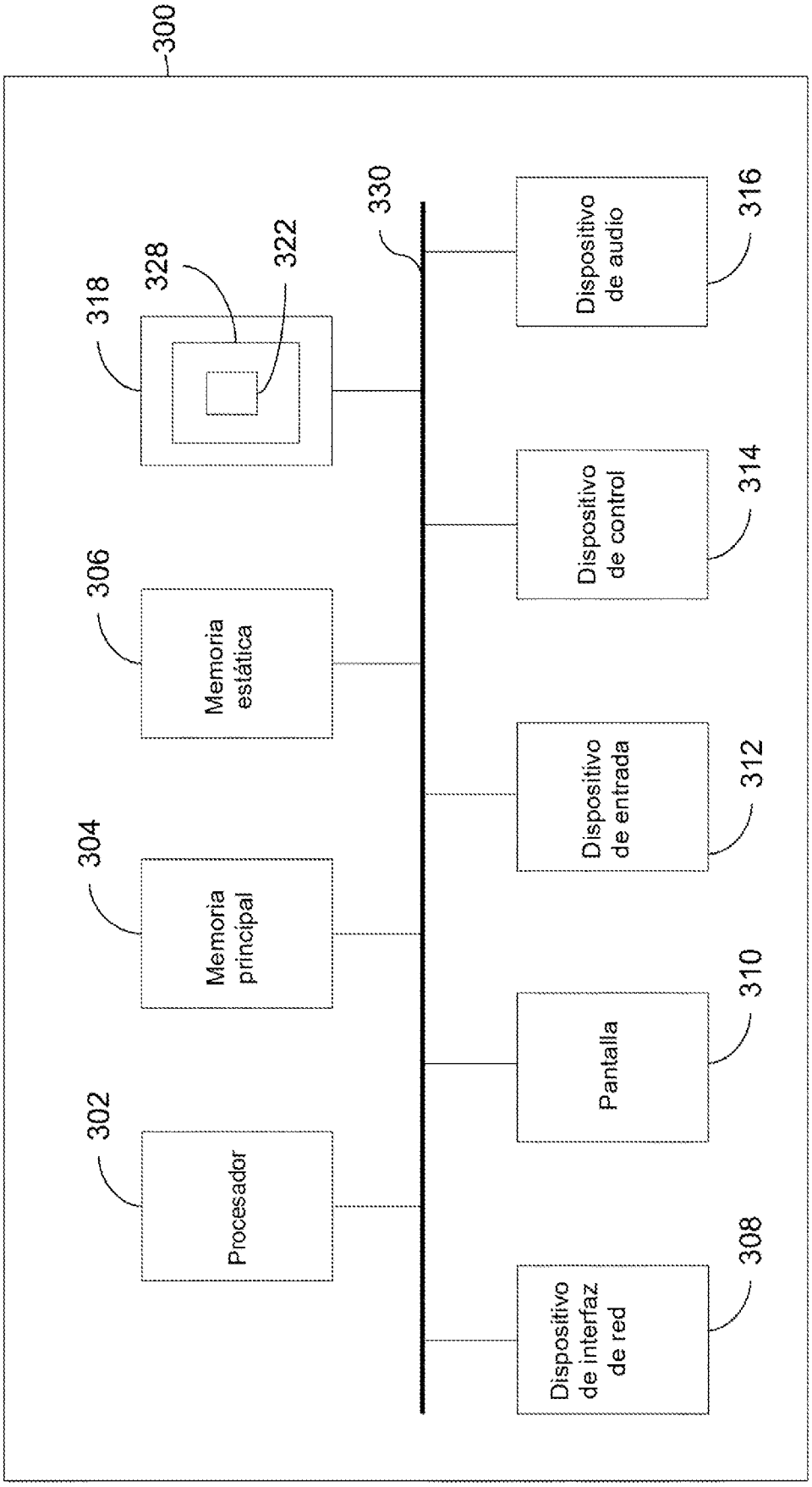
300
330
318
328
322
306
Memoria estática
304
Memoria principal
302
Procesador
Dispositivo de audio
316
Dispositivo de control
314
Dispositivo de entrada
312
Pantalla
310
Dispositivo de interfaz de red
308

Fig. 4