(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 637**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.10.2015 PCT/IB2015/058204**

(87) Fecha y número de publicación internacional: **27.04.2017 WO17068399**

(96) Fecha de presentación y número de la solicitud europea: **23.10.2015 E 15798204 (2)**

(97) Fecha y número de publicación de la concesión europea: **04.12.2019 EP 3366019**

(54) Título: **Método y aparato para almacenamiento en caché y entrega de contenido seguro**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.07.2020

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

ZHU, ZHONGWEN y
POURZANDI, MAKAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y aparato para almacenamiento en caché y entrega de contenido seguro

Campo técnico

Se proporciona un método y un aparato para almacenamiento en caché y entrega de contenido seguro a un dispositivo de comunicación.

Antecedentes

En las redes de entrega de contenidos actuales, el Protocolo de Transferencia de Hipertexto (HTTP) se usa como mecanismo principal de entrega. Dado que el activo, o datos tales como un título o contenido, se entrega en un entorno no seguro, esto permite que el nodo de entrega verifique el activo. Entonces, el nodo de entrega puede decidir almacenar en caché el activo en base a la verificación del contenido. De esta forma, el nodo de entrega puede servir el mismo activo a diferentes abonados. Esto conduce a una reducción significativa en el viaje de ida y vuelta del cliente al servidor, lo que mejora la experiencia del usuario.

El Grupo de Dirección de Ingeniería de Internet (IESG)/Grupo de Trabajo de Ingeniería de Internet (IETF) ha lanzado recientemente HTTP 2, dentro del cual, la Seguridad de Capa de Transporte (TLS) es obligatoria para el tráfico HTTP. Esto significa que en el futuro, el contenido se entregará a través de una conexión segura de extremo a extremo. Los navegadores principales están siendo desarrollados para soportar el nuevo estándar.

A partir del documento EP 2 779 523 A1 se conoce un sistema de nuevo cifrado, que comprende un aparato de compartición de archivos y un aparato de nuevo cifrado que son comunicables con un aparato cliente. El aparato de compartición de archivos comprende medios para adquirir, tras la recepción de una solicitud de archivo que incluye un ID de miembro para identificar al miembro y un nombre de archivo de un archivo cifrado desde el aparato de cliente, el primer archivo cifrado de un medio de almacenamiento de archivos en base al nombre de archivo incluido en la solicitud de archivo.

A partir del documento US 2012/0317655 A1 se conoce un sistema de interconexión de redes que comprende un servicio de aplicaciones que se ejecuta en una infraestructura en la nube y está configurado para recibir contenido cifrado dual de un proveedor de contenidos y volver a cifrar el contenido cifrado dual para habilitar el control dinámico de grupo de usuarios para autorización de usuarios basada en grupo. El servicio de almacenamiento en la nube está acoplado al servicio de aplicaciones para almacenar el contenido cifrado dual de un proveedor de contenidos y el contenido cifrado dual de nuevo cifrado del servicio de aplicaciones.

A partir del documento US 2009/0210697 A1 se conoce mejorar los sistemas de igual a igual de BitTorrent para habilitar la gestión de derechos digitales sin cambios de infraestructura.

Compendio

Según invención, un método de operación implementado por un dispositivo de comunicación de un abonado configurado para operación en una red de comunicación incluye enviar una solicitud de contenido a un sistema de CP alcanzable a través de la red de comunicación, la solicitud de contenido que identifica el contenido objetivo, tal como video, y que incluye una clave pública del dispositivo de comunicación. El método incluye recibir una respuesta del sistema de CP que identifica una CDN e incluye un testigo de autorización y una clave de contenido que se deriva de la clave pública del dispositivo de comunicación y una clave privada del sistema de CP. El método también incluye enviar el testigo de autorización a la CDN y recibir, correspondientemente, un testigo de entrega y una dirección de un DN. El método incluye entonces enviar el testigo de entrega y la clave de contenido al DN y recibir, correspondientemente, contenido cifrado del DN, el contenido cifrado que comprende al menos una parte del contenido objetivo que se cifra inicialmente por el CP usando una clave pública del CP, y que se cifra además por la CDN usando la clave de contenido proporcionada por el dispositivo de comunicación. El método incluye entonces descifrar el contenido cifrado usando una clave privada del dispositivo de comunicación, para obtener contenido descifrado para reproducción multimedia en el dispositivo de comunicación del abonado.

Según la invención, un dispositivo de comunicación de un abonado configurado para operación en una red de comunicación incluye circuitería de interfaz de comunicación configurada para enviar señales a la red de comunicación y recibir señales de la red de comunicación. El dispositivo de comunicación también incluye circuitería de procesamiento asociada operativamente con la interfaz de comunicación. La circuitería de procesamiento está configurada para enviar una solicitud de contenido a un sistema de CP alcanzable a través de la red de comunicación, la solicitud de contenido que identifica el contenido objetivo y que incluye una clave pública del dispositivo de comunicación. La circuitería de procesamiento también está configurada para recibir una respuesta del sistema de CP que identifica una CDN y que incluye un testigo de autorización y una clave de contenido que se deriva de la clave pública del dispositivo de comunicación y una clave privada del sistema de CP. La circuitería de procesamiento está configurada para enviar el testigo de autorización a la CDN y recibir, correspondientemente, un testigo de entrega y una dirección de un DN. La circuitería de procesamiento está configurada para enviar el testigo de entrega y la clave de contenido al DN y recibir, correspondientemente, contenido cifrado del DN, el contenido

cifrado que comprende al menos una parte del contenido objetivo que se cifra inicialmente por el CP usando una clave pública del CP, y que se cifra además por la CDN usando la clave de contenido proporcionada por el dispositivo de comunicación. La circuitería de procesamiento está configurada para descifrar el contenido cifrado usando una clave privada del dispositivo de comunicación, para obtener contenido descifrado para reproducción multimedia en el dispositivo de comunicación.

Según la invención, un método de operación en una CDN implementado por uno o más nodos de la CDN incluye recibir una solicitud de contenido objetivo, en donde la solicitud se origina desde un dispositivo de comunicación de un abonado que opera en una red de comunicación que incluye o está en comunicación con la CDN, y en donde la solicitud incluye un testigo de autorización asociado con un sistema de CP. El método incluye verificar el testigo de autorización y, condicionado a la verificación del testigo de autorización, seleccionar un DN dentro de la CDN, para su uso en la entrega del contenido objetivo al dispositivo de comunicación y enviar un testigo de entrega al dispositivo de comunicación, para su envío de vuelta por el dispositivo de comunicación al DN seleccionado. El testigo de entrega y una clave de contenido se reciben posteriormente desde el dispositivo de comunicación en el DN seleccionado, la clave de contenido que se deriva por el sistema de CP usando una clave pública del sistema de CP. El testigo de entrega se verifica y, condicionado a la verificación del testigo de entrega, se genera contenido cifrado que comprende al menos una parte del contenido objetivo, en base a la obtención de contenido cifrado inicialmente que está cifrado por el sistema de CP usando una clave privada del sistema de CP y una clave pública del dispositivo de comunicación y el contenido cifrado inicialmente se cifra además usando la clave de contenido y se envía al dispositivo de comunicación.

Según la invención, una CDN incluye una primera circuitería de interfaz de comunicación configurada para recibir una solicitud de contenido objetivo, en donde la solicitud se origina desde un dispositivo de comunicación que opera en una red de comunicación que incluye o está en comunicación con la CDN, y en donde la solicitud incluye un testigo de autorización asociado con un sistema de CP. La CDN también incluye una primera circuitería de procesamiento asociada operativamente con la primera circuitería de interfaz de comunicación y configurada para verificar el testigo de autorización. Condicionado a la verificación del testigo de autorización, la primera circuitería de procesamiento selecciona un DN dentro de la CDN, para su uso en la entrega del contenido objetivo al dispositivo de comunicación, y envía un testigo de entrega al dispositivo de comunicación, para su envío de vuelta por el dispositivo de comunicación al DN seleccionado. La CDN también incluye una segunda circuitería de interfaz de comunicación configurada para recibir el testigo de entrega y una clave de contenido, que se envían posteriormente a la CDN por el dispositivo de comunicación, la clave de contenido que se deriva por el sistema de CP usando una clave pública del sistema de CP. La CDN incluye una segunda circuitería de procesamiento asociada operativamente con la segunda circuitería de interfaz de comunicación y configurada para verificar el testigo de entrega. Condicionado a la verificación del testigo de entrega, la segunda circuitería de procesamiento genera contenido cifrado que comprende al menos una parte del contenido objetivo, en base a la obtención de contenido cifrado inicialmente que se cifra por el sistema de CP usando una clave privada del sistema de CP y una clave pública del dispositivo de comunicación. La segunda circuitería de procesamiento cifra además el contenido cifrado inicialmente usando la clave de contenido y envía el contenido cifrado al dispositivo de comunicación.

La invención incluye además productos de programas de ordenador y medios legibles por ordenador no transitorios que almacenan instrucciones que, cuando se ejecutan por un circuito de procesamiento, realizan las operaciones de las realizaciones descritas anteriormente.

Breve descripción de los dibujos

La Fig. 1 es un diagrama de bloques de una realización de un dispositivo de comunicación, una red de comunicación, una red de entrega de contenidos y un sistema proveedor de contenidos.

La Fig. 2 es un diagrama de bloques de una realización de un dispositivo de comunicación, una red de comunicación, una red de entrega de contenidos y un sistema de proveedor de contenidos, con respecto a la generación e intercambio de claves de cifrado y testigos para entrega de contenidos al dispositivo de comunicación.

La Fig. 3 es un diagrama de flujo de llamada o flujo de señal que ilustra una señalización de ejemplo entre un dispositivo de comunicación, una red de comunicación, una red de entrega de contenidos y un sistema proveedor de contenidos, con respecto a la entrega de contenidos al dispositivo de comunicación.

La Fig. 4 es un diagrama de flujo lógico de una realización de un método de procesamiento implementado por un dispositivo de comunicación, para obtener contenido de un sistema proveedor de contenidos, que se entrega desde una red de entrega de contenidos.

La Fig. 5 es un diagrama de flujo lógico de una realización de un método de procesamiento implementado por una red de entrega de contenidos, para proporcionar contenido a un dispositivo de comunicación.

La Fig. 6 es un diagrama de bloques de una implementación funcional de un dispositivo de comunicación, según algunas realizaciones.

La Fig. 7 es un diagrama de bloques de una implementación funcional de una red de entrega de contenidos, según algunas realizaciones.

Descripción detallada

Si las conexiones seguras de extremo a extremo se han de usar como se especifica para HTTP 2, por su naturaleza, todos los nodos intermedios no pueden almacenar en caché y encaminar tráfico de una forma tradicional. Esto es debido a que esos nodos intermedios no tienen forma de conocer el contenido dentro de los paquetes. Todos los paquetes se ven diferentes y, por lo tanto, no hay ningún valor en el almacenamiento en caché del contenido en el nodo de entrega (DN).

Puede ser beneficioso determinar cómo las redes de entrega de contenidos (CDN) pueden entregar contenido cifrado a los usuarios finales (abonados) de modo que el tráfico de red se pueda descargar. Al mismo tiempo, los abonados y proveedores de contenidos (CP) no quieren revelar sus planteamientos comerciales, perfiles y hábitos de servicio. Hay una creciente demanda del operador de ser ciego al contenido servido a los abonados. Por consiguiente, algunas realizaciones proporcionan un sistema de archivos cifrados/mecanismos de almacenamiento en caché que no revelan información a los operadores.

En algunas realizaciones, un CP es responsable de cifrar todos los datos que están yendo a ser entregados a sus abonados. El contenido objetivo, tal como un archivo de película, se cifra por el CP con su clave pública y se almacena en una CDN. En base a la solicitud del archivo de película de un abonado, el CP recupera la clave pública del abonado, y genera una nueva clave, o una clave de contenido, en base a la clave pública del abonado y la clave privada propia del CP. Esta clave de contenido se pasa a un nodo de entrega DN de la CDN a través del abonado. El DN vuelve a cifrar el archivo de película cifrado usando esta clave de contenido y lo entrega al abonado. El abonado puede descifrar el archivo de película cifrado usando su clave privada. De esta forma, las CDN no tienen la capacidad de saber qué hay en el archivo cifrado. Las CDN se pueden desplegar dentro o fuera de una red de operador. En el caso de despliegue interno, el DN está mucho más cerca de los abonados dado que el operador posee la red de acceso. Diversas realizaciones descritas en la presente memoria permiten que los CP seleccionen diferentes CDN para entregar contenido objetivo a sus abonados de una forma segura. La gestión de claves segura se proporciona por la red de operador, donde las interfaces usan HTTP seguro (HTTPS), como ejemplo.

Además del uso de la nueva clave de contenido, el contenido objetivo se puede entregar de manera segura usando testigos de autorización y de entrega de contenidos. Un CP genera un testigo de autorización usando un secreto compartido entre la CDN y el sistema de CP, y el CP da el testigo de autorización al abonado de modo que el abonado habilite que la CDN envíe el testigo de entrega al abonado. La CDN genera un testigo de entrega usando un secreto compartido entre un nodo de encaminamiento de solicitud (encaminador de solicitud o RR) de la CDN y un DN de la CDN seleccionado por el RR. El RR da el testigo de entrega al abonado de modo que el abonado pueda autorizar al DN seleccionado para proporcionar el contenido objetivo al abonado.

La Fig. 1 ilustra un dispositivo de comunicación 10 de ejemplo, un sistema de CP 14 de ejemplo y una CDN 18 de ejemplo que se comunican sobre una red de comunicación 12 y que están configurados según las enseñanzas de la presente memoria. El dispositivo de comunicación 10 es, por ejemplo, un equipo de usuario (UE) de un abonado o cualquier otro dispositivo informático que se comunica con el sistema de CP 14, la CDN 18 y/u otros dispositivos de comunicación sobre la red de comunicación 12. El dispositivo de comunicación 10 incluye circuitería de procesamiento 26, circuitería de interfaz de comunicación 20 y almacenamiento 28. La CDN 18 comprende un encaminador de solicitud (RR) 40 que incluye una primera circuitería de comunicación 42 y una primera circuitería de procesamiento 44. La CDN 18 también incluye uno o más nodos de entrega (DN) 50-1 a 50-M, cada DN 50 que incluye una segunda circuitería de interfaz de comunicación 52, una segunda circuitería de procesamiento 54 y un almacén de datos local 56. El sistema de CP 14 incluye uno o más servidores de CP 30, que incluyen cada uno circuitería de interfaz de comunicación 32, circuitería de procesamiento 34 y un almacén de contenido 36.

La circuitería de interfaz de comunicación 20 del dispositivo de comunicación 10 incluye circuitería de transceptor tal como la circuitería receptora 22 y la circuitería de transmisión 24 para la comunicación con otros dispositivos de comunicación, encaminadores y nodos con o sin red de comunicación 12. La circuitería de interfaz de comunicación 20 y el control de soporte y la configuración de la circuitería de procesamiento 26 pueden permitir que el dispositivo de comunicación 10 se comunique usando redes de ordenadores cableadas y/o inalámbricas, incluyendo el uso de más de una Tecnología de Acceso por Radio (RAT). Por ejemplo, el dispositivo de comunicación puede soportar múltiples RAT celulares, tales como Acceso Múltiple por División de Código de Banda Ancha (WCDMA) y Evolución a Largo Plazo (LTE), y puede soportar además RAT no celulares, tales como Comunicaciones de Campo Cercano (NFC), comunicaciones de Dispositivo a Dispositivo (D2D), protocolos Wi-Fi™ IEEE 802.11, protocolos Bluetooth®, etc. El dispositivo de comunicación también se puede configurar para operación en una Red Pública Móvil Terrestre (PLMN).

La circuitería de procesamiento 26 del dispositivo de comunicación 10 puede comprender más de un circuito de procesamiento. Por ejemplo, la circuitería de procesamiento 26 incluye uno o más microprocesadores, microcontroladores, Procesadores de Señal Digital o DSP, Circuitos Integrados de Aplicaciones Específicas o ASIC, Agrupaciones de Puertas Programables en Campo o FPGA, o Dispositivos Lógicos Programables Complejos o

CPLD. En general, la circuitería de procesamiento 26 comprende circuitería de procesamiento digital configurada apropiadamente e incluye o está asociada con circuitos de soporte, tales como circuitería de reloj, circuitería de control de potencia, circuitería de entrada/salida, y circuitería de interfaz que interconecta la circuitería de procesamiento 26 con la circuitería de interfaz de comunicación 20, por ejemplo, para transmisión de datos y de señalización de control, recepción de datos y de señalización de control, control de configuración, mediciones de intensidad de señal, etc.

La circuitería de procesamiento 26, en general, puede comprender uno o más circuitos fijos, uno o más circuitos programados, o cualquier mezcla de los mismos. En al menos una realización, la circuitería de procesamiento 26 está adaptada especialmente para llevar a cabo cualquiera de las operaciones de procesamiento del lado del dispositivo de comunicación enseñadas en la presente memoria, en base a su ejecución de instrucciones de programa de ordenador almacenadas en un medio legible por ordenador en o accesible por la circuitería de procesamiento 26.

En una realización de ejemplo, el almacenamiento 28 proporciona almacenamiento no transitorio para un programa de ordenador 30 y datos de configuración 32. En este caso, “no transitorio” significa que el almacenamiento 28 proporciona almacenamiento permanente, semipermanente o al menos temporalmente persistente para el programa de ordenador 30 y, como tal, abarca almacenamiento en memoria de trabajo no volátil y/o volátil de las instrucciones del programa de ordenador que comprende el programa de ordenador 30. Lo mismo es cierto para los datos de configuración 32, que pueden ser datos configurados previamente, datos determinados dinámicamente o una mezcla de los mismos. El almacenamiento 28 comprende al menos un tipo de medio legible por ordenador y puede comprender una mezcla de tipos. Tipos de ejemplos no limitantes de circuitos o dispositivos de almacenamiento incluyen un disco duro, un disco de estado sólido o SSD, memoria rápida, memoria EEPROM o ROM, y DRAM y/o SRAM con o sin batería de respaldo.

En algunas realizaciones, la circuitería de procesamiento 26 está configurada para operar el dispositivo de comunicación 10 en la red de comunicación 12 y enviar una solicitud de contenido a un sistema de CP 14 alcanzable a través de la red de comunicación 12, la solicitud de contenido que identifica el contenido objetivo y que incluye una clave pública del dispositivo de comunicación 10. La circuitería de procesamiento está configurada para recibir una respuesta del sistema de CP 14 que identifica una CDN e incluye un testigo de autorización y una nueva clave, o clave de contenido, que se deriva de la clave pública del dispositivo de comunicación 10 y una clave privada del sistema de CP 14. La circuitería de procesamiento 26 se configura también para enviar el testigo de autorización a la CDN 18 y recibir, correspondientemente, un testigo de entrega y una dirección de un DN 50. La circuitería de procesamiento 26 está configurada para enviar el testigo de entrega y la clave de contenido al DN 50 y recibir, correspondientemente, contenido cifrado del DN 50, el contenido cifrado que comprende al menos una parte del contenido objetivo que se cifra inicialmente por el CP usando una clave pública del CP, y que se cifra además por la CDN 18 usando la clave de contenido proporcionada por el dispositivo de comunicación 10. La circuitería de procesamiento 26 del dispositivo de comunicación 10 está configurada para descifrar el contenido cifrado usando una clave privada del dispositivo de comunicación 10, para obtener contenido descifrado para reproducción multimedia en el dispositivo de comunicación 10.

Volviendo a la CDN 18, la primera circuitería de interfaz de comunicación 42 en el RR 40 de la CDN 18 incluye circuitería para comunicación con otros dispositivos de comunicación, encaminadores y nodos con o sin red de comunicación 12. La primera circuitería de interfaz de comunicación 42 y el control y la configuración de soporte de la primera circuitería de procesamiento 44 pueden permitir que el dispositivo de comunicación 10 se comunique usando redes de ordenadores cableadas y/o inalámbricas.

La primera circuitería de procesamiento 44 de la CDN 18 puede comprender más de un circuito de procesamiento. Por ejemplo, la primera circuitería de procesamiento 44 incluye uno o más microprocesadores, microcontroladores, Procesadores de Señal Digital o DSP, Circuitos Integrados de Aplicaciones Específicas o ASIC, Agrupaciones de Puertas Programables en Campo o FPGA, o Dispositivos Lógicos Programables Complejos o CPLD. En general, la primera circuitería de procesamiento 44 comprende circuitería de procesamiento digital configurada apropiadamente e incluye o está asociada con circuitos de soporte, tal como circuitería de reloj, circuitería de control de potencia, circuitería de entrada/salida, y circuitería de interfaz que interconecta la primera circuitería de procesamiento 44 con la primera circuitería de interfaz de comunicación 42, por ejemplo, para transmisión de datos y de señalización de control, recepción de datos y de señalización de control, control de configuración, mediciones de intensidad de señal etc.

La primera circuitería de procesamiento 44, en general, puede comprender uno o más circuitos fijos, uno o más circuitos programados, o cualquier mezcla de los mismos. En al menos una realización, la primera circuitería de procesamiento 44 está adaptada especialmente para llevar a cabo cualquiera de las operaciones del RR 40 de las operaciones de procesamiento del lado de la CDN enseñadas en la presente memoria, en base a su ejecución de instrucciones de programa de ordenador almacenadas en un medio legible por ordenador o accesible por la primera circuitería de procesamiento 44. La segunda circuitería de procesamiento 54 está adaptada especialmente para llevar a cabo cualquiera de las operaciones del DN 50 de las operaciones de procesamiento del lado de la CDN enseñadas en la presente memoria, en base a su ejecución de instrucciones de programa de ordenador almacenadas en un medio legible por ordenador, tal como el almacén de datos local 56, en o accesible por la

segunda circuitería de procesamiento 54. En una realización de ejemplo, el almacén de datos local 56 puede ser cualquier mezcla de dispositivos o circuitos de almacenamiento que incluye un disco duro, un disco de estado sólido o SSD, memoria rápida, memoria EEPROM o ROM, y DRAM y/o SRAM con o sin batería de respaldo. El almacén de datos local 56 proporciona almacenamiento no transitorio para un programa de ordenador y datos de configuración.

En algunas realizaciones, la primera circuitería de procesamiento 44 de la CDN 18 está configurada para recibir una solicitud de contenido objetivo, en donde la solicitud se origina desde un dispositivo de comunicación 10 que opera en una red de comunicación 12 que incluye, está acoplada comunicativamente a, o en comunicación con la CDN 18, y en donde la solicitud incluye un testigo de autorización asociado con un sistema de CP 14. La primera circuitería de procesamiento 44 del RR 40 de la CDN 18 está operativamente asociada con la primera circuitería de interfaz de comunicación 42 y configurada para verificar el testigo de autorización. Tras la verificación del testigo de autorización, la primera circuitería de procesamiento 44 está configurada para seleccionar un DN 50 dentro de la CDN 18 para su uso en la entrega del contenido objetivo al dispositivo de comunicación 10 y enviar un testigo de entrega al dispositivo de comunicación 10, para el envío de vuelta por el dispositivo de comunicación 10 al DN 50 seleccionado.

La segunda circuitería de interfaz de comunicación 52 del DN 50 seleccionado de la CDN 18 está configurada para recibir el testigo de entrega y una clave de contenido, que se envía posteriormente a la CDN 18 por el dispositivo de comunicación 10, la clave de contenido que se deriva por el sistema de CP 14 usando una clave privada del sistema de CP 14 y una clave pública del dispositivo de comunicación 10. La segunda circuitería de procesamiento 54 está asociada operativamente con la segunda circuitería de interfaz de comunicación 52 y configurada para verificar el testigo de entrega. Tras la verificación del testigo de entrega, la segunda circuitería de procesamiento 54 está configurada para generar contenido cifrado que comprende al menos una parte del contenido objetivo, en base a la obtención de contenido cifrado inicialmente que se cifra por el sistema de CP 14 usando una clave pública del sistema de CP 14, y para cifrar además el contenido cifrado inicialmente usando la clave de contenido. La segunda circuitería de procesamiento 54 también está configurada para enviar el contenido cifrado al dispositivo de comunicación 10.

Las Figuras 2 y 3 se usarán para explicar una implementación de ejemplo. La Figura 2 ilustra un diagrama de bloques general de una arquitectura que incluye el dispositivo de comunicación 10 en comunicación con el sistema de CP 14, que también está en comunicación con múltiples CDN, tales como una CDN 18-1 y una CDN 18-2. La CDN 18-1 incluye dos capas de DN, un DN central 70-1 y unos DN de borde de servicio 50-1 y 50-2. La CDN 18-1 también incluye un encaminador de solicitud (RR) 40-1. Del mismo modo, la CDN 18-2 incluye un DN central 70-2, unos DN de servicio 50-3 y 50-4. La CDN 18-2 también incluye un RR 40-2. La red de comunicación 12 incluye un generador de claves 62 y un nodo de acceso, autenticación y autorización (AAA) 60. La Figura 3 muestra un flujo secuencial de los pasos que implican los elementos ilustrados en la Figura 2.

Para cualquier servicio proporcionado por un proveedor de contenidos (CP) a sus abonados, la comunicación de datos es esencial. Los datos entregados desde el servidor central a sus abonados se pueden poner en dos categorías, datos personales o datos comunes. Datos personales, tales como el uso de aplicaciones, perfil, información de crédito personal, no se puede compartir. Los datos comunes, tales como un archivo de película o una actualización de software, se pueden compartir con algunos o todos los abonados del CP. En general, los datos personales son diferentes de un abonado a otro, y su tamaño es limitado. Los datos personales no requieren que se envíe un ancho de banda de red alto desde el servidor del proveedor de contenidos al dispositivo del abonado. Por lo tanto, se pueden entregar directamente desde el sistema de CP 14 al dispositivo de comunicación 10.

Los datos comunes son normalmente de mayor tamaño y requieren un ancho de banda de red alto para ser entregados. La CDN 18 se considera como el elemento de red principal para entregar los datos comunes. Para utilizar la red CDN de manera más eficiente, los datos comunes se han de almacenar en caché en los DN 50. Con el fin de facilitar el almacenamiento en caché y la entrega de los datos, un objeto de medios común (CMO) se introduce para volver a empaquetar un archivo multimedia grande en varios CMO manejables. El CP usa un par de claves pública/privada para cifrar los CMO. Cada CMO se cifra con una clave pública de CP y tiene un identificador único o URL asignado. Los CMO con el mismo identificador tienen el mismo contenido.

Las realizaciones descritas en la presente memoria entregan los CMO a los abonados del servicio de una forma segura. Según algunas realizaciones, se puede describir un mecanismo en los siguientes pasos, que se muestran secuencialmente en las Figuras 2 y 3. En el paso 1, el dispositivo de comunicación 10 solicita un par de claves, pública y privada, de la red de comunicación 12. En el paso 2, las claves que se generan por el generador de claves 62 se reciben por el dispositivo de comunicación 10.

En el paso 3, la clave pública (K_pub) y la clave privada (K_pri) se almacenan en el dispositivo de comunicación 10. En el paso 4, se establece una conexión segura con el sistema de CP 14 usando la clave pública (K_pub). Tras el éxito, en el paso 5, se solicitan datos, tales como video, por el abonado a través del dispositivo de comunicación 10 en el paso 6. El dispositivo de comunicación 10 del abonado envía su clave pública (K_pub) al sistema de CP 14 tras solicitar el video. En la preparación de tal solicitud, el sistema de CP 14 empaqueta archivos de medios (o bien fuera de línea antes de cualquier solicitud o en respuesta a una solicitud), incluyendo el video solicitado, en uno o más

CMO, tales como el CMO-1 y el CMO-2. El origen de CP, proporcionado por un programa de software 30 ejecutado por la circuitería de procesamiento 26 del sistema de CP 14, cifra esos CMO usando la clave pública (Kcp_pub) del sistema de CP 14. El sistema de CP 14 también ha seleccionado una CDN 18-1 para entregar esos CMO. Esta selección también se puede hacer dinámicamente tras una solicitud de un abonado, en algunas realizaciones.

El programa de ordenador 30 del sistema de CP 14 también proporciona un portal de CP para recibir una clave pública (K_pub) desde el dispositivo de comunicación 10. En el paso 7, el portal de CP genera una nueva clave, o clave de contenido (K_nueva), en base a su clave privada (Kcp_pri) y la clave pública (K_pub) 10 del dispositivo de comunicación, y un testigo A para el video.

La generación de la nueva clave por el sistema de CP 14 se presta a sí misma a una discusión contextual del uso de nuevo cifrado de intermediario (PRE). Desde un punto de vista de alto nivel, PRE es un mecanismo, que implica algoritmos criptográficos, que se usa generalmente cuando un remitente B quiere revelar los contenidos de mensajes o archivos, enviados a él y cifrados con su clave pública, a un tercero C sin revelar su clave privada a un tercero C. Por consiguiente, el remitente B podría designar un intermediario para volver a cifrar uno de sus mensajes que se ha de enviar a un tercero C. Además, el remitente B no quiere que el intermediario sea capaz de leer los contenidos de sus mensajes. Esto genera una nueva clave que el tercero C puede usar para descifrar el mensaje. Ahora, si el receptor A envía un mensaje a B que fue cifrado bajo la clave pública del remitente B, el intermediario alterará el mensaje, permitiendo que el tercero C lo descifre con la nueva clave. Este método permite una serie de aplicaciones tales como reenvío de correo electrónico, monitorización de la aplicación de la ley y distribución de contenidos.

Conceptualmente, la delegación permite que el receptor A (titular de la clave) genere una clave de nuevo cifrado que se usa por un intermediario para volver a cifrar un mensaje ya cifrado enviado por el remitente B en un nuevo mensaje cifrado para un delegado C. Al hacerlo así, el delegado C será capaz de descifrar el mensaje enviado por el remitente B al receptor A sin ver la clave privada del receptor A. En otras palabras, el receptor A delega sus derechos de cifrado/descifrado al delegado C de modo que el delegado C pueda leer mensajes enviados al receptor A por el remitente B. El receptor A es, de este modo, el delegador.

Según algunas realizaciones, el sistema de CP 14 tiene el papel de delegador A, el abonado en el dispositivo de comunicación 10 tiene el papel de delegado C, y la CDN 18 tiene el papel de nuevo cifrador de intermediario. A diferencia del planteamiento PRE normal, donde un remitente y un receptor existen como entidades separadas, el sistema de CP 14 según diversas realizaciones asume el papel tanto del remitente B como del receptor A. De esta forma, el sistema de CP 14 puede enviar un archivo cifrado con su clave pública (Kcp_pub) a sí mismo. En este esquema, solamente el sistema de CP 14 puede descifrar el archivo cifrado con su propia clave privada (Kcp_pi). Esto significa que el operador/la CDN 18 no puede leer este archivo. Algunas de las ventajas de las realizaciones implican la forma en que se usa el nuevo cifrado en este caso. Es decir, la clave pública propia del sistema de CP 14 se usa para cifrar sus propios mensajes. Esto difiere de la forma normal en que se usa el PRE. Este cifrado se usa más tarde para delegar los archivos de lectura/descifrado del sistema de CP al abonado en el dispositivo de comunicación 10.

Continuando con la implementación de ejemplo en la Figura 2, en el paso 8 el sistema de CP 14 devuelve la clave de contenido (K_nueva) de vuelta al dispositivo de comunicación 10, con el testigo A autorizando el acceso al archivo de video o el o los CMO correspondientes. El sistema de CP 14 también puede devolver una dirección IP del RR 40-1 en la CDN 18-1 seleccionada. Obsérvese que esto es diferente del PRE normal, donde la nueva clave de nuevo cifrado se envía en lugar del intermediario de nuevo cifrado. La respuesta puede incluir los URL (localizadores uniformes de recursos) de CMO y datos personales privados. En el paso 9, el dispositivo de comunicación 10 recupera los URL de CMO y la clave de contenido (K_nueva). Si es necesario, el dispositivo de comunicación 10 resuelve el nombre de dominio completamente calificado (FQDN) para identificar el RR 40 en la CDN 18 seleccionada por el sistema de CP 14.

En el paso 10, el dispositivo de comunicación 10 envía la solicitud con el testigo A al RR 40-1 en la CDN 18-1 seleccionada para buscar el video, o el o los CMO del video. La CDN 18-1 recibe la clave de nuevo cifrado del dispositivo de comunicación 10. El paso 11 incluye la verificación por el RR 40-1 del testigo A. Después de que se realiza una autenticación con éxito para el testigo A, el paso 12 incluye verificar el FQDN o URL para determinar si el CP es de confianza. El paso 13 incluye la selección basada en proximidad y contenido. En el paso 14, el RR 40-1 selecciona un DN 50-1 que es capaz de servir al abonado en ese momento, y genera el testigo B para marcar la verificación realizada por el RR 40-1. En el paso 15, el testigo B y la dirección IP del DN 50-1 seleccionado se devuelven al dispositivo de comunicación 10.

En los pasos 16 y 17, se configura con éxito una conexión segura. En el paso 18, el dispositivo de comunicación 10 envía la solicitud con la clave de contenido (K_nueva) y el testigo B al DN 50-1 seleccionado. En el paso 19, el DN 50-1 valida el testigo B para acceder al CMO-1 solicitado, para asegurar que la solicitud proviene del RR 40-1 de confianza.

Como se ilustra por los pasos 20-28, si el CMO no está en la memoria caché local del DN 50-1, la clave de contenido (K_nueva) se almacena y se solicita el CMO desde el DN central 70-1. Este DN central 70-1 solicita el

CMO desde el CP origen del sistema de CP 14, que devuelve el CMO cifrado con la clave pública del sistema de CP 14 (Kcp_pub). El DN central 70-1 almacena el CMO cifrado. Mediante el paso 28, el CMO cifrado se pasa al DN 50-1 solicitante. En el paso 29, el CMO cifrado se almacena en el DN 50-1. También en el paso 29, el DN 50-1 vuelve a cifrar la película solicitada (uno o más CMO) con la clave de contenido (K_nueva) y envía el CMO-1 al dispositivo de comunicación 10 en el paso 30. En lugar de enviar el CMO- 1, el DN 50-1 podría permitir alternativamente la descarga, difusión de forma continua u otras formas de transmisión al dispositivo de comunicación 10. En el paso 31, el abonado 10 recibe el CMO-1 y lo descifra usando su clave privada. Obsérvese que la clave de contenido (K_nueva) puede tener un tiempo de expiración; la clave de contenido (K_nueva) en este caso puede expirar en el momento en que se descifra el CMO-1.

En otra realización, el video puede estar compuesto por un CMO-1 almacenado en el DN 50-1 y un CMO-2 almacenado en el DN 50-4. En este caso, el testigo A se puede usar para solicitar el CMO-2 de la película desde el RR 40-2 de la CDN 18-2, en el paso 32. El testigo B se puede devolver en el paso 33. En los pasos 34 y 35, el testigo B se usa con la clave de contenido para obtener el CMO-2, que se devuelve por el DN 50-4.

A diferencia del PRE normal donde los mensajes individuales se envían a los delegadores, que también son los receptores, el planteamiento de algunas realizaciones modifica este esquema con el fin de ser capaz de enviar archivos cifrados a muchos delegados, o muchos dispositivos de comunicación 10. En esencia, el receptor/delegador para el esquema delegado del sistema de PRE normal se modifica por varias realizaciones en un esquema de un delegador (sistema de CP 14) a muchos delegados (dispositivos de comunicación 10) y de un sistema de intercambio de mensajes basado en individuo a un sistema de archivos cifrados públicos. Obsérvese que para este PRE modificado, los papeles de remitente, receptor, delegador y delegado se mezclan entre el sistema de CP 14 y el abonado en el dispositivo de comunicación 10. El sistema de CP 14, según diversas realizaciones, es el remitente A y el receptor B al mismo tiempo. El delegado C es el abonado en el dispositivo de comunicación 10 y el PRE proporciona que el sistema de CP 14 sea el remitente y el receptor de los mensajes y el dispositivo de comunicación 10 sea el delegado C que lee los mensajes. Este sistema de PRE modificado permite almacenar en caché el contenido cifrado y manejar las solicitudes cifradas relacionadas.

Independientemente de sus detalles de implementación, el dispositivo de comunicación 10 en una o más realizaciones está configurado para realizar un método 400 tal como se muestra en la Figura 4. El método 400 incluye enviar una solicitud de contenido a un sistema de CP 14 alcanzable a través de la red de comunicación, la solicitud de contenido que identifica contenido objetivo y que incluye una clave pública del dispositivo de comunicación 10 (Bloque 402). Enviar la solicitud de contenido al sistema de CP 14 puede incluir realizar un intercambio de clave pública con el sistema de CP 14 y establecer, correspondientemente, una conexión segura al sistema de CP 14, y enviar la solicitud de contenido sobre la conexión segura al sistema de CP 14. El método 400 también incluye recibir una respuesta desde el sistema de CP 14 que identifica una CDN 18 e incluye un testigo de autorización y una clave de contenido que se deriva de la clave pública del dispositivo de comunicación 10 y una clave privada del sistema de CP 14 (Bloque 404).

El método 400 también incluye enviar el testigo de entrega y la clave de contenido al DN 50 y recibir, correspondientemente, contenido cifrado desde el DN 50, el contenido cifrado que comprende al menos una parte del contenido objetivo que se cifra inicialmente por el CP usando una clave pública del CP, y que se cifra además por la CDN 18 usando la clave de contenido proporcionada por el dispositivo de comunicaciones 10 (Bloque 406). Enviar el testigo de entrega y la clave de contenido al DN 50 puede incluir establecer una conexión segura al DN 50, y enviar el testigo de entrega y la clave de contenido sobre la conexión segura al DN 50. En algunos casos, el sistema de CP 14 empaqueta el contenido objetivo como uno o más CMO, cada CMO que se cifra por separado por el sistema de CP 14 y que tiene un testigo de autorización, clave de contenido y asociación de DN correspondientes. La asociación de DN puede incluir información que asocia el CMO respectivo a uno o más DN 50, que puede autorizar la entrega del CMO respectivo tras la verificación de la clave de contenido. El método 400 puede incluir entonces el envío del testigo de autorización y del testigo de entrega sobre una base por CMO.

El método 400 también incluye descifrar el contenido cifrado usando una clave privada del dispositivo de comunicación, para obtener contenido descifrado para reproducción multimedia en el dispositivo de comunicación (Bloque 408).

Independientemente de sus detalles de implementación, la CDN 18 en una o más realizaciones está configurada para realizar un método 500 tal como se muestra en la Figura 5. El método 500 incluye recibir una solicitud de contenido objetivo, en donde la solicitud se origina a partir de un dispositivo de comunicación 10 que opera en una red de comunicación 12 que incluye o está en comunicación con la CDN 18, y en donde la solicitud incluye un testigo de autorización asociado con un sistema de CP 14 (Bloque 502). El método 500 también incluye verificar el testigo de autorización (Bloque 504). En algunos casos, el sistema de CP 14 genera el testigo de autorización usando un primer secreto compartido, compartido entre la CDN 18 y el sistema de CP 14. En estos casos, verificar el testigo de autorización comprende usar el primer secreto compartido para verificar el testigo de autorización. Se determina si la verificación tiene éxito (Bloque 506). Si no tiene éxito, se procesa el fallo de verificación (Bloque 508).

Si la verificación tiene éxito, el método 500 incluye seleccionar un DN 50 dentro de la CDN 18, para su uso en la entrega del contenido objetivo al dispositivo de comunicación 10 (Bloque 510) y enviar un testigo de entrega al

dispositivo de comunicación 10, para envío de vuelta por el dispositivo de comunicación 10 al DN 50 seleccionado (Bloque 512). Seleccionar el DN 50 seleccionado puede incluir realizar una selección basada en la proximidad, basada en evaluar las trayectorias de entrega correspondientes entre el dispositivo de comunicación 10 y los respectivos de dos o más DN 50 dentro de la CDN 18. Seleccionar el DN 50 también puede incluir realizar una selección basada en contenidos, basada en al menos uno de: determinar cuál o cuáles entre los dos o más DN 50 están autorizados o aprovisionados de otro modo para entregar contenido que se origina en el sistema de CP 14 y determinar cuál o cuáles entre los dos o más DN 50 se sabe que tienen copias locales del contenido cifrado inicialmente correspondiente al contenido objetivo. También se pueden usar otros métodos de selección conocidos por los expertos en la técnica.

El método 500 también incluye recibir posteriormente el testigo de entrega y una clave de contenido del dispositivo de comunicación 10 en el DN 50 seleccionado, la clave de contenido que se deriva por el sistema de CP 14 usando una clave privada del sistema de CP 14 y una clave pública del dispositivo de comunicación 10 (Bloque 514). En el bloque 516, se verifica el testigo de entrega. Entonces se determina si la verificación tuvo éxito (Bloque 518). Si no es así, se procesa el fallo de verificación (Bloque 520). En algunos casos, la CDN 18 genera el testigo de entrega usando un segundo secreto compartido, compartido entre el nodo de entrega 50 seleccionado y un nodo de encaminamiento de solicitud 40 que maneja la solicitud del contenido objetivo entrante desde el dispositivo de comunicación 10. La verificación del testigo de entrega comprende el nodo de entrega 50 seleccionado usando el segundo secreto compartido para verificar el testigo de entrega.

Si la verificación tiene éxito, el método 500 incluye generar contenido cifrado que comprende al menos una parte del contenido objetivo, en base a la obtención de contenido cifrado inicialmente que está cifrado por el sistema de CP usando una clave pública del sistema de CP y cifrando además el contenido cifrado inicialmente usando la clave de contenido (Bloque 522). En algunos casos, el contenido cifrado inicialmente se obtiene de un almacén de datos local 56 asociado con el DN 50 seleccionado cuando el contenido cifrado inicialmente está disponible en el almacén de datos local 56. En otros casos, el método 500 incluye obtener el contenido cifrado inicialmente desde el sistema de CP 14 cuando el contenido cifrado inicialmente no está disponible en el almacén de datos local 56. El método 500 incluye además enviar el contenido cifrado al dispositivo de comunicación 10 (Bloque 524).

Algunas realizaciones proporcionan a un operador beneficiarse de su red de acceso mientras que entregan los contenidos cifrados a sus abonados de servicio de una forma segura. En tales casos, el CP externaliza su infraestructura de CDN al operador. Un abonado puede beneficiarse teniendo una buena experiencia de usuario con una solución que preserva su privacidad hacia el operador. El operador finalmente entrega los archivos cifrados al usuario en base a la disponibilidad de recursos y al tiempo de latencia en sus recursos. Por ejemplo, las redes de entrega más cercanas al abonado o menos cargadas se pueden usar para entrega de contenidos, minimizando la latencia para el usuario. Por lo tanto, el operador no puede leer lo que se descarga por el abonado.

En diversas realizaciones, se usa un esquema de nuevo cifrado de intermediario no interactivo para el PRE. Esto significa que la clave de nuevo cifrado se genera a partir de la clave privada del delegador y la clave pública del abonado. Se han propuesto mecanismos para esquemas de nuevo cifrado de intermediario no interactivo, tal como se describe en un documento titulado “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage” de Giuseppe Ateniese, Kevin Fu, Matthew Green y Susan Hohenberger. Transacciones de ACM sobre Información y Seguridad de Sistemas (TISSEC) 9.1 (2006): 1-30. No obstante, en este planteamiento, los bloques se cifran con una clave maestra, se descargan por el cliente y se transmiten por el cliente al servidor de acceso un nuevo cifrado. El control de acceso decide entonces permitir el acceso o no en base a la información previa proporcionada por el propietario del contenido. Según un planteamiento diferente, que se usa por algunas realizaciones, el contenido no se manipula o transmite por el abonado. El abonado recibe los datos de nuevo cifrados al final, pero no tiene voz sobre qué descargar y desde dónde. Tales decisiones son ahora responsabilidad de la CDN, o los DN y el RR. Esto significa que el operador, aunque no consciente del contenido, tiene control de qué descargar y desde dónde.

Además, un planteamiento de distribución de claves de algunas realizaciones difiere del que se trata en el documento de ACM en que las claves de cifrado no están bloqueadas con bloques de datos, y el abonado transmite su propia clave pública al CP, que a su vez genera la clave de nuevo cifrado y la envía al abonado. En el planteamiento del documento de ACM, el propietario del contenido envía claves de nuevo cifrado al control de acceso. Principalmente, en el planteamiento de diversas realizaciones descritas en la presente memoria, el nuevo cifrado de claves está entre el abonado y el CP, mientras que en el planteamiento del documento de ACM, el nuevo cifrado está entre el CP y la CDN.

Al final, el planteamiento del documento de ACM no está adaptado para almacenar en caché los archivos. Como cada bloque se cifra con una clave, esto significa que una vez que se revela la clave de un bloque, entonces el archivo se puede descargar y descifrar por cualquiera. Esta vulnerabilidad de seguridad empujaría lo más probable al operador a sustituir los archivos regularmente. Por el contrario, en el planteamiento de las diversas realizaciones descritas en la presente memoria, el mismo archivo se puede compartir entre muchos abonados, en la medida que el archivo/contenido se vuelva a cifrar. De este modo, las técnicas descritas actualmente están mejor adaptadas para distribuir el mismo contenido a diferentes abonados, en la medida que el planteamiento del documento de ACM

es específico para controlar el acceso a un archivo almacenado en un servidor de acceso no seguro y almacenamiento no de confianza.

Se debería entender que los métodos 400 y 500 ilustrados en las Figuras 2-5 son ejemplos de las técnicas descritas más plenamente anteriormente. Cada uno de estos métodos se puede modificar según cualquiera de las variaciones y detalles tratados. Los métodos ilustrados en las Figuras 2-5, y las variantes de los mismos, se pueden implementar usando los circuitos de procesamiento ilustrados en la Figura 1, según sea apropiado, donde los circuitos de procesamiento están configurados, por ejemplo, con código de programa apropiado almacenado en circuitos de memoria, para llevar a cabo las operaciones descritas anteriormente. Mientras que algunas de estas realizaciones se basan en un microprocesador programado u otro elemento de procesamiento programado, se apreciará que no todos los pasos de estas técnicas se realizan necesariamente en un único microprocesador o incluso en un único módulo. Realizaciones de las técnicas descritas actualmente incluyen además productos de programas de ordenador para su aplicación en un terminal inalámbrico, así como productos de programas de ordenador correspondientes para su aplicación en un aparato de estación base u otro aparato de nodo de red.

Este código de programa o las instrucciones del programa de ordenador también se pueden almacenar en un medio legible por ordenador no transitorio y tangible que puede dirigir a un ordenador u otro aparato de procesamiento de datos programables a funcionar de una manera particular, de manera que las instrucciones almacenadas en el medio legible por ordenador producen un artículo de fabricación que incluye instrucciones que implementan las funciones/actos especificados en los diagramas de bloques y/o bloques o bloques de diagramas de flujo. Por consiguiente, las realizaciones de los presentes conceptos inventivos se pueden incorporar en hardware y/o software (incluyendo microprogramas, software residente, microcódigo, etc.) que se ejecutan en un procesador tal como un procesador de señal digital, a los que se puede hacer referencia colectivamente como “circuitería”, “un módulo” o variantes de los mismos.

Se apreciará además que diversos aspectos de las realizaciones descritas anteriormente se pueden entender como que se llevan a cabo por “módulos” funcionales, que pueden ser instrucciones de programa que se ejecutan en un circuito de procesador apropiado, circuitería digital codificada por hardware y/o circuitería analógica, o combinaciones apropiadas de los mismos.

Por ejemplo, la Figura 6 ilustra un módulo funcional o arquitectura de circuito de ejemplo que se puede implementar en un dispositivo de comunicación 10, por ejemplo, en base a la circuitería de procesamiento 26 y el almacenamiento 28. La realización ilustrada incluye, al menos funcionalmente, un módulo de solicitud de contenido 602 para enviar una solicitud de contenido a un sistema de CP 14 alcanzable a través de la red de comunicación 12, la solicitud de contenido que identifica el contenido objetivo y que incluye una clave pública del dispositivo de comunicación 10. La implementación incluye un módulo de clave de contenido 604 para recibir una respuesta desde el sistema de CP 14 que identifica una CDN 18 e incluye un testigo de autorización y una clave de contenido que se deriva de la clave pública del dispositivo de comunicación 10 y una clave privada del sistema de CP 14. La implementación incluye un módulo de testigo de entrega 606 para enviar el testigo de autorización a la CDN 18 y recibir, correspondientemente, un testigo de entrega y una dirección de un DN 50. La implementación incluye un módulo de contenido 608 para enviar el testigo de entrega y la clave de contenido al DN 50 y recibir, correspondientemente, contenido cifrado del DN 50, el contenido cifrado que comprende al menos una parte del contenido objetivo que se cifra inicialmente por el CP usando una clave pública del CP, y que se cifra además por la CDN 18 usando la clave de contenido proporcionada por el dispositivo de comunicación 10. La implementación también incluye un módulo de descifrado 610 para descifrar el contenido cifrado usando una clave privada del dispositivo de comunicación 10, para obtener contenido descifrado para reproducción multimedia en el dispositivo de comunicación 10.

La Figura 7 ilustra un módulo funcional o arquitectura de circuito de ejemplo que se puede implementar en una CDN 18, por ejemplo, en base a la circuitería de procesamiento 44, 54 y el almacenamiento 56. La realización ilustrada incluye, al menos funcionalmente, un módulo de solicitud de contenido 702 para recibir una solicitud de contenido objetivo, en donde la solicitud se origina en un dispositivo de comunicación 10 que opera en una red de comunicación 12 que incluye o está en comunicación con la CDN 18, y en donde la solicitud incluye un testigo de autorización asociado con un sistema de CP 14. La implementación también incluye un módulo de testigo de entrega 704 para verificar el testigo de autorización y, condicionado a la verificación del testigo de autorización: seleccionar un DN 50 dentro de la CDN 18, para su uso en la entrega del contenido objetivo al dispositivo de comunicación 10, y enviar un testigo de entrega al dispositivo de comunicación 10, para envío de vuelta por el dispositivo de comunicación 10 al DN 50 seleccionado. La implementación incluye además un módulo de contenido 706 para recibir posteriormente el testigo de entrega y una clave de contenido del dispositivo de comunicación 10 en el nodo de entrega 50 seleccionado, la clave de contenido que se deriva por el sistema de CP 14 usando una clave privada del sistema de CP 14 y una clave pública del dispositivo de comunicación 10, verificar el testigo de entrega y, condicionado a la verificación del testigo de entrega: generar contenido cifrado que comprenda al menos una parte del contenido objetivo, en base a la obtención de contenido cifrado inicialmente que está cifrado por el sistema de CP 14 usando una clave privada del sistema de CP 14 y una clave pública del dispositivo de comunicación 10 y cifrando además el contenido cifrado inicialmente usando la clave de contenido, y enviando el contenido cifrado al dispositivo de comunicación 10.

Las modificaciones y otras variantes de la realización o realizaciones descritas vendrán a la mente de un experto en la técnica que tiene el beneficio de las enseñanzas presentadas en las descripciones anteriores y las figuras asociadas. Por lo tanto, se ha de entender que la realización o realizaciones no se han de limitar a los ejemplos específicos descritos y que las modificaciones y otras variantes se pretende que estén incluidas dentro del alcance de la invención como se define por las reivindicaciones.

Aunque se pueden emplear en la presente memoria términos específicos, se usan solamente en un sentido genérico y descriptivo y no con propósitos de limitación.

REIVINDICACIONES

1. Un método (400) de operación implementado por un dispositivo de comunicación (10) configurado para operación en una red de comunicación (12), el método (400) que comprende:

enviar (402) una solicitud de contenido a un sistema de Proveedor de Contenidos, CP (14) alcanzable a través de la red de comunicación (12), la solicitud de contenido que identifica el contenido objetivo y que incluye una clave pública del dispositivo de comunicación (10);

recibir (404) una respuesta desde el sistema de CP (14), la respuesta que identifica una Red de Entrega de Contenidos, CDN, (18) y que incluye un testigo de autorización y una clave de contenido que se deriva de la clave pública del dispositivo de comunicación (10) y una clave privada del sistema de CP (14);

enviar (406) el testigo de autorización a la CDN (18) y recibir, correspondientemente, un testigo de entrega y una dirección de un nodo de entrega (50);

enviar (408) el testigo de entrega y la clave de contenido al nodo de entrega (50) y recibir, correspondientemente, contenido cifrado desde el nodo de entrega (50), el contenido cifrado que comprende al menos una parte del contenido objetivo que se cifra inicialmente por el CP usando una clave pública del CP, y que se cifra además por la CDN (18) usando la clave de contenido proporcionada por el dispositivo de comunicación (10); y

descifrar (410) el contenido cifrado usando una clave privada del dispositivo de comunicación (10), para obtener contenido descifrado para reproducción multimedia en el dispositivo de comunicación (10).

2. El método (400) de la reivindicación 1, en donde enviar (402) la solicitud de contenido al sistema de CP (14) comprende realizar un intercambio de clave pública con el sistema de CP (14) y establecer, correspondientemente, una conexión segura al sistema de CP (14), y enviar la solicitud de contenido sobre la conexión segura al sistema de CP (14) y, opcionalmente, en donde enviar (408) el testigo de entrega y la clave de contenido al nodo de entrega (50) comprende establecer una conexión segura al nodo de entrega (50), y enviar el testigo de entrega y la clave de contenido sobre la conexión segura al nodo de entrega (50) y, opcionalmente, en donde el sistema de CP (14) empaqueta el contento objetivo como uno o más Objetos de Gestión de Contenido, CMO, cada CMO que se cifra por separado por el sistema de CP (14) y que tiene un testigo de autorización, clave de contenido y asociación de nodos de entrega correspondientes, y en donde el método (400) incluye enviar el testigo de autorización y el testigo de entrega sobre una base por CMO.

3. El método (400) de cualquiera de las reivindicaciones 1-2, en donde el dispositivo de comunicación (10) comprende un dispositivo de comunicación inalámbrico (10) configurado para operación en una Red Pública Móvil Terrestre, PLMN.

4. Un dispositivo de comunicación (10) configurado para operación en una red de comunicación (12), el dispositivo de comunicación (10) que comprende:

circuitería de interfaz de comunicación (20) configurada para enviar señales a la red de comunicación (12) y recibir señales de la red de comunicación (12); y

circuitería de procesamiento (26) asociada operativamente con la interfaz de comunicación (20) y configurada para:

enviar una solicitud de contenido a un sistema de Proveedor de Contenidos, CP (14) alcanzable a través de la red de comunicación (12), la solicitud de contenido que identifica contenido objetivo y que incluye una clave pública del dispositivo de comunicación (10);

recibir una respuesta desde el sistema de CP (14), la respuesta que identifica una Red de Entrega de Contenidos, CDN, (18) y que incluye un testigo de autorización y una clave de contenido que se deriva de la clave pública del dispositivo de comunicación (10) y una clave privada del sistema de CP (14);

enviar el testigo de autorización a la CDN (18) y recibir, correspondientemente, un testigo de entrega y una dirección de un nodo de entrega (50);

enviar el testigo de entrega y la clave de contenido al nodo de entrega (50) y recibir, correspondientemente, contenido cifrado desde el nodo de entrega (50), el contenido cifrado que comprende al menos una parte del contenido objetivo que se cifra inicialmente por el CP usando una clave pública del CP, y que se cifra además por la CDN (18) usando la clave de contenido proporcionada por el dispositivo de comunicación (10); y

descifrar el contenido cifrado usando una clave privada del dispositivo de comunicación (10), para obtener contenido descifrado para reproducción multimedia en el dispositivo de comunicación (10).

5. El dispositivo de comunicación (10) de la reivindicación 4, en donde la circuitería de procesamiento (26) está configurada para enviar la solicitud de contenido al sistema de CP (14) realizando un intercambio de clave pública

con el sistema de CP (14) y establecer, correspondientemente, una conexión segura al sistema de CP (14), y enviar la solicitud de contenido sobre la conexión segura al sistema de CP (14), y opcionalmente, en donde la circuitería de procesamiento (26) está configurada para enviar el testigo de entrega y la clave de contenido al nodo de entrega (50) estableciendo una conexión segura al nodo de entrega (50), y enviar el testigo de entrega y la clave de contenido sobre la conexión segura al nodo de entrega (50) y, opcionalmente, en donde el sistema de CP (14) empaqueta el contento objetivo como uno o más Objetos de Gestión de Contenido, CMO, cada CMO que está cifrado por separado por el sistema de CP (14) y que tiene un testigo de autorización, clave de contenido y asociación de nodos de entrega correspondientes, y en donde la circuitería de procesamiento (26) está configurada para enviar el testigo de autorización y el testigo de entrega sobre una base por CMO.

6. El dispositivo de comunicación (10) de cualquiera de las reivindicaciones 4-5, en donde el dispositivo de comunicación (10) comprende un dispositivo de comunicación inalámbrico configurado para operación en una Red Pública Móvil Terrestre, PLMN.

7. Un método (500) de operación en una Red de Entrega de Contenidos, CDN (18), el método (500) implementado por uno o más nodos de la CDN (18) y que comprende:

recibir (502) una solicitud de contenido objetivo, en donde la solicitud se origina en un dispositivo de comunicación (10) que opera en una red de comunicación (12) que incluye o está en comunicación con la CDN (18), y en donde la solicitud incluye un testigo de autorización asociado con un sistema de proveedor de contenidos, CP;

verificar (504) el testigo de autorización y, condicionado a la verificación del testigo de autorización:

seleccionar (510) un nodo de entrega (50) dentro de la CDN (18), para su uso en la entrega del contenido objetivo al dispositivo de comunicación (10);

enviar (512) un testigo de entrega al dispositivo de comunicación (10), para envío de vuelta por el dispositivo de comunicación (10) al nodo de entrega (50) seleccionado;

recibir (514) posteriormente el testigo de entrega y una clave de contenido desde el dispositivo de comunicación (10) en el nodo de entrega seleccionado (50), la clave de contenido que se deriva por el sistema de CP (14) usando una clave privada del sistema de CP (14) y una clave pública del dispositivo de comunicación (10); y

verificar (516) el testigo de entrega y, condicionado a la verificación del testigo de entrega:

generar (522) contenido cifrado que comprende al menos una parte del contenido objetivo, en base a la obtención de contenido cifrado inicialmente que está cifrado por el sistema de CP (14) usando una clave pública del sistema de CP (14) y cifrar además el contenido cifrado inicialmente usando la clave de contenido; y

enviar (524) el contenido cifrado al dispositivo de comunicación (10).

8. El método (500) de la reivindicación 7, en donde obtener el contenido cifrado inicialmente comprende obtener el contenido cifrado inicialmente de un almacén de datos local (56) asociado con el nodo de entrega (50) seleccionado cuando el contenido cifrado inicialmente está disponible en el almacén de datos local (56) y obtener el contenido cifrado inicialmente del sistema de CP (14) cuando el contenido cifrado inicialmente no está disponible en el almacén de datos local (56).

9. El método (500) de la reivindicación 7 u 8, en donde seleccionar (510) el nodo de entrega (50) seleccionado comprende realizar una selección basada en la proximidad, basada en la evaluación de las trayectorias de entrega correspondientes entre el dispositivo de comunicación (10) y los respectivos de dos o más nodos de entrega (50) dentro de la CDN (18).

10. El método (500) de la reivindicación 9, en donde seleccionar el nodo de entrega (50) seleccionado comprende además realizar una selección basada en contenido, en base a al menos uno de:

determinar cuál o cuáles entre los dos o más nodos de entrega (50) están autorizados o aprovisionados de otro modo para entregar contenido que se origina en el sistema de CP (14); y

determinar cuál o cuáles entre los dos o más nodos de entrega (50) se sabe que tienen copias locales del contenido cifrado inicialmente correspondientes al contenido objetivo.

11. El método (500) de cualquiera de las reivindicaciones 7-10, en donde el sistema de CP (14) genera el testigo de autorización usando un primer secreto compartido, compartido entre la CDN (18) y el sistema de CP (14), y en donde verificar el testigo de autorización comprende usar el primer secreto compartido para verificar el testigo de autorización; y, opcionalmente, en donde la CDN (18) genera el testigo de entrega usando un segundo secreto compartido, compartido entre el nodo de entrega (50) seleccionado y un nodo de encaminamiento de solicitud (40) de la CDN (18) que maneja la solicitud del contenido objetivo entrante desde el dispositivo de comunicación (10), y en donde verificar el testigo de entrega comprende que el nodo de entrega (50) seleccionado usando el segundo secreto compartido verifique el testigo de entrega, o, en donde las operaciones (502-524) se realizan usando un

mecanismo de nuevo cifrado de intermediario, PRE, en donde la CDN (18) actúa como intermediario para el mecanismo de PRE, y en donde el mecanismo de PRE utiliza la clave de contenido para nuevo cifrado para habilitar por ello la entrega del contenido objetivo del sistema de CP (14) al dispositivo de comunicación (10) sin exponer el contenido objetivo a la CDN (18) y sin exponer la clave privada del sistema de CP (14) al dispositivo de comunicación (10).

12. Una Red de Entrega de Contenidos, CDN (18), que comprende:

una primera circuitería de interfaz de comunicación (42) configurada para recibir una solicitud de contenido objetivo, en donde la solicitud se origina en un dispositivo de comunicación (10) que opera en una red de comunicación (12) que incluye o está en comunicación con la CDN (18), y en donde la solicitud incluye un testigo de autorización asociado con un sistema de Proveedor de Contenidos, CP;

una primera circuitería de procesamiento (44) asociada operativamente con la primera circuitería de interfaz de comunicación (42) y configurada para verificar el testigo de autorización y, condicionado a la verificación del testigo de autorización:

seleccionar un nodo de entrega (50) dentro de la CDN (18), para su uso en la entrega del contenido objetivo al dispositivo de comunicación (10); y

enviar un testigo de entrega al dispositivo de comunicación (10), para envío de vuelta por el dispositivo de comunicación (10) al nodo de entrega seleccionado (50);

una segunda circuitería de interfaz de comunicación (52) configurada para recibir el testigo de entrega y una clave de contenido, que se envía posteriormente a la CDN (18) por el dispositivo de comunicación (10), la clave de contenido que se deriva por el sistema de CP (14) usando una clave privada del sistema de CP (14) y una clave pública del dispositivo de comunicación (10); y

una segunda circuitería de procesamiento (54) asociada operativamente con la segunda circuitería de interfaz de comunicación (52) y configurada para verificar el testigo de entrega y, condicionado a la verificación del testigo de entrega:

generar contenido cifrado que comprenda al menos una parte del contenido objetivo, en base a la obtención de contenido cifrado inicialmente que se cifra por el sistema de CP (14) usando una clave pública del sistema de CP (14) y cifrando además el contenido cifrado inicialmente usando la clave de contenido; y

enviar el contenido cifrado al dispositivo de comunicación (10).

13. La CDN (18) de la reivindicación 12, en donde la CDN (18) incluye un nodo de encaminamiento de solicitud (40) que comprende la primera circuitería de interfaz de comunicación (42) y la primera circuitería de procesamiento (44), e incluye además dos o más nodos de entrega (50), uno de los cuales se selecciona por el nodo de encaminamiento de solicitud (40) como el nodo de entrega (50) seleccionado e incluye la segunda circuitería de interfaz de comunicación (52) y la segunda circuitería de procesamiento (54), y, opcionalmente, en donde la segunda circuitería de procesamiento (52) está configurada para obtener el contenido cifrado inicialmente obteniendo el contenido cifrado inicialmente de un almacén de datos local (56) asociado con el nodo de entrega (50) seleccionado cuando el contenido cifrado inicialmente está disponible en el almacén de datos local (56), y obtener el contenido cifrado inicialmente del sistema de CP (14) cuando el contenido cifrado inicialmente no está disponible en el almacén de datos local (56).

14. La CDN (18) de cualquiera de las reivindicaciones 12-13, en donde la primera circuitería de procesamiento (44) está configurada para seleccionar el nodo de entrega (50) seleccionado realizando una selección basada en la proximidad, basada en la evaluación de las trayectorias de entrega correspondientes entre el dispositivo de comunicación (10) y los respectivos de dos o más nodos de entrega (50) dentro de la CDN (18).

15. La CDN (18) de la reivindicación 14, en donde la primera circuitería de procesamiento (44) está configurada para seleccionar el nodo de entrega (50) realizando además una selección basada en contenido, basada en al menos uno de: determinar cuál o cuáles entre los dos o más nodos de entrega (50) están autorizados o aprovisionados de otro modo para entregar contenido que se origina en el sistema de CP (14); y determinar cuál o cuáles entre los dos o más nodos de entrega (50) se sabe que tienen copias locales del contenido cifrado inicialmente correspondiente al contenido objetivo.

16. La CDN (18) de cualquiera de las reivindicaciones 12-15, en donde el sistema de CP (14) genera el testigo de autorización usando un primer secreto compartido, compartido entre la CDN (18) y el sistema de CP (14), y en donde la primera circuitería de procesamiento (44) está configurada para usar el primer secreto compartido para verificar el testigo de autorización y, opcionalmente, en donde la primera circuitería de procesamiento (44) está configurada para generar el testigo de entrega usando un segundo secreto compartido, compartido entre el nodo de entrega (50) seleccionado y un nodo de encaminamiento de solicitud (40) que maneja la solicitud del contenido

objetivo entrante desde el dispositivo de comunicación (10), y en donde la segunda circuitería de procesamiento (54) está configurada para usar el segundo secreto compartido para verificar el testigo de entrega.

17. Un producto de programa de ordenador que comprende instrucciones de programa (30) para un procesador (26) en un dispositivo de comunicación (10), en donde las instrucciones de programa (30) están configuradas para hacer que el dispositivo de comunicación (10) cuando las instrucciones de programa (30) se ejecutan por el procesador (26):

enviar (402) una solicitud de contenido a un sistema de Proveedor de Contenidos, CP (14) alcanzable a través de la red de comunicación (12), la solicitud de contenido que identifica el contenido objetivo y que incluye una clave pública del dispositivo de comunicación (10);

recibir (404) una respuesta del sistema de CP (14), la respuesta que identifica una Red de Entrega de Contenidos, CDN, (18) y que incluye un testigo de autorización y una clave de contenido que se deriva de la clave pública del dispositivo de comunicación (10) y una clave privada del sistema de CP (14);

enviar (406) el testigo de autorización a la CDN (18) y reciba, correspondientemente, un testigo de entrega y una dirección de un nodo de entrega (50);

enviar (408) el testigo de entrega y la clave de contenido al nodo de entrega (50) y reciba, correspondientemente, contenido cifrado del nodo de entrega (50), el contenido cifrado que comprende al menos una parte del contenido objetivo que se cifra inicialmente por el CP usando una clave pública del CP, y que se cifra además por la CDN (18) usando la clave de contenido proporcionada por el dispositivo de comunicación (10); y

descifrar (410) el contenido cifrado usando una clave privada del dispositivo de comunicación (10), para obtener contenido descifrado para reproducción multimedia en el dispositivo de comunicación (10).

18. Un medio legible por ordenador no transitorio (28) que comprende, almacenado en el mismo, el producto de programa de ordenador de la reivindicación 17.

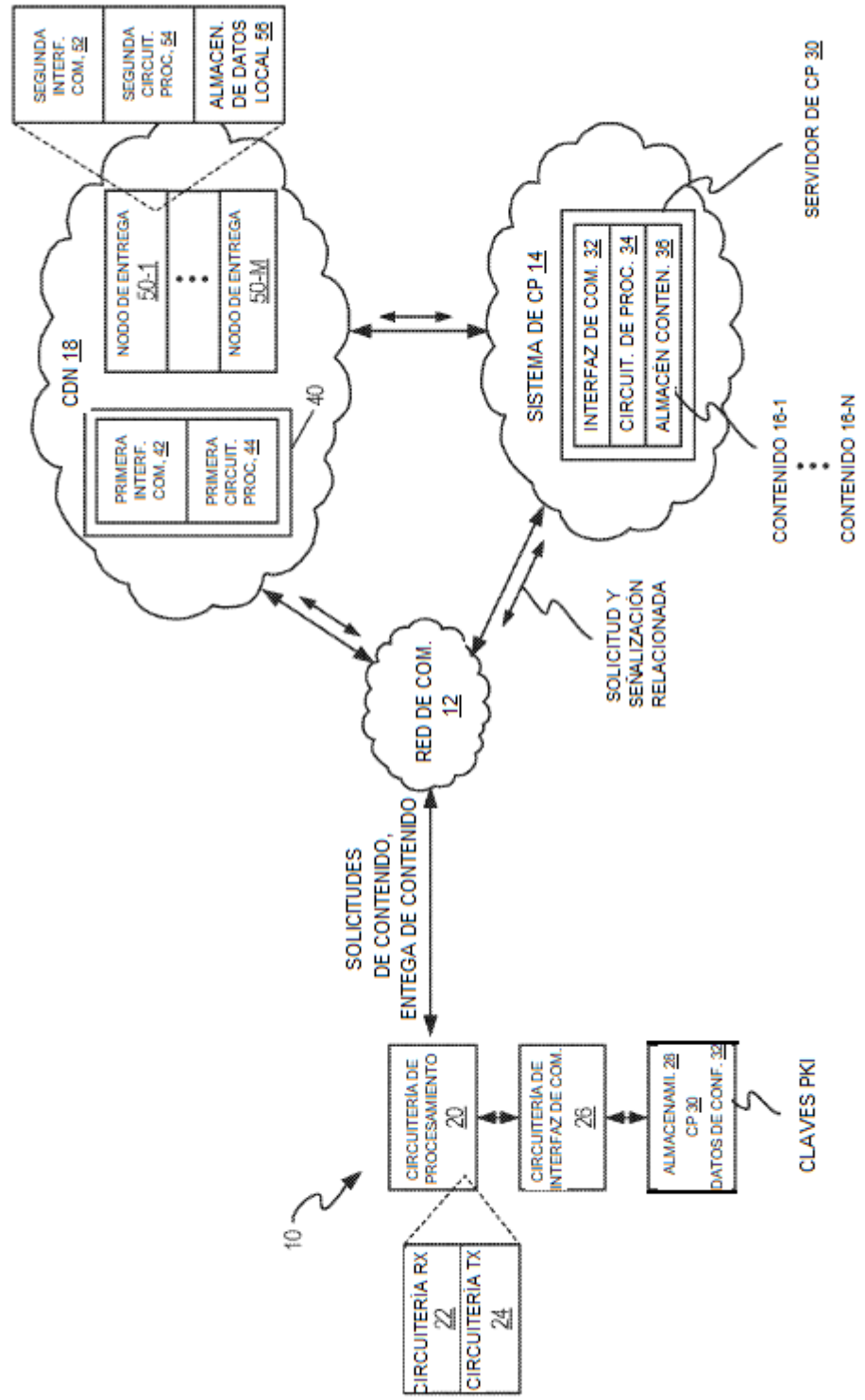
SEGUNDA INTERF. COM. 52
SEGUNDA CIRCUIT. PROC. 54
ALMACEN. DE DATOS LOCAL 56
CDN 18
NODO DE ENTREGA 50-1
NODO DE ENTREGA 50-M
PRIMERA INTERF. COM. 42
PRIMERA CIRCUIT. PROC. 44
40
SISTEMA DE CP 14
INTERFAZ DE COM. 32
CIRCUIT. DE PROC. 34
ALMACÉN CONTEN. 36
SERVIDOR DE CP 30
CONTENIDO 16-1
CONTENIDO 16-N
RED DE COM. 12
SOLICITUD Y SEÑALIZACIÓN RELACIONADA
SOLICITUDES DE CONTENIDO, ENTEGA DE CONTENIDO
CIRCUITERÍA DE PROCESAMIENTO 20
CIRCUITERÍA DE INTERFAZ DE COM. 26
ALMACENAMI. 28
CP 30
DATOS DE CONF. 38
CLAVES PKI
CIRCUITERÍA RX 22
CIRCUITERÍA TX 24
10

FIG. 1

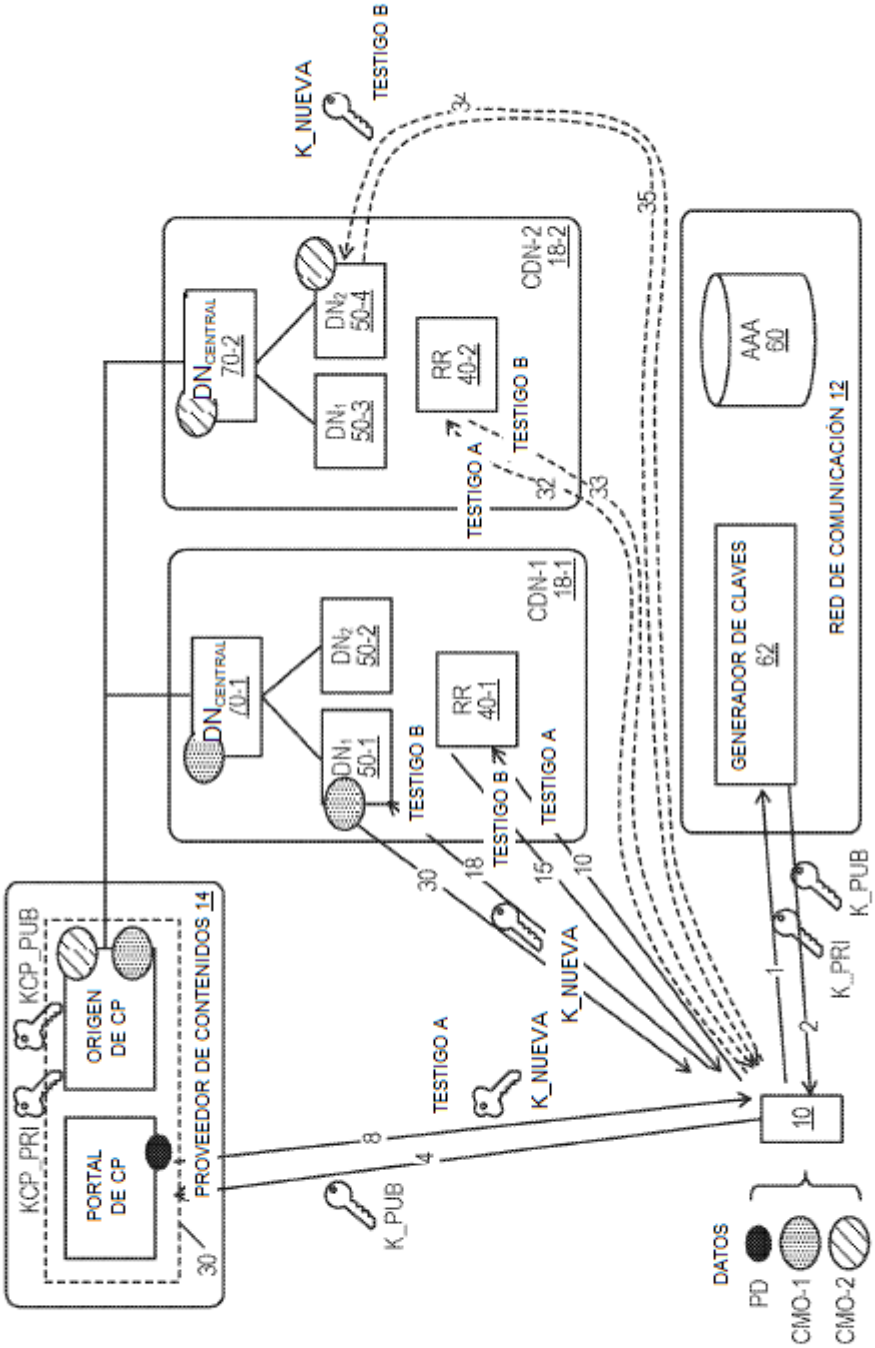
PROVEEDOR DE CONTENIDOS 14
PORTAL DE CP
ORIGEN DE CP
KCP_PRI
KCP_PUB
30
K_PUB
8
4
TESTIGO A
K_NUEVA
10
K_PRI
K_PUB
1
2
GENERADOR DE CLAVES 62
AAA 60
RED DE COMUNICACIÓN 12
DATOS
PD
CMO-1
CMO-2
CDN-1 18-1
DN CENTRAL 40-1
DN1 50-1
DN2 50-2
RR 40-1
TESTIGO B
TESTIGO A
30
18
15
10
CDN-2 18-2
DN CENTRAL 70-2
DN1 50-3
DN2 50-4
RR 40-2
TESTIGO A
TESTIGO B
32
33
K_NUEVA
TESTIGO B
34
35

FIG. 2

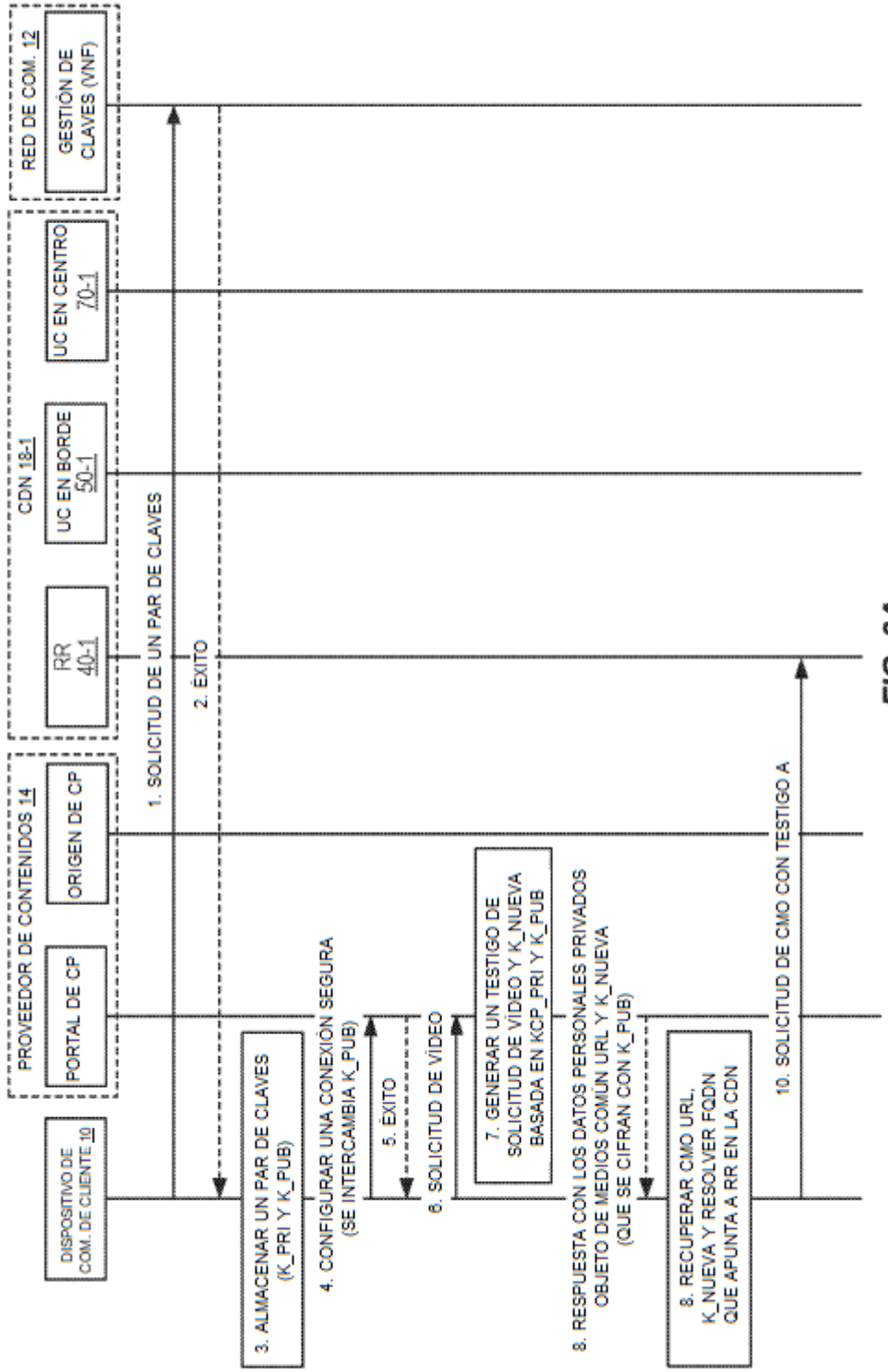
RED DE COM. 12
GESTIÓN DE CLAVES (VNF)
CDN 18-1
UC EN CENTRO 70-1
UC EN BORDE 50-1
RR 40-1
PROVEEDOR DE CONTENIDOS 14
ORIGEN DE CP
PORTAL DE CP
DISPOSITIVO DE COM. DE CLIENTE 10
1. SOLICITUD DE UN PAR DE CLAVES
2. ÉXITO
3. ALMACENAR UN PAR DE CLAVES (K_PRI Y K_PUB)
4. CONFIGURAR UNA CONEXIÓN SEGURA (SE INTERCAMBIA K_PUB)
5. ÉXITO
6. SOLICITUD DE VÍDEO
7. GENERAR UN TESTIGO DE SOLICITUD DE VÍDEO Y K_NUEVA BASADA EN KCP_PRI Y K_PUB
8. RESPUESTA CON LOS DATOS PERSONALES PRIVADOS OBJETO DE MEDIOS COMÚN URL Y K_NUEVA (QUE SE CIFRAN CON K_PUB)
8. RECUPERAR CMO URL, K_NUEVA Y RESOLVER FQDN QUE APUNTA A RR EN LA CDN
10. SOLICITUD DE CMO CON TESTIGO A

FIG. 3A

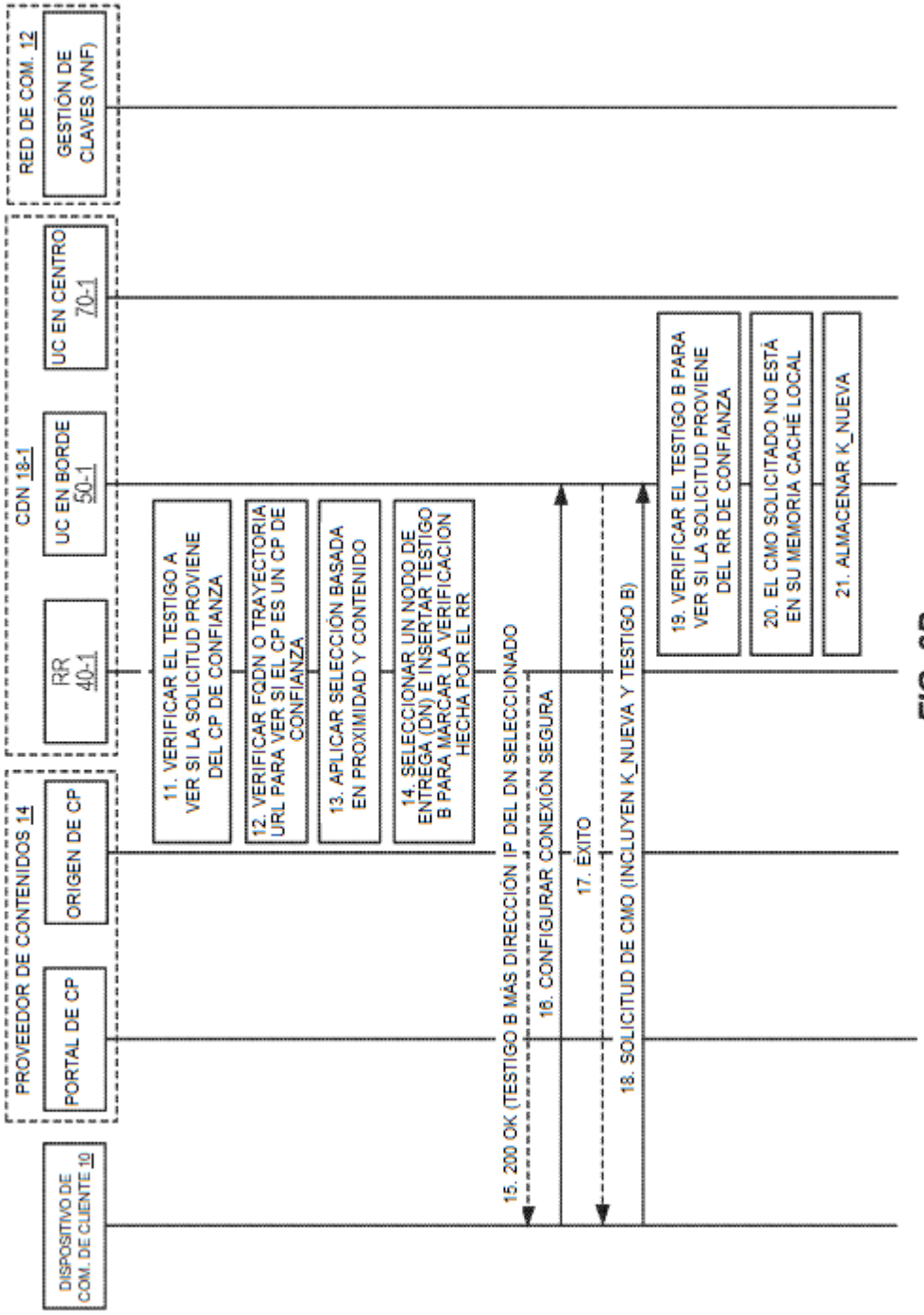
DISPOSITIVO DE COM. DE CLIENTE 10
PROVEEDOR DE CONTENIDOS 14
PORTAL DE CP
ORIGEN DE CP
CDN 18-1
RR 40-1
UC EN BORDE 50-1
UC EN CENTRO 70-1
RED DE COM. 12
GESTIÓN DE CLAVES (VNF)
11. VERIFICAR EL TESTIGO A VER SI LA SOLICITUD PROVIENE DEL CP DE CONFIANZA
12. VERIFICAR FQDN O TRAYECTORIA URL PARA VER SI EL CP ES UN CP DE CONFIANZA
13. APLICAR SELECCIÓN BASADA EN PROXIMIDAD Y CONTENIDO
14. SELECCIONAR UN NODO DE ENTREGA (DN) E INSERTAR TESTIGO B PARA MARCAR LA VERIFICACIÓN HECHA POR EL RR
15. 200 OK (TESTIGO B MÁS DIRECCIÓN IP DEL DN SELECCIONADO
16. CONFIGURAR CONEXIÓN SEGURA
17. ÉXITO
18. SOLICITUD DE CMO (INCLUYEN K_NUEVA Y TESTIGO B)
19. VERIFICAR EL TESTIGO B PARA VER SI LA SOLICITUD PROVIENE DEL RR DE CONFIANZA
20. EL CMO SOLICITADO NO ESTÁ EN SU MEMORIA CACHÉ LOCAL
21. ALMACENAR K_NUEVA

FIG. 3B

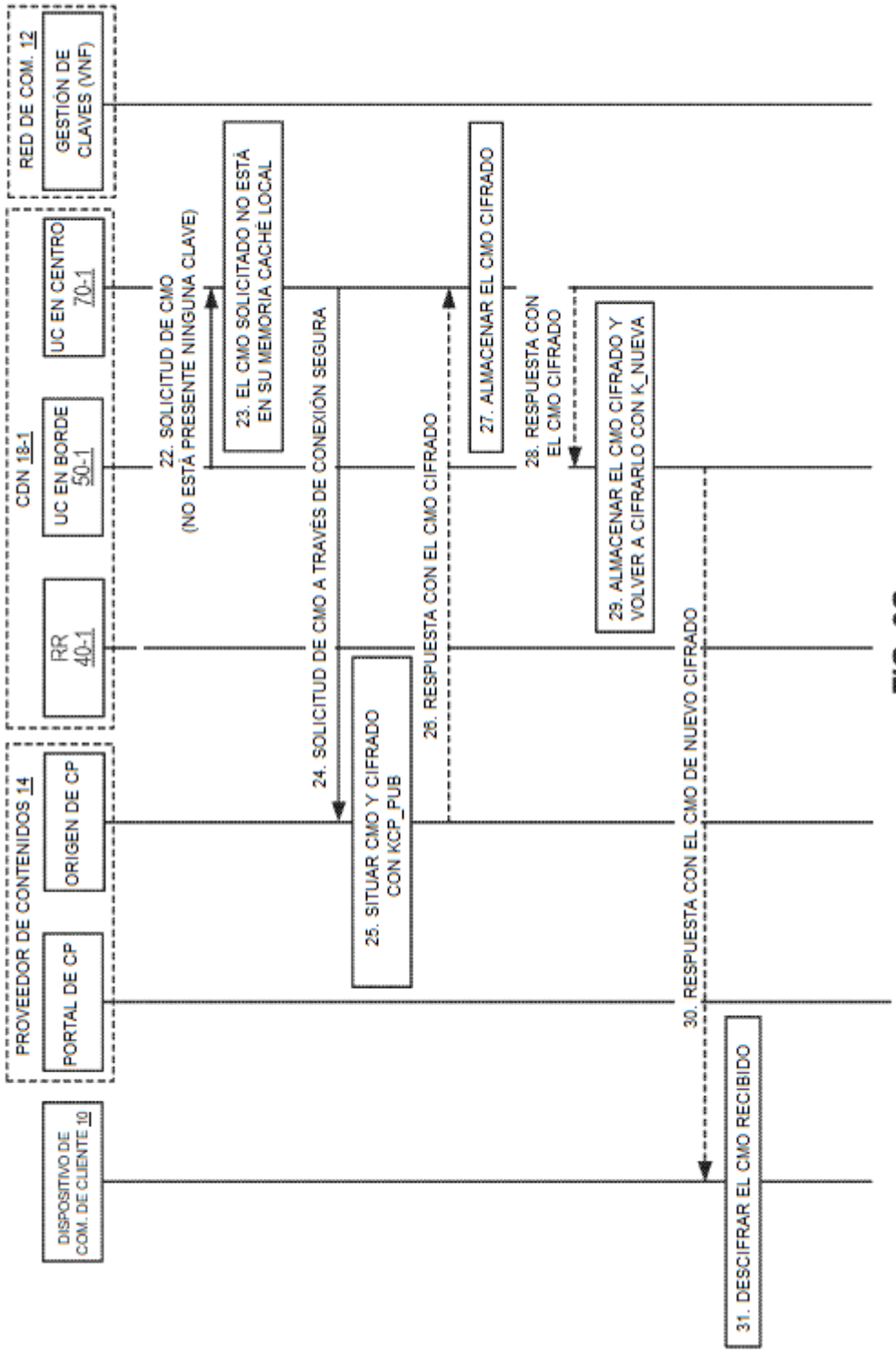
DISPOSITIVO DE COM. DE CLIENTE 10
PROVEEDOR DE CONTENIDOS 14
PORTAL DE CP
ORIGEN DE CP
CDN 18-1
RR 40-1
UC EN BORDE 50-1
UC EN CENTRO 70-1
RED DE COM. 12
GESTIÓN DE CLAVES (VNF)
22. SOLICITUD DE CMO (NO ESTÁ PRESENTE NINGUNA CLAVE)
23. EL CMO SOLICITADO NO ESTÁ EN SU MEMORIA CACHÉ LOCAL
24. SOLICITUD DE CMO A TRAVÉS DE CONEXIÓN SEGURA
25. SITUAR CMO Y CIFRADO CON KCP_PUB
26. RESPUESTA CON EL CMO CIFRADO
27. ALMACENAR EL CMO CIFRADO
28. RESPUESTA CON EL CMO CIFRADO
29. ALMACENAR EL CMO CIFRADO Y VOLVER A CIFRARLO CON K_NUEVA
30. RESPUESTA CON EL CMO DE NUEVO CIFRADO
31. DESCIFRAR EL CMO RECIBIDO

FIG. 3C

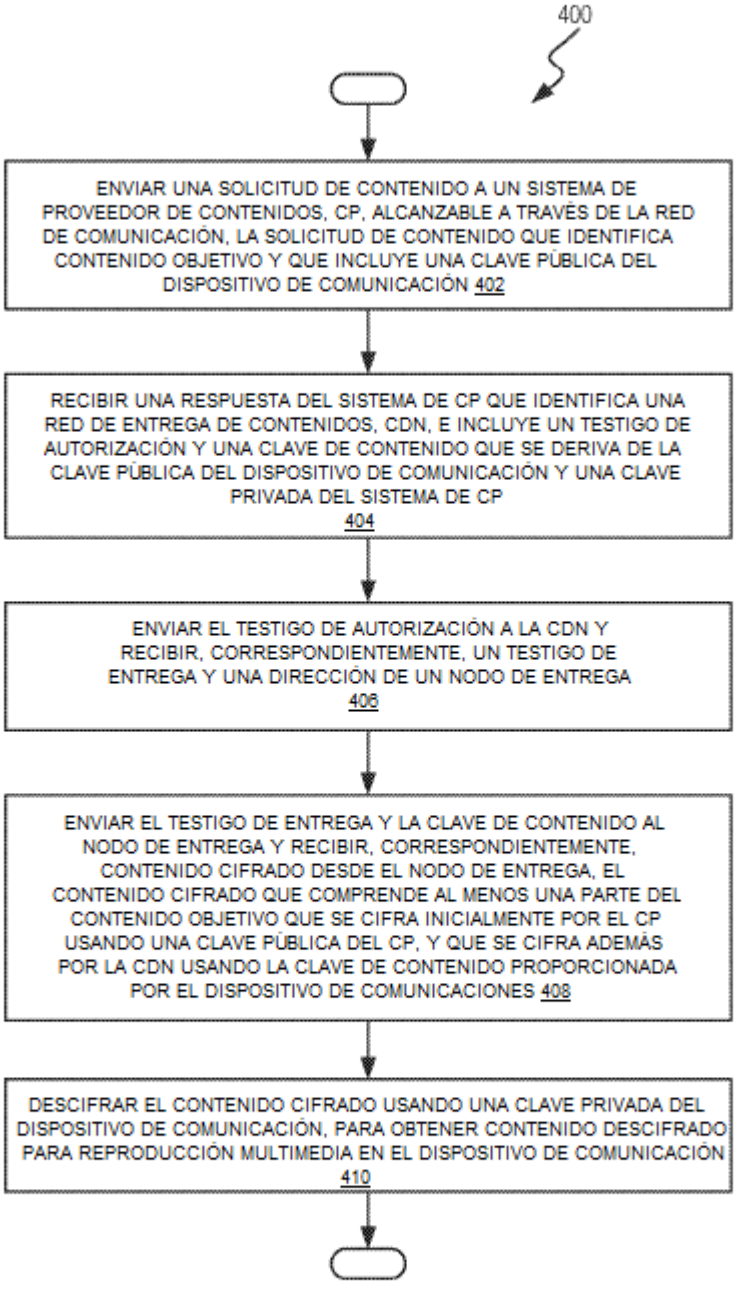
400
ENVIAR UNA SOLICITUD DE CONTENIDO A UN SISTEMA DE PROVEEDOR DE CONTENIDOS, CP, ALCANZABLE A TRAVÉS DE LA RED DE COMUNICACIÓN, LA SOLICITUD DE CONTENIDO QUE IDENTIFICA CONTENIDO OBJETIVO Y QUE INCLUYE UNA CLAVE PÚBLICA DEL DISPOSITIVO DE COMUNICACIÓN 402
RECIBIR UNA RESPUESTA DEL SISTEMA DE CP QUE IDENTIFICA UNA RED DE ENTREGA DE CONTENIDOS, CDN, E INCLUYE UN TESTIGO DE AUTORIZACIÓN Y UNA CLAVE DE CONTENIDO QUE SE DERIVA DE LA CLAVE PÚBLICA DEL DISPOSITIVO DE COMUNICACIÓN Y UNA CLAVE PRIVADA DEL SISTEMA DE CP 404
ENVIAR EL TESTIGO DE AUTORIZACIÓN A LA CDN Y RECIBIR, CORRESPONDIENTEMENTE, UN TESTIGO DE ENTREGA Y UNA DIRECCIÓN DE UN NODO DE ENTREGA 406
ENVIAR EL TESTIGO DE ENTREGA Y LA CLAVE DE CONTENIDO AL NODO DE ENTREGA Y RECIBIR, CORRESPONDIENTEMENTE, CONTENIDO CIFRADO DESDE EL NODO DE ENTREGA, EL CONTENIDO CIFRADO QUE COMPRENDE AL MENOS UNA PARTE DEL CONTENIDO OBJETIVO QUE SE CIFRA INICIALMENTE POR EL CP USANDO UNA CLAVE PÚBLICA DEL CP, Y QUE SE CIFRA ADEMÁS POR LA CDN USANDO LA CLAVE DE CONTENIDO PROPORCIONADA POR EL DISPOSITIVO DE COMUNICACIONES 408
DESCIFRAR EL CONTENIDO CIFRADO USANDO UNA CLAVE PRIVADA DEL DISPOSITIVO DE COMUNICACIÓN, PARA OBTENER CONTENIDO DESCIFRADO PARA REPRODUCCIÓN MULTIMEDIA EN EL DISPOSITIVO DE COMUNICACIÓN 410

FIG. 4

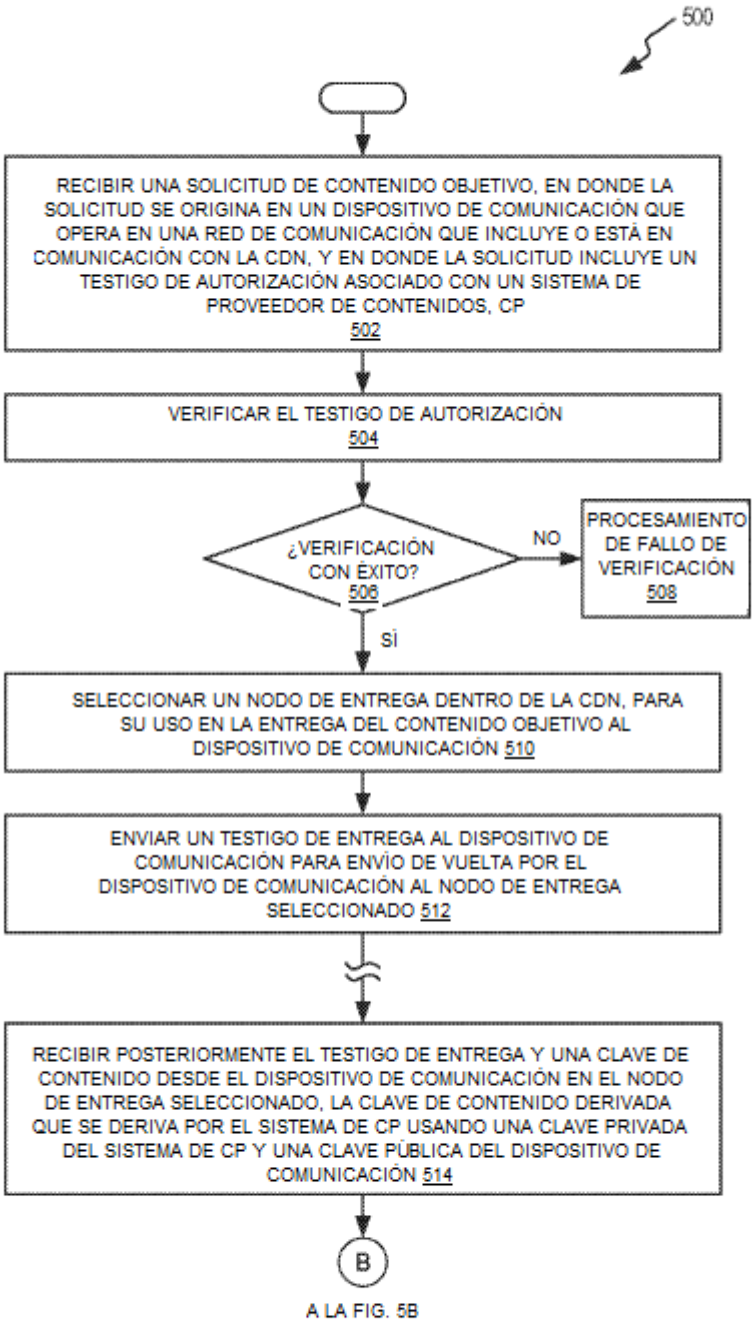
500
RECIBIR UNA SOLICITUD DE CONTENIDO OBJETIVO, EN DONDE LA SOLICITUD SE ORIGINA EN UN DISPOSITIVO DE COMUNICACIÓN QUE OPERA EN UNA RED DE COMUNICACIÓN QUE INCLUYE O ESTÁ EN COMUNICACIÓN CON LA CDN, Y EN DONDE LA SOLICITUD INCLUYE UN TESTIGO DE AUTORIZACIÓN ASOCIADO CON UN SISTEMA DE PROVEEDOR DE CONTENIDOS, CP
502
VERIFICAR EL TESTIGO DE AUTORIZACIÓN
504
¿VERIFICACIÓN CON ÉXITO?
506
NO
PROCESAMIENTO DE FALLO DE VERIFICACIÓN
508
SÍ
SELECCIONAR UN NODO DE ENTREGA DENTRO DE LA CDN, PARA SU USO EN LA ENTREGA DEL CONTENIDO OBJETIVO AL DISPOSITIVO DE COMUNICACIÓN 510
ENVIAR UN TESTIGO DE ENTREGA AL DISPOSITIVO DE COMUNICACIÓN PARA ENVÍO DE VUELTA POR EL DISPOSITIVO DE COMUNICACIÓN AL NODO DE ENTREGA SELECCIONADO 512
RECIBIR POSTERIORMENTE EL TESTIGO DE ENTREGA Y UNA CLAVE DE CONTENIDO DESDE EL DISPOSITIVO DE COMUNICACIÓN EN EL NODO DE ENTREGA SELECCIONADO, LA CLAVE DE CONTENIDO DERIVADA QUE SE DERIVA POR EL SISTEMA DE CP USANDO UNA CLAVE PRIVADA DEL SISTEMA DE CP Y UNA CLAVE PÚBLICA DEL DISPOSITIVO DE COMUNICACIÓN 514
B
A LA FIG. 5B

FIG. 5A

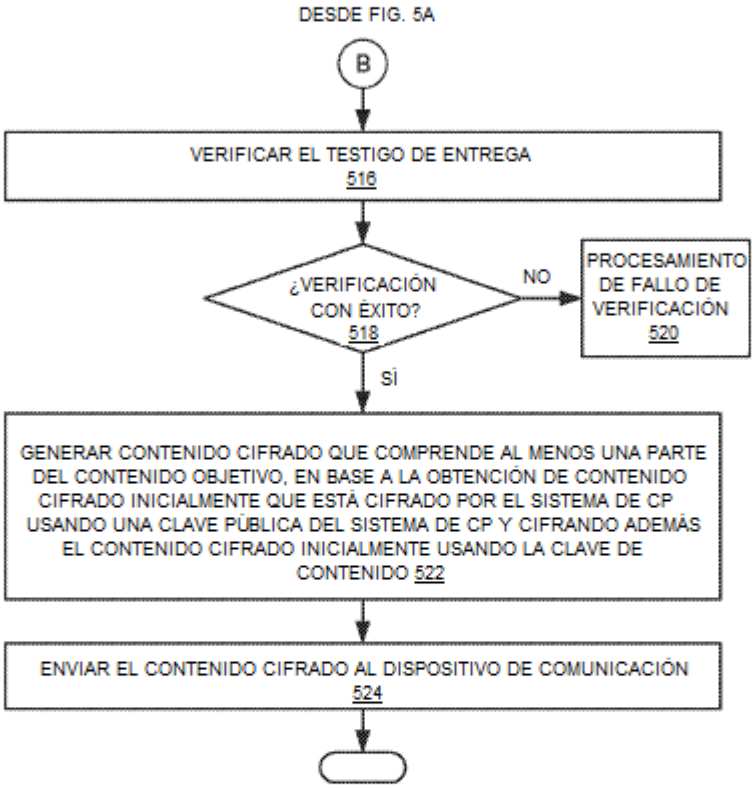
DESDE FIG. 5A
B
VERIFICAR EL TESTIGO DE ENTREGA
516
¿VERIFICACIÓN CON ÉXITO?
518
NO
PROCESAMIENTO DE FALLO DE VERIFICACIÓN
520
SÍ
GENERAR CONTENIDO CIFRADO QUE COMPRENDE AL MENOS UNA PARTE DEL CONTENIDO OBJETIVO, EN BASE A LA OBTENCIÓN DE CONTENIDO CIFRADO INICIALMENTE QUE ESTÁ CIFRADO POR EL SISTEMA DE CP USANDO UNA CLAVE PÚBLICA DEL SISTEMA DE CP Y CIFRANDO ADEMÁS EL CONTENIDO CIFRADO INICIALMENTE USANDO LA CLAVE DE CONTENIDO 522
ENVIAR EL CONTENIDO CIFRADO AL DISPOSITIVO DE COMUNICACIÓN
524

FIG. 5B