(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 645 101**

(51) Int. CI.:

H04W 24/02	(2009.01)	***H04W 16/28***	(2009.01)
H04N 21/442	(2011.01)	***H04W 24/04***	(2009.01)
H04L 12/26	(2006.01)	***H04W 72/00***	(2009.01)
H04L 29/06	(2006.01)	***H04W 76/02***	(2009.01)
H04N 21/643	(2011.01)	***H04W 88/06***	(2009.01)
H04W 28/02	(2009.01)	***H04N 21/2343***	(2011.01)
H04W 40/34	(2009.01)	***H04N 21/258***	(2011.01)
H04W 72/04	(2009.01)	***H03M 13/15***	(2006.01)
H04L 29/08	(2006.01)	***H04N 19/89***	(2014.01)
H04L 5/00	(2006.01)	***H03M 13/19***	(2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.12.2013 PCT/US2013/076837**

(87) Fecha y número de publicación internacional: **24.07.2014 WO14113183**

(96) Fecha de presentación y número de la solicitud europea: **20.12.2013 E 13871935 (6)**

(97) Fecha y número de publicación de la concesión europea: **13.09.2017 EP 2946583**

(54) Título: **Autentificación de URL de contenidos para dash**

(30) Prioridad:

17.01.2013 US 201361753914 P
16.05.2013 US 201361824338 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.12.2017

(73) Titular/es:

INTEL IP CORPORATION (100.0%)
2200 Mission College Boulevard
Santa Clara, CA 95054, US

(72) Inventor/es:

OYMAN, OZGUR

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Autentificación de URL de contenidos para dash.

Aplicaciones relacionadas

Esta solicitud reivindica la prioridad de la solicitud de patente provisional de Estados Unidos con número de serie 61/753,914, presentada el 17 de enero de 2013, con número de expediente del apoderado P53504Z. Esta solicitud reivindica la prioridad de la solicitud de patente provisional de Estados Unidos con número de serie 61/824,338, presentada el 16 de Mayo de 2013, con número de expediente del apoderado P56282Z.

Antecedentes

La tecnología de comunicaciones de móviles inalámbricas utiliza varios estándares y protocolos para transmitir datos entre un nodo (p. ej. una estación de trasmisión) y un dispositivo inalámbrico (p. ej. un dispositivo móvil). Algunos dispositivos inalámbricos se comunican utilizando acceso múltiple por división de frecuencias ortogonales (OFDMA) en una trasmisión de enlace descendente (DL) y acceso múltiple por división de frecuencia de portadora única (SC-FDMA) en una trasmisión de enlace ascendente (UL). Entre los estándares y protocolos que utilizan acceso múltiple por división de frecuencias ortogonales (OFDM) para transmitir señales se incluye la evolución a largo plazo (LTE) del Proyecto Asociación de Tercera Generación (3GPP), el estándar 802.16 (p. ej. 802.16e, 802,16m) del Instituto de Ingeniería Eléctrica y Electrónica (IEEE), que se conoce en la industria bajo el nombre de WiMax (interoperabilidad mundial para acceso por microondas), y el estándar IEEE 802.11, que se conoce en la industria bajo el nombre de WiFi.

En los sistemas LTE de red de acceso radioeléctrica (RAN) en 3GPP, el nodo puede ser una combinación de Nodos B (también conocido como Nodos B evolucionados, Nodos B mejorados, eNodoB, o eNB) de red de acceso de radio terrestre universal evolucionado (E-UTRAN) y controladores de red radioeléctrica (RNC), que se comunica con el dispositivo inalámbrico, que se conoce como el equipo del usuario (UE). La trasmisión de enlace descendente (DL) puede ser una comunicación del nodo (p. ej. eNodeB) al dispositivo inalámbrico (p. ej. UE), y la trasmisión de enlace ascendente (UL) puede ser una comunicación del dispositivo inalámbrico al nodo.

El dispositivo inalámbrico puede utilizarse para recibir entregas multimedia de vídeos de Internet utilizando varios protocolos, tales como la transmisión continua por protocolo de transferencia de hipertexto (HTTP). Uno protocolo que provee transmisión continua de vídeos basada en HTTP es la transmisión continua adaptativa dinámica sobre HTTP (DASH).

Un documento pertinente del estado de la técnica es el "*study of ISO/IEC DIS 23009-4 Segment encryption and authentication*" de estándar internacional publicado el 15 de octubre de 2012.

Breve descripción de los dibujos

Las características y ventajas de la divulgación serán evidentes a partir de la siguiente descripción detallada, tomada en conjunto con los dibujos que la acompañan, que juntos ilustran, a modo de ejemplo, características de la invención; y, en donde:

la FIG. 1 muestra un diagrama de bloque de un cliente y de servidores para la transmisión continua adaptativa dinámica sobre protocolo de transferencia de hipertexto (HTTP) (DASH) según un ejemplo;

la FIG. 2 muestra un diagrama de bloque de una configuración de un fichero de metadatos de descripción de presentación de medios (MPD) según un ejemplo;

la FIG. 3 muestra un ejemplo de un fichero en formato (3GP) del proyecto asociación de tercera generación (3GPP) que utiliza una instanciación del formato de fichero (ISO-BMFF) de la Organización Internacional de Normalización (ISO-base) según un ejemplo;

la FIG. 4 muestra un diagrama de flujo de una autentificación de un localizador uniforme de recursos (URL) de contenidos para transmisión continua adaptativa dinámica sobre protocolo de transferencia de hipertexto (HTTP) (DASH) en un dispositivo de cliente (p. ej. UE) según un ejemplo;

la FIG. 5 (es decir, la Tabla 2) muestra una tabla de sintaxis de lenguaje de marcado extensible (XML-syntax) de grupo común y la representación de atributos y elementos según un ejemplo;

la FIG. 6 representa la funcionalidad de los circuitos del ordenador de un dispositivo cliente (p. ej. UE) operativo para una autentificación de un localizador uniforme de recursos (URL) de contenidos para transmisión continua adaptativa dinámica sobre protocolo de transferencia de hipertexto (HTTP) (DASH) según un ejemplo;

la FIG. 7 muestra un diagrama de flujo de un método para proveer autentificación de un localizador uniforme de recursos (URL) de contenidos para transmisión continua adaptativa dinámica sobre protocolo de transferencia de hipertexto (HTTP) (DASH) en un dispositivo cliente según un ejemplo;

la FIG. 8 muestra un diagrama de un servidor, un nodo (p. ej. eNB), y un equipo de usuario (UE) según un ejemplo; y

la FIG. 9 muestra un diagrama de un dispositivo inalámbrico (p.ej. UE) según un ejemplo.

Se hará referencia ahora a las realizaciones de ejemplo ilustradas, y en la presente memoria se utilizará lenguaje específico para describirlas. De todos modos, se ha de comprender que con ello no se pretende limitar el alcance de la invención.

Descripción detallada

Antes de que se divulgue y describa la presente invención, se ha de comprender que esta invención no está limitada a las estructuras, etapas del proceso, o materiales específicos aquí descritos, sino que se extiende a equivalentes de los mismos, tal y como reconocerán aquellos con experiencia ordinaria en las técnicas pertinentes. También se ha de comprender que la terminología empleada en la presente memoria se utiliza solo con el fin de describir ejemplos particulares y no pretende con ella limitarla. Un mismo número de referencia en diferentes dibujos representa el mismo elemento. Se han provisto los números en los diagramas de flujos y los procesos para ofrecer mayor claridad en la representación de etapas y operaciones, y no suponen necesariamente ningún orden o secuencia particular.

Realizaciones de ejemplo

A continuación se ofrece una visión inicial general de las realizaciones de tecnología y más adelante se describen en mayor detalle realizaciones de tecnología específicas. Este compendio inicial está destinado a ayudar a los lectores a comprender la tecnología con más rapidez, pero no está destinado a identificar características clave o características esenciales de la tecnología, tampoco está destinado a limitar el alcance de la materia reivindicada.

La presente descripción provee un dispositivo cliente según la reivindicación 1 y un método según la reivindicación 10. La transmisión continua (HTTP) por protocolo de transferencia de hipertexto se puede utilizar como una forma de realizar entregas multimedia de vídeos de Internet. En la transmisión continua por HTTP, se puede efectuar la partición de un fichero multimedia en uno o más segmentos para entregarlo a un cliente por medio del protocolo HTTP. Las entregas basadas en HTTP son fiables y fáciles de implementar debido a la amplia adopción de tanto los protocolos de HTTP como los protocolos subyacentes de HTTP, incluido el protocolo de control de transmisión (TCP)/protocolo de internet (IP). Las entregas basadas en HTTP permiten crear servicios de transmisión continua fáciles y cómodos de utilizar ya que evitan la traducción de direcciones de red (NAT) y los problemas ocasionados por cortafuegos. La entrega o la transmisión continua basada en HTTP también permiten utilizar servidores y cachés HTTP estándar en lugar de utilizar servidores de transmisión continua especializados. La entrega basada en HTTP también puede ofrecer escalabilidad debido a la información de estado mínima o reducida del lado del servidor. Microsoft IIS Smooth Streaming, Apple HTTP Live Streaming, y Adobe HTTP Dynamic Streaming son algunos ejemplos de tecnologías de transmisión continua por HTTP.

La transmisión continua adaptativa dinámica por HTTP (DASH) puede ser un protocolo de transmisión continua por HTTP estandarizado. En DASH, un fichero de metadatos de descripción de presentación de medios (MPD) provee información sobre la estructura y las diferentes versiones de las representaciones del contenido de medios almacenada en el servidor, que incluye las diferentes tasas de bits, velocidades de trama, resoluciones, o tipos de códec. Además, DASH también puede especificar formatos de segmentos. El fichero de metadatos de MPD puede contener información sobre la inicialización y los segmentos de medios para un reproductor de medios (p. ej. el reproductor de medios puede comprobar el segmento de inicialización para determinar un formato contenedor y la información de temporización de medios) para asegurar el mapeo de segmentos dentro de una línea temporal de presentación de medios para conmutación y presentación sincrónica con otras representaciones. En base a esta información de metadatos de MPD que describe la relación de los segmentos para formar una presentación de medios, los clientes (o dispositivos de cliente) pueden solicitar los segmentos usando métodos HTTP GET o GET parcial. El cliente puede controlar totalmente la sesión de transmisión continua. Por ejemplo, el cliente puede controlar una solicitud puntual y reproducir con fluidez la secuencia de segmentos, y también puede ajustar potencialmente las tasas de bits u otros atributos (p.ej. para reaccionar a cambios de estado del dispositivo o de las preferencias del usuario). La tecnología DASH también ha sido estandarizada por otras organizaciones como Moving Picture Experts Group (MPEG), Open IPTV Forum (OIPF), y Hybrid Broadcast Broadband TV (HbbTV).

Un cliente DASH puede recibir contenido multimedia descargando los segmentos a través de una serie de transacciones de solicitud-respuesta HTTP. DASH proporciona la capacidad de conmutar de forma dinámica entre distintas representaciones de tasas de bits del contenido de medios a medida que cambia el ancho de banda disponible. De esta manera, DASH permite una adaptación rápida a las condiciones cambiantes de la red y del enlace inalámbrico, las preferencias del usuario y las capacidades del dispositivo, tales como la resolución de visualización, el tipo de unidad central de procesamiento (CPU), o los recursos de memoria disponibles, y demás condiciones.

En DASH, un fichero de metadatos de descripción de presentación de medios (MPD) puede proveer información sobre la estructura y las diferentes versiones de las representaciones del contenido de medios almacenado en un servidor 212 web/de medios, como muestra la FIG 1. Las diferentes versiones de las representaciones del contenido

de medios pueden incluir diferentes tasas de bits, velocidades de trama, resoluciones, tipos de códec, u otros tipos de información similares. Además, DASH también puede especificar los formatos de segmentos, que pueden contener información sobre la inicialización y los segmentos de medios para que un motor de medios pueda asegurar el mapeo de segmentos dentro de una línea temporal de presentación de medios para conmutación y presentación sincrónica con otras representaciones. En base a la información de metadatos de MPD, que describe la relación de los segmentos y cómo los segmentos forman una presentación de medios, un cliente 220 puede solicitar los segmentos usando un mensaje HTTP GET 240 o una serie de mensajes GET parciales. El cliente puede controlar la sesión de transmisión continua, como puede ser una solicitud puntual y una reproducción fluida de una secuencia de segmentos, o puede ajustar potencialmente las tasas de bits u otros atributos para reaccionar a cambios de estado del dispositivo o a una preferencia del usuario.

La FIG. 1 muestra un marco de transmisión continua basada en DASH. Un codificador de medios 214 en el servidor web/de medios 212 puede codificar una entrada de medios 210 a partir de una entrada de datos de audio/vídeo en un formato para almacenamiento o transmisión continua. Se puede utilizar un segmentador de medios 216 para dividir la entrada de medios en una serie de fragmentos o porciones 232, que pueden enviarse a un servidor web 218. El cliente 220 puede solicitar nuevos datos en porciones utilizando mensajes HTTP GET 234 enviados al servidor web (p. ej. un servidor HTTP).

Por ejemplo, un navegador de web 222 del cliente 220 puede solicitar contenido multimedia utilizando un mensaje HTTP GET 240. El servidor web 218 puede proveer al cliente una MPD 242 para el contenido multimedia. Se puede utilizar la MPD para dar el índice de cada segmento y las ubicaciones correspondientes del segmento, como se muestra en la información de metadatos 252 asociada. El navegador de web puede obtener medios del servidor segmento a segmento siguiendo la MPD 242, como se muestra en 236. Por ejemplo, el navegador de web puede solicitar un primer fragmento utilizando un HTTP GET URL (frag. 1 solic.) 244. Se puede utilizar un localizador uniforme de recursos (URL) o localizador universal de recursos para decirle al servidor web qué segmento va a solicitar el cliente 254. El servidor web puede proveer el primer fragmento (p. ej. fragmento 1 246). Para fragmentos subsiguientes, el navegador de web puede solicitar un fragmento i utilizando un HTTP GET URL (solic. frag. i) 248, donde i es un número entero que es un índice del fragmento. En consecuencia, el servidor web puede proveer un fragmento i 250. Se pueden presentar los fragmentos al cliente por medio de un reproductor/descodificador de medios 224.

Tal y como se representa en la FIG. 2, DASH puede especificar diferentes formatos para un fichero de metadatos 402 de descripción de presentación de medios (MPD) que provee información sobre la estructura y las diferentes versiones de las representaciones del contenido de medios almacenados en el servidor, así como de los formatos de segmentos. En DASH, los metadatos 402 de una descripción de presentación de medios (MPD) pueden proveer información sobre la estructura y las diferentes versiones de las representaciones del contenido de medios almacenadas en un servidor web/de medios. En el ejemplo que se ilustra en la FIG. 2, los metadatos MPD se pueden dividir temporalmente en periodos 404 que tienen una duración predeterminado, tales como 60 segundos en este ejemplo. Cada periodo puede incluir una pluralidad de conjuntos de adaptación 406. Cada conjunto de adaptación puede proveer información sobre uno o más componentes de medios con un número de alternativas codificadas. Por ejemplo, el conjunto de adaptación 0 en este ejemplo puede incluir una variedad de alternativas de audio codificadas diferentes, como pueden ser diferentes tasas de bits, sonido mono, estéreo, envolvente, etc. Además de ofrecer distintas calidades de audio para una presentación multimedia durante el periodo ID, el conjunto de adaptación también puede incluir audio en lenguajes distintos. Las diferentes alternativas que se ofrecen en el conjunto de adaptación se denominan representaciones 408.

En la FIG. 2, se muestra cómo el conjunto de adaptación 1 ofrece vídeo a diferentes tasas de bits, como 5 mega-bits por segundos (Mbps), 2 Mbps, 500 kilo-bits por segundo (kbps), o un modo control de reproducción. El modo de control de reproducción se puede utilizar para buscar, avanzar, retroceder o cambiar la ubicación dentro del fichero multimedia de transmisión continua. Además, el vídeo también puede estar disponible en diferentes formatos, tales como vídeos de dos dimensiones (2D) o tres dimensiones (3D), o vídeos en orientación vertical u horizontal. Cada representación 408 puede incluir información de segmento 410. La información de segmento puede incluir información de inicialización 412 y los datos de segmento de medios 414 reales. En este ejemplo, un fichero MPEG-4 (MP4) se envía por transmisión continua de un servidor a un dispositivo móvil. A pesar de que en este ejemplo se utiliza MP4, se puede utilizar una gran variedad de códecs distintos. Un códec es un dispositivo, aplicación, elemento o programa informático capaz de codificar o descodificar una señal o transmisión de datos digitales.

La señal multimedia en el conjunto de adaptación se puede dividir en segmentos aún más pequeños. En el ejemplo de la FIG. 2, el segmento de vídeo de 60 segundos del conjunto de adaptación 1 se divide luego en cuatro sub-segmentos 414 de 15 segundos cada uno. Estos ejemplos no están concebidos para que sean limitantes. La longitud real del conjunto de adaptación y de cada segmento de medios o sub-segmento depende del tipo de medios, los requerimientos del sistema, los posibles tipos de interferencia, etc. Los segmentos o sub-segmentos de medios reales pueden durar desde menos de un segundo a varios minutos.

El estándar DASH puede incluir un marco de autentificación de segmentos que permite utilizar firmas o resúmenes digitales para segmentos tipo DASH para verificar la autenticidad del origen y del contenido. Se pueden proveer las firmas (o resúmenes) para segmentos o sub-segmentos de medios, así como para la inicialización, el índice, y los

segmentos de conmutación de flujo de bits. Tal como se usa en la presente memoria, los términos firma y resumen se pueden utilizar de forma intercambiable para la misma característica o elemento. El marco de autentificación de segmentos puede calcular una firma de un segmento sin codificar, y almacenar el valor externamente. Una interfaz de MPD puede proveer plantillas de URL para obtener las firmas, utilizando HTTP o HTTP seguro (HTTPS). El HTTPS es un protocolo de comunicación para comunicarse de forma segura a través de una red de ordenadores, que es utilizado ampliamente en Internet. El cliente puede obtener la firma, y luego calcular la firma de forma local en un segmento o sub-segmento de medios sin codificar utilizando una clave de validación, y puede rechazar el segmento o sub-segmento de medios en caso de no haber coincidencia entre la firma obtenida y la firma calculada. El dispositivo de cliente no podrá mostrar o reproducir el segmento o sub-segmento de medio que ha sido rechazado.

En un ejemplo, las firmas se pueden calcular con una función hash utilizando claves de autentificación o validación en combinación con el URL del segmento o sub-segmento de medios. Un servidor o una entidad confiable pueden proveer las claves.

La autentificación de segmentos puede ser independiente de un esquema de protección de contenidos, y puede utilizarse en segmentos sin codificar, así como en segmentos codificados que fueron codificados utilizando un sistema de gestión de derechos digitales (DRM). Por ejemplo, se puede utilizar un descriptor de autentificación de contenidos (p. ej. ContentAuthentication) en la MPD para declarar el marco de autentificación y transmitir las firmas de URL. Se pueden utilizar múltiples esquemas de autentificación de contenidos. Por ejemplo, se pueden especificar dos esquemas en el estándar DASH para la autentificación de contenidos, incluido el resumen SHA-256, identificado por el nombre de recurso uniforme (URN) "urn:mpeg:dash:sea:sha256", y la firma HMAC-SHA1, identificada con "urn:mpeg:dash:sea:hmac-sha1". El código de autentificación de mensajes en clave-hash (HMAC) es una construcción específica para calcular un código de autentificación de mensajes (MAC) con una función hash criptográfica en combinación con una clave criptográfica. SHA-1 (o SHA1) es una función hash criptográfica diseñada por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y publicada por el Instituto Nacional de Estándares y Tecnología (NIST) como un Estándar Federal de Procesamiento de la Información de los Estados Unidos. Además, un elemento de resumen de contenido (p. ej. ContentDigest) puede proveer una plantilla para construir un URL, que se puede utilizar también para descargar una firma para un segmento o sub-segmento de medios específico. De manera similar, un elemento de firma de contenido (p. ej. ContentSignature) puede proveer un URL para la adquisición de una clave y una plantilla para construir un URL (o URI), que se puede utilizar también para descargar la firma para un segmento o sub-segmento de medios específico. Un identificador de recurso uniforme (URI) puede incluir un URL o un URN.

El estándar DASH puede definir métodos para autentificar segmentos DASH. Como se detalla en la presente memoria, DASH puede proveer la tecnología (p. ej. servidores, terminales o dispositivos de cliente, equipos de usuario (UE), métodos, circuitos de ordenador, sistemas, mecanismos, procesos o procedimientos) para autentificar los URL en la MPD. Sin autentificación de contenidos URL y si el mapeo del URL de un segmento DASH deseado en la MPD son incorrectos, el usuario puede recibir una transmisión continua de datos inesperada. Los mapeos incorrectos se pueden introducir a través de varios elementos en el sistema de distribución de contenidos utilizado para entregar el contenido de la fuente de contenido al usuario final. Por ejemplo, una situación en la que se introducen mapeos de URL incorrectos se puede dar cuando un distribuidor compila una lista de URL. Un proveedor de contenidos puede proveer generación de contenidos DASH y los servicios de entrega a distribuidores de transmisión continua de contenidos, como pueden ser proveedores de Internet u operadores móviles que proveen acceso a contenidos DASH a usuarios finales. Un acuerdo de nivel de servicios entre un proveedor de contenidos y un distribuidor puede incluir una cláusula en la que el proveedor de contenidos se compromete a dar un nivel específico de precisión de provisión de contenido, así como cláusulas de penalización si no se cumple el nivel específico de precisión. De esta manera, vincular un URL al contenido que representa puede ser beneficioso, lo cual puede garantizar que el contenido deseado se entrega a los usuarios. La tecnología se puede utilizar para validar que el cliente (o usuario) deseado tenga acceso al contenido deseado. Comunicar las claves de validación para autentificar URL por medio de firmas (o resúmenes), lo cual puede ser indicativo de una fuente de contenido, puede permitir al cliente DASH comprobar la validez de las MPD de los URL y garantizar que el contenido se recibe desde la fuente esperada. Utilizar las MPD o segmentos de medios para validar la señal y/o claves de autentificación, firmas, o resúmenes o sus ubicaciones (p. ej. URL) puede ser beneficioso para entregar contenido de forma adecuada.

Otro ejemplo de la capacidad de firma de URL (o autentificación de URL) puede ser para la autentificación de cliente, que se puede utilizar para controlar el acceso a un recurso específico y también para identificar contenido que no está destinado a cierto grupo de usuarios. Los proveedores de servicios y contenidos pueden restringir el acceso a cierto contenido y limitar las visualizaciones de contenido con el fin de proteger derechos de autor y para cumplir con las obligaciones que imponen sus licencias. La autentificación de cliente se puede realizar para controlar el acceso a un recurso específico y también para identificar contenido que no está destinado a ciertos grupos de usuarios. Por ejemplo, las claves de autentificación para ciertos tipos de material restringido, como por ejemplo, material protegido por derechos de autor o contenido de pago, se pueden distribuir solo a usuarios autorizados. En otro ejemplo, se puede proveer la información de clasificación de edades (p. ej. apto para todos los públicos, con supervisión parental, para mayores de 13 años, de 14 o de 18) para ofrecer control parental. En dichas configuraciones, una clave de autentificación específica del cliente se puede entregar a los usuarios deseados, y

solo los usuarios con la clave de autentificación correcta podrán acceder al contenido. Los programas, aplicaciones o dispositivos de reproducción pueden operar con modos específicos que permiten y/o prohíben reproducir contenidos DASH identificados por las claves de autentificación para el contenido.

Una plataforma de servicios puede insertar una clave de autentificación específica de un cliente como un parámetro de un URL de acceso, que luego un servidor de entrega puede comprobar antes de completar la solicitud. El cliente DASH puede insertar varios parámetros de autentificación en una consulta de los URL de segmentos de medios, y así se pueden generar URL específicos para un cliente. En otro ejemplo, las claves de autentificación para generar URL de segmentos de medios a partir de los URL de la MPD se pueden entregar a los clientes DASH a través de la MPD o por medio de otros mecanismos de entrega.

Por ejemplo, las firmas y/o resúmenes de URL se pueden generar para los URL contenidos en el fichero de MPD. En una configuración, la información sobre las firmas se puede comunicar por medio del fichero de MPD. La firma puede estar contenida dentro del fichero de MPD, o los URL que indican estas firmas pueden estar contenidos dentro del fichero de MPD, una lista o plantilla con las reglas de construcción de URL para generar los URL de estas firmas pueden estar contenidas en el fichero de MPD. De esta manera, el fichero de MPD puede incluir una firma, un URL que indica esta firma, una lista de reglas de construcción de URL para generar el URL para la firma, o unas reglas de construcción de URL basadas en una plantilla para generar el URL para la firma.

Por ejemplo, se puede utilizar un descriptor URLAuthentication en la MPD para declarar el marco de autentificación y comunicar las firmas URL. Se pueden definir múltiples esquemas de autentificación de contenidos. Además, un elemento URLDigest puede proveer una plantilla para construir un URL, que se puede utilizar también para descargar la firma de un URL dado. Asimismo, un elemento URLSignature puede proveer un URL para adquirir una clave y una plantilla para construir un URL, que luego se puede utilizar para descargar la firma de un URL dado.

Los diferentes componentes de un URL se pueden autentificar de diferentes maneras. Por ejemplo, se puede incluir un conjunto de firmas para el URL base (p. ej. en la MPD 402 DASH, periodo 404, conjunto de adaptación 406, o nivel de representación 408) para la autentificación del URL base 420, y luego los componentes de URL restantes que apuntan a representaciones y segmentos específicos DASH se pueden firmar (o autentificar) por separado, como se muestra en la FIG. 2. En otro ejemplo, se puede incluir un conjunto de firmas para el atributo @sourceURL en el elemento SegmentBase (p. ej. el segmento base DASH) que puede contener un URL absoluto de un segmento DASH para la autentificación de un segmento base 422 DASH. En otro ejemplo, se puede incluir un conjunto de firmas para el elemento Location que incluye un URL absoluto para la MPD para la autentificación de ubicación 424 de MPD DASH. Autentificar la ubicación de la MPD y del URL base, y comunicar las firmas correspondientes al cliente DASH puede ser beneficioso para validar la fuente de contenido.

Para las listas de reproducción DASH (donde cada segmento DASH se asigna a un URL contenido dentro de la MPD), cada URL específico de una lista de reproducción se puede firmar o autentificar con firmas (p. ej. en el periodo 404 DASH, conjunto de adaptación 406, o nivel de representación 408) para la autentificación de la lista de segmentos 422 DASH. Para las plantillas DASH (donde el cliente DASH genera el URL de cada segmento DASH según una regla predeterminada), cada URL específico de una plantilla se puede firmar o autentificar con firmas (p. ej. en el periodo DASH, conjunto de adaptación, o nivel de representación) para la autentificación de la plantilla de segmentos 422 DASH.

En otra configuración, se puede portar o integrar la información sobre las firmas URL en los segmentos DASH en lugar de la MPD. En un ejemplo, se pueden incluir la firmas a nivel de fichero en un contenedor con formato de fichero de medios base de la Organización Internacional de Normalización (ISO-BMFF) (p. ej. un segmento de inicialización, tal como en un contenedor "moov" 316 para ISO-BMFF, o en segmentos de medios, tal como en un contenedor "moof" para ISO-BMFF, como muestra la FIG. 3). En otra configuración se puede incluir un indicador en la MPD para avisar de la presencia de información integrada en las firmas dentro de los segmentos DASH para que el cliente DASH pueda prepararse para recibir las firmas antes de recibir el segmento.

Por ejemplo, las firmas URL 330 se pueden integrar en un fichero (3GP) con formato de fichero 3GPP (p. ej. en un fichero mp4 314 en un formato de fichero de grupo de expertos en imágenes en movimiento-4 312 (MPEG-4)) con una instanciación de un formato de fichero de medios base de la Organización Internacional de Normalización (ISO-BMFF) 310 como parte de aplicaciones de descarga y transmisión continua, como se representa en la FIG. 3. El fichero de contenido (p. ej. el fichero mp4 314) puede incluir un segmento de inicialización, como un contenedor "moov" 316 y datos de medios (mdat 318). El contenedor moov puede incluir un descriptor de objecto inicial (IOD) 320, una pista de formato binario 322 para la escena (BIFS), una pista de descriptor de objeto (OD), una pista de vídeo 326, y una pista de audio 328. Las firmas 330 integradas en el URL se pueden incluir en el contenedor moov. El mdat puede incluir unidades de acceso (AC) de audio, vídeo, intercaladas, ordenadas temporalmente, BIFS, y OD.

La FIG. 4 muestra un diagrama de flujo de la autentificación de URL de contenidos para un cliente DASH (p. ej. UE). El cliente DASH puede solicitar contenido DASH de un servidor 102, como puede ser un servidor web, un servidor de medios, un servidor de autentificación, un servidor de servicios de transmisión por conmutación de paquetes (PSS) 3GPP LTE, un servidor DASH, o un servidor de sub-sistema multimedia integrado (IMS) basado en PSS y

servicios de transmisión de multimedia y multi-emisión (MBMS) (IMS_PSS_MBMS). El cliente DASH puede recibir una clave de validación 104 de URL del servidor o de una entidad confiable. En otro ejemplo, se puede recibir la clave de validación utilizando el mismo mecanismo de las firmas URL. El cliente DASH puede recibir un fichero de MPD DASH del servidor 106. En una alternativa, el fichero de MPD puede incluir información sobre la firma, que puede incluir las firmas URL, un URL que lleva a la firma de URL, una lista de reglas de construcción de URL para generar el URL para la firma de URL, o unas reglas de construcción de URL basadas en una plantilla para generar el URL para la firma de URL, o un indicador que indique la presencia de información integrada en las firmas URL dentro de los segmentos DASH. El cliente DASH puede obtener las firmas URL a partir de la información de la firma 108 basándose en el tipo de información sobre la firma incluido en el fichero de MPD. En otra alternativa, el cliente DASH puede recibir un segmento DASH del servidor 110. El segmento DASH puede incluir información sobre la firma, que puede incluir las firmas URL, un URL que lleva a la firma de URL, una lista de reglas de construcción de URL para generar el URL para la firma de URL, o unas reglas de construcción de URL basadas en una plantilla para generar el URL para la firma de URL. El cliente DASH puede obtener las firmas URL a partir de la información de la firma 112 basándose en el tipo de información sobre la firma incluido en el segmento DASH. El cliente DASH puede calcular de forma local las firmas URL para la MPD o el contenido 114 DASH utilizando la clave de validación DASH con el URL de contenido. El cálculo de las firmas URL se puede realizar antes o después de obtener la firma de URL del servidor. La firma de URL calculada de forma local se puede comparar con la firma 116 URL obtenida (o recibida). Si las firmas URL no coinciden, se podrá ignorar (o rechazar) el fichero 118 de MPD o el segmento DASH. Si las firmas URL coinciden, se validará el fichero de MPD o el segmento DASH, y el cliente DASH podrá solicitar el segmento DASH autentificado del servidor 120. El cliente DASH podrá recibir el segmento DASH autentificado del servidor 122. Entonces se podrá reproducir (o presentar) 124 el segmento DASH autentificado.

En otro ejemplo, se puede proveer una etiqueta de autenticidad de URL para segmentos URL a través del fichero de MPD, utilizando un elemento UrlAuthenticity que declara el marco de autentificación y comunica la clave de autentificación y las firmas URL. La autentificación URL es opcional si se utiliza un descriptor SupplementaryProperty, y obligatoria si se utiliza con un descriptor EssentialProperty. El valor de @schemeIdUri tanto en EssentialProperty como en SupplementalProperty puede ser "urn:mpeg:dash:sea:urlauth:2013" si se utiliza el marco de autentificación de elemento UrlAuthenticity.

En otra configuración, el elemento UrlAuthenticity se puede implementar en una MPD DASH basada en la especificación técnica 3GPP (TS) 26.247 V11.0.0 (2012-09), o se puede definir como una EssentialProperty o SupplementalProperty basada en el grupo conjunto de la Organización Internacional de Normalización/Comisión Electrotécnica Internacional (IEC) 23009-1:2012, dependiendo de la aplicación. El elemento UrlAuthenticity puede proveer un URL para obtener una clave y una plantilla para construir un URL, que luego se puede utilizar para descargar la etiqueta de autenticidad de un URL de segmento de MPD dado. Por ejemplo, el elemento UrlAuthenticity se puede incluir en la MPD, donde la MPD puede tener atributos y elementos comunes. La semántica del elemento UrlAuthenticity se muestra en la tabla 1. El elemento UrlAuthenticity puede incluir los siguientes atributos: @authSchemeIdUri, @authUrlTemplate, @authTagLength, @keyUrlTemplate, @validityExpires, o @inbandAuthTag. Cada elemento o atributo puede tener un nombre de atributo o elemento, uso o descripción. La columna "uso" en la tabla 1 puede tener un atributo señalado como "M" (obligatorio), "O" (opcional), "OD" (opcional con valor por defecto), o "CM" (obligatorio condicionalmente).

Tabla 1:

Nombre de elemento o atributo	**Uso**	**Descripción**
UrlAuthenticity		Especifica la información necesaria para calcular una etiqueta de autenticidad para un URL de segmento.
@authSchemeIdUri	M	Especifica el algoritmo utilizado para calcular la etiqueta de autenticidad
@authUrlTemplate	M	Especifica la plantilla para crear el URL utilizado para obtener el valor de la etiqueta de autenticidad. Puede estar ausente si @inbandAuthTag es verdadero
@authTagLength	O	Especifica el tamaño de la etiqueta de autenticidad en bits. En caso de estar ausente, el tamaño de la etiqueta es el mismo que en el del algoritmo identificado por @authSchemeIdUri
@keyUrlTemplate	O	Especifica la plantilla para generar el URI de la clave, utilizando sintaxis y sustitución de variables como se define en ISO/IEC

Nombre de elemento o atributo	Uso	Descripción
		23009-1:2012,5.3.9.4.4.
@validityExpires	M	Especifica (en tiempo real) el tiempo cuando expira la autenticidad del URL
@inbandAuthTag	OD	Si es verdadero, la etiqueta de autenticidad aparece dentro de los segmentos asociados (en caso de que se especifique dicho transporte en banda)
Leyenda:		
Para atributos: M=Obligatorio, O=Opcional, OD=Opcional con valor por defecto, CM=Obligatorio condicionalmente		
Para elementos: <minOccurs>...<maxOccurs> (N=ilimitado)		
Los elementos están en **negrita**; los atributos no están en negrita y van precedidos por una @.		

Se puede ver un ejemplo de sintaxis de lenguaje de marcado extensible (XML-syntax) para el elemento de UrlAuthenticity en la tabla 2, que se muestra en la FIG. 5.

Transmitir las claves de validación para autentificar URL por medio de firmas que indican una fuente de contenido permite al cliente DASH comprobar la validez de las MPD de los URL. El cliente DASH también puede recibir las claves de autentificación de contenido específico para varios componentes DASH (p. ej. el periodo 404 DASH, el conjunto de adaptación 406 o la representación 408 (FIG. 2)). Esta transmisión o señal permite al cliente obtener las firmas URL, y luego calcular las firmas URL de forma local en base a los URL en la MPD recibida y en correspondencia con la clave de autentificación, y también rechazar el contenido correspondiente en caso de no haber coincidencia. Se puede indicar dicha validación de información de URL de contenidos (firmas o claves de autentificación) o sus ubicaciones (URL) como parte de la MPD o de los segmentos de medio. El marco o el proceso pueden calcular una firma o un URL de segmento, y almacenar el valor externamente junto con la verificación de la firma y/o las claves de autentificación. La interfaz de MPD puede proveer plantillas de URL para obtener las firmas, utilizando HTTP o HTTPS. El cliente DASH puede obtener las firmas y las claves de autentificación, y luego calcular las firmas de forma local en un URL de segmento dado, y puede rechazar el URL cuando no coinciden.

La autentificación de URL de contenidos DASH puede tener varias aplicaciones (o casos de uso). Cinco casos de uso muestran algunas de las ventajas y beneficios de la autentificación de URL de contenidos DASH. En el primer caso de uso, Alice puede tener una aplicación de cliente compatible con DASH que le permite mirar contenido en formato DASH. Puede tener una suscripción de servicio de transmisión continua para móviles con el operador de telecomunicaciones de mejor cobertura. Puede estar interesada en mirar una película, "*A Dash through the Clouds*", que está disponible en formato DASH. El operador puede restringir el acceso a la película a usuarios autorizados y utilizar mecanismos de autentificación basados en 3GPP para restringir el acceso (p. ej. autentificación de contenido URL). Como puede que Alice ya tenga una suscripción con el servicio de transmisión continua para móviles, se puede autentificar su aplicación de cliente y podrá disfrutar de la película.

En un segundo caso de uso, tanto Alice como Bob pueden tener una aplicación de cliente compatible con DASH que les permite mirar contenido en formato DASH. Ambos pueden tener una suscripción de servicio de transmisión continua para móviles con el operador de telecomunicaciones de mejor cobertura. Bob puede pagar para tener un plan "superior de transmisión continua" mientras que Alice prefiere (y paga) un plan "básico de transmisión continua". Ambos pueden tener interés en mirar la película "*A Dash through the Clouds*". La película está disponible en formato DASH en diferentes tasas de bits y/o resoluciones. Debido la suscripción superior de Bob, la aplicación de cliente de Bob puede tener acceso a transmisión continua y recibirla en varias tasas de bits y/o resoluciones que ofrece el servicio (p. ej. al seleccionar, en cualquier momento, la mejor resolución según el ancho de banda y las capacidades del dispositivo). La aplicación de cliente de Alice puede tener restringido el acceso a las tasas de bits y/o resoluciones más altas debido a su suscripción básica, por lo que la aplicación de cliente de Alice que utiliza autentificación de URL de contenidos solo podrá recibir transmisión continua de un conjunto limitado de las tasas de bits y/o resoluciones disponibles.

En un tercer caso de uso, el operador de telecomunicaciones de mejor cobertura (operador) puede haber invertido mucho dinero recientemente en la infraestructura del operador, y puede estar buscando nuevas oportunidades de negocio para incrementar los ingresos por servicios del operador, concentrándose en la cadena de valor de distribución de contenido a través de Internet (over-the-top, OTT). En particular, el operador puede querer sacar ventaja de sus sistemas de información y equipo de redes (p. ej. subsistema de suscriptores local (HSS)) que puede contener información de usuario valiosa, incluidas claves de autentificación, identidades de usuario, y perfiles de servicio de usuario. Dicha información de usuario permite al operador realizar una serie de funciones de control que incluyen la autentificación de usuario, la autorización de acceso a servicios de un usuario, y la facturación en nombre de proveedores de red de distribución de contenidos (CDN) y de contenido. El operador puede haber firmado un acuerdo de nivel de servicios (SLA) sobre la autentificación y/o seguridad con un proveedor de servicios DASH, MyDASH, para distribuir contenido MyDASH en formato DASH al cumplir con la autentificación y autorización de usuario de parte de MyDASH en la arquitectura de autentificación genérica (GAA) 3GPP del operador. MyDASH puede tener un servicio de suscripción de diferentes niveles e implementar restricciones de acceso a contenido específico para autentificación de cliente utilizando la autentificación de URL de contenido.

En un cuarto caso de uso, el operador de telecomunicaciones de mejor cobertura (opeador) puede haber firmado recientemente un acuerdo de nivel de servicios (SLA) con un proveedor de contenido a través de Internet (OTT) DASH , MyDASH, para distribuir y/o revender contenido en formato DASH de MyDASH. El operador puede planificar utilizar el contenido en formato DASH de MyDASH para ofrecer varios servicios nuevos a sus clientes. El operador puede utilizar la autentificación de URL de contenidos DASH para garantizar la integridad del contenido y de los metadatos asociados para ofrecer una experiencia coherente al usuario. Además de las inversiones que haga el operador en su infraestructura para garantizar la seguridad, el operador también puede utilizar la tecnología descrita en la presente memoria para protegerse de posibles intromisiones durante la entrega de contenido DASH desde MyDASH. El operador puede incluir una cláusula en la que MyDASH se compromete a dar un nivel específico de precisión de provisión de contenido, así como cláusulas de penalización si no se cumple el nivel específico de precisión. Por su parte, MyDASH puede activar mecanismos de autentificación para que el operador pueda validar la integridad del contenido y de la MPD entregados.

En un quinto caso de uso, el operador de telecomunicaciones de mejor cobertura (opeador) puede firmar acuerdos de nivel de servicios (SLA) con varios proveedores de contenidos a través de Internet (OTT) DASH para distribuir y/o revender el contenido en formato DASH de dichos proveedores. El operador puede utilizar dichos contenidos en formato DASH para ofrecer varios servicios nuevos a sus clientes. El operador puede utilizar la autentificación de URL de contenidos DASH para garantizar la integridad del contenido y de los metadatos asociados para ofrecer una experiencia coherente al usuario. En particular, el operador puede ofrecer un servicio de empalme de transmisión continua para crear integración de medios combinando el contenido de varias fuentes. Por ejemplo, puede agregar un anuncio, tanto para vídeo bajo demanda (VOD) y transmisión continua en vivo, que son un ejemplo posible de integración de medios. Dichos esquemas (p. ej. integración de medios) pueden utilizar generación o reescritura de MPD dinámicas, pero dichos esquemas no pueden modificar o eliminar URL de segmentos ni otros metadatos utilizados para la autentificación de URL de contenidos. La modificación inadecuada de MPD y de URL de segmentos u otros metadatos puede ocasionar interrupciones en la reproducción, y en el caso de anuncios que no se hayan reproducido, la modificación inadecuada de MPD y de URL de segmentos u otros metadatos puede resultar en la pérdida de ingresos para los proveedores de contenidos y para el operador.

Otro ejemplo ofrece la funcionalidad 500 de los circuitos del ordenador de un dispositivo de cliente operativo para una autentificación de un localizador uniforme de recursos (URL) de contenidos para transmisión continua adaptativa dinámica por protocolo de transferencia de hipertexto (HTTP) (DASH), como muestra el diagrama de flujo de la FIG. 6. La funcionalidad se puede implementar como un método o se puede ejecutar como instrucciones de una máquina, donde las instrucciones se incluyen en al menos un medio legible por ordenador o un medio de almacenamiento no transitorio legible por ordenador. Los circuitos de ordenador se pueden configurar para obtener un indicador de clave de autentificación de URL y un indicador de firma de URL de contenidos de un servidor, como en el bloque 510. Los circuitos de ordenador también se pueden configurar para generar una firma de URL calculada para una descripción de presentación de medios (MPD) DASH a partir del indicador de clave de autentificación de URL, como en el bloque 520. Los circuitos de ordenador también se pueden configurar para solicitar el segmento DASH cuando la firma de URL calculada coincide con la firma de URL de contenidos recibida, autenticando de esta manera el URL de contenidos, en donde la firma de URL de contenidos recibida se deriva en el servidor a partir del URL de contenidos que está dentro del URL de segmento DASH, como en el bloque 530. Los circuitos de ordenador también se pueden configurar para recibir el segmento DASH utilizando el URL de contenidos autenticado, como en el bloque 540.

En un ejemplo, los circuitos de ordenador configurados para recibir el indicador de clave de autentificación de URL y el indicador de firma de URL de contenidos también se pueden configurar para recibir el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos por medio de un fichero de metadatos de descripción de presentación de medios (MPD). El indicador de clave de autentificación de URL puede incluir una clave de autentificación de URL, o el indicador de firma de URL de contenidos puede incluir una firma de URL de contenidos. En otra configuración, el indicador de clave de autentificación de URL puede incluir un URL de indicador de clave que indica a la clave de autentificación de URL, o el indicador de firma de URL de contenidos puede incluir un URL de indicador de firma que indica a la firma de URL de contenidos. Los circuitos de ordenador también se

pueden configurar para: obtener la clave de autentificación de URL utilizando el URL de indicador de clave; u obtener la firma de URL de contenidos utilizando el URL de indicador de firma.

En otro ejemplo, el indicador de clave de autentificación de URL puede incluir una regla de construcción de URL que provee una plantilla para reconstruir los URL de la clave de autentificación, o el indicador de firma de URL de contenidos puede incluir una regla de construcción de URL que provee una plantilla para reconstruir los URL a partir de las firmas de URL de contenidos. Los circuitos de ordenador también se pueden configurar para: generar los URL de la clave de autentificación utilizando la regla de construcción de URL; o generar los URL de las firmas de URL de contenidos utilizando la regla de construcción de URL. En otra configuración, se puede utilizar un descriptor URL Authenticity para declarar un marco de autentificación por medio del indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos. El descriptor URL Authenticity puede incluir un elemento URL Digest o un elemento URL Signature. Los circuitos de ordenador también se pueden configurar para construir un URL de firma utilizando una plantilla a partir del elemento URL Digest, y para descargar una firma de URL de contenidos a partir del URL de firma. O los circuitos de ordenador también se pueden configurar para: construir un URL de autentificación de clave a partir del elemento URL Signature; descargar una clave de autentificación de URL a partir del URL de autentificación de clave; construir un URL de firma utilizando una plantilla a partir del elemento URL Signature; y descargar una firma de URL de contenidos a partir del URL de firma.

En otro ejemplo, se puede utilizar el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos para autentificar un URL base para una MPD DASH, periodo, conjunto de adaptación, o nivel de representación, o se puede utilizar el indicador de clave de autentificación URL, o el indicador de firma de URL de contenidos para autentificar un URL de segmento de la MPD. En otra configuración, se puede utilizar el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos para autentificar una lista de reproducción DASH, incluida una pluralidad de URL de segmentos DASH. Se puede utilizar el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos para autentificar cada URL específico de una lista de reproducción en la lista de reproducción DASH. En otro ejemplo, se puede utilizar el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos para generar una plantilla DASH para una pluralidad de URL de segmentos DASH. El indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos puede indicar una regla predeterminada para autentificar cada URL específica de una plantilla.

En otra configuración, los circuitos de ordenador se pueden configurar para recibir el indicador de clave de autentificación de URL y el indicador de firma de URL de contenidos también se puede configurar para recibir un fichero metadatos de descripción de presentación de medios (MPD), incluido el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos. El indicador de clave de autentificación de URL puede indicar que la clave de autentificación de URL está integrada en el segmento DASH, o el indicador de firma de URL de contenidos puede indicar que la firma de URL de contenidos está integrada en el segmento DASH. Los circuitos de ordenador configurados para recibir el segmento DASH también se pueden configurar para recibir la clave de autentificación de URL o la firma de URL de contenidos dentro del segmento DASH.

En otro ejemplo, los circuitos de ordenador configurados para recibir el indicador de clave de autentificación de URL y el indicador de firma de URL de contenidos también se pueden configurar para recibir el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos por medio de un contenedor con formato de fichero de medios base de la Organización Internacional de Normalización (ISO-BMFF) en el segmento DASH. El indicador de clave de autentificación de URL puede incluir una clave de autentificación de URL, o el indicador de firma de URL de contenidos puede incluir una firma de URL de contenidos. El segmento DASH puede incluir un segmento de inicialización o un contenedor moov para el ISO-BMFF, o el segmento DASH puede incluir un segmento de medio o un contenedor moof para el ISO-BMFF. El dispositivo de cliente puede incluir un terminal móvil (MT), un equipo de usuario (UE), o una estación móvil (MS). En otro ejemplo, el dispositivo de cliente puede incluir una antena, una cámara, una pantalla táctil, un altavoz, un micrófono, un procesador de gráficos, un procesador de aplicaciones, una memoria interna, o un puerto de memoria no volátil.

Otro ejemplo ofrece el método 600 para ofrecer una autentificación de un localizador uniforme de recursos (URL) de contenidos para transmisión continua adaptativa dinámica por protocolo de transferencia de hipertexto (HTTP) (DASH) en un dispositivo de cliente, como muestra el diagrama de flujo de la FIG. 7. El método se ejecuta como instrucciones en una máquina o circuitos de ordenador, donde las instrucciones se incluyen en al menos un medio legible por ordenador o un medio de almacenamiento no transitorio legible por ordenador. El método incluye la operación de recibir un indicador de clave de validación de URL de un servidor de autentificación, como en el bloque 610. La siguiente operación del método puede ser calcular una firma de URL calculada para una descripción de presentación de medios (MPD) DASH utilizando el indicador de clave de autentificación de URL, como en el bloque 620. El método también puede incluir solicitar el segmento DASH cuando el URL del segmento DASH ha sido validado usando la firma de URL calculada, como en el bloque 630.

En un ejemplo, la operación de recibir el indicador de clave de validación de URL también puede incluir recibir el indicador de clave de validación de URL por medio del fichero de metadatos de descripción de presentación de medios (MPD). En una configuración, el indicador de clave de validación de URL puede incluir una clave de validación de URL o una firma de URL de contenidos. La operación de validar el URL del segmento DASH utilizando la firma de URL calculada también puede incluir comparar una firma de URL de contenidos generada por servidor

con la firma de URL calculada por el dispositivo de cliente. En otra configuración, el indicador de clave de validación de URL puede incluir un URL de indicador de clave que indica a la clave de validación de URL, o un URL de indicador de firma que indica a la firma de URL de contenidos. El método también puede incluir: obtener la clave de validación de URL utilizando el URL de indicador de clave; u obtener la firma de URL de contenidos utilizando el URL de indicador de firma.

En otra configuración, el indicador de clave de validación de URL puede incluir una regla de construcción de URL que provee una plantilla para reconstruir los URL de la clave de autentificación, o una regla de construcción de URL que provee una plantilla para reconstruir los URL para la firma de URL de contenidos. El método también puede incluir: generar los URL de la clave de validación utilizando la regla de construcción de URL; o construir los URL de las firmas de URL de contenidos utilizando la regla de construcción de URL. El indicador de clave de validación de URL se puede utilizar para autentificar un URL de base para una MPD DASH, periodo, conjunto de adaptación, o nivel de representación. O el indicador de clave de validación de URL se puede utilizar para autentificar un URL de segmento de la MPD.

La FIG. 8 muestra un ejemplo de dispositivo de cliente 720 para proveer autentificación de URL de contenidos para DASH, un nodo 710, y un servidor 730 para autentificación de URL de contenidos para DASH. El dispositivo de cliente se puede configurar para la autentificación de URL de contenidos para DASH, como se describe en 500, en la FIG. 6. En otra configuración, el dispositivo de cliente se puede operar para proveer autentificación de URL de contenidos para DASH, como se describe en 600, en la FIG. 7. El dispositivo de cliente 720 puede incluir un procesador 722 y un transceptor 724. En un ejemplo, el dispositivo de cliente puede comunicarse con el servidor a través del nodo. El nodo 710 puede incluir una estación base (BS), un Nodo B (NB), un nodo evolucionado (eNodeB o eNB), una unidad de banda base (BBU), una cabeza de radio remota (RRH), un equipo de radio remoto (RRE), una unidad de radio remota (RRU), o un módulo de procesamiento central (CPM).

Con referencia a la FIG. 8. el servidor 720 puede incluir un procesador y un transceptor. Se puede configurar el procesador para generar una firma de URL de contenidos, un indicador de clave de autentificación de URL, un indicador de firma de URL de contenidos para un URL de segmento DASH. Se puede utilizar el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos para generar una firma de URL calculada para el URL de segmento DASH. El transceptor se puede configurar para: transmitir un indicador de clave de autentificación de URL y un indicador de firma de URL de contenidos; recibir una solicitud de URL del dispositivo de cliente para el segmento DASH; y transmitir un segmento DASH al dispositivo de cliente asociado con la solicitud de URL.

En un ejemplo, el transceptor también se puede configurar para transmitir el indicador de clave de autentificación de URL y el indicador de firma de URL de contenidos a través de un fichero de metadatos de descripción de presentación de medios (MPD). El indicador de clave de autentificación de URL puede incluir una clave de autentificación de URL, o el indicador de firma de URL de contenidos puede incluir una firma de URL de contenidos. En otro ejemplo, el indicador de clave de autentificación de URL puede incluir un URL de indicador de clave que indica a la clave de autentificación de URL, o el indicador de firma de URL de contenidos puede incluir un URL de indicador de firma que indica a la firma de URL de contenidos. El transceptor también se puede configurar para: transmitir la clave de autentificación de URL cuando se recibe el URL de indicador de clave; o transmitir la firma de URL de contenidos cuando se recibe el URL de indicador de firma.

En otra configuración, el indicador de clave de autentificación de URL puede incluir una regla de construcción de URL que puede proveer una plantilla para construir los URL de clave de autentificación. O el indicador de firma de URL de contenidos puede incluir una regla de construcción de URL que puede proveer una plantilla para construir los URL para las firmas de URL de contenidos. En otro ejemplo, el indicador de clave de autentificación del URL o el indicador de firma de URL de contenidos se pueden utilizar para autentificar un URL de base para una MPD DASH, periodo, conjunto de adaptación, o nivel de representación. O se puede utilizar el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos para autentificar un URL de segmento de la MPD.

En otra configuración, el transceptor también se puede configurar para recibir la firma de URL calculada del dispositivo de cliente. El procesador también se puede configurar para validar el dispositivo de cliente con la firma de URL calculada. El servidor puede incluir un servidor web, un servidor de medios, un servidor de autentificación, un servidor de servicios de transmisión por conmutación de paquetes (PSS) de evolución de largo plazo (LTE) del Proyecto Asociación de Tercera Generación (3GPP), un servidor para transmisión continua adaptativa dinámica por protocolo de transferencia de hipertexto (HTTP) (DASH), o un servidor de subsistema multimedia integrado (IMS) basado en PSS y servicios de transmisión de multimedia y multi-emisión (MBMS) (IMS_PSS_MBMS).

La FIG. 9 muestra una ilustración de ejemplo del dispositivo de cliente, como puede ser un terminal móvil (MT), un nodo móvil, un equipo de usuario (UE), una estación móvil (EM); un dispositivo móvil inalámbrico, un dispositivo de comunicación móvil, una tableta, un terminal, u otro tipo de dispositivo móvil inalámbrico. El dispositivo inalámbrico puede incluir una o más antenas configuradas para comunicarse con un nodo, un macro nodo, un nodo de baja potencia (LPN), o una estación de transmisión, como puede ser una estación base (BS), un nodo B evolucionado (eNB), una unidad de banda base (BBU), una cabeza de radio remota (RRH), un equipo de radio remoto (RRE), una

estación repetidora (RS), un equipo de radio (RE), una unidad de radio remota (RRU), o un módulo de procesamiento central (CPM), u otro tipo de punto de acceso de redes inalámbricas de área amplia (WWAN). El dispositivo inalámbrico puede estar configurado para comunicarse utilizando al menos un estándar de comunicación inalámbrica que incluye 3GPP LTE, WiMAX, acceso de alta velocidad por paquetes (HSPA), Bluetooth, y WiFi. El dispositivo inalámbrico puede comunicarse utilizando antenas separadas para cada estándar de comunicación inalámbrica o antenas compartidas para múltiples estándares de comunicación inalámbrica. El dispositivo inalámbrico puede comunicarse en una red de área local inalámbrica (WLAN), una red de área personal inalámbrica (WPAN) y/o una WWAN.

La FIG. 9 también muestra una ilustración de un micrófono y uno o más altavoces que se pueden utilizar para entrada y salida de audio del dispositivo inalámbrico. La pantalla de visualización puede ser una pantalla de cristal líquido (LCD), u otro tipo de pantalla de visualización, tal y como una pantalla de diodo orgánico emisor de luz (OLED). La pantalla de visualización puede estar configurada como una pantalla táctil. La pantalla táctil puede utilizar una tecnología capacitiva, resistiva o cualquier otro tipo de tecnología de pantalla táctil. Se puede acoplar un procesador de aplicación y un procesador de gráficos a una memoria interna para ofrecer capacidades de procesamiento y visualización. También se puede utilizar un puerto de memoria no volátil para ofrecer opciones de entrada/salida de datos a un usuario. Un puerto de memoria no volátil también se puede utilizar para expandir las capacidades de memoria del dispositivo inalámbrico. Un teclado puede estar integrado al dispositivo inalámbrico o conectado de forma inalámbrica al dispositivo inalámbrico para ofrecer una entrada adicional al usuario. También se puede proveer un teclado virtual utilizando la pantalla táctil.

Diversas técnicas, o determinados aspectos de porciones de las mismas, pueden tener la forma de código de programa (es decir, instrucciones) realizadas en medios tangibles, tal y como disquetes, memoria de solo lectura en disco compacto (CD-ROM), discos duros, medios de almacenamiento no transitorios legibles por ordenador, o cualquier otro tipo de medio de almacenamiento legible por ordenador en donde, cuando el código de programa se carga y ejecuta en una máquina, tal y como un ordenador, la máquina se convierte en un aparato para poner en práctica las diversas técnicas. Los circuitos pueden incluir hardware, firmware, código de programa, código ejecutable, instrucciones para el ordenador, y/o software. Un medio de almacenamiento no transitorio legible por ordenador puede incluir un medio de almacenamiento legible por ordenador que no incluya señal. En el caso de la ejecución de código de programa en ordenadores programables, el dispositivo informático puede incluir un procesador, un medio de almacenamiento legible por el ordenador (que incluye memoria volátil y no volátil y/o elementos de almacenamiento), al menos un dispositivo de entrada, y al menos un dispositivo de salida. La memoria volátil y no volátil y/o elementos de almacenamiento pueden ser una memoria de acceso aleatorio (RAM), memoria programable y borrable de solo lectura (EPROM), memoria flash, memoria óptica, disco duro magnético, unidad de estado sólido, u otro medio de almacenamiento de datos electrónicos. El nodo y el dispositivo inalámbrico también pueden incluir un módulo transceptor (es decir, un transceptor), un módulo contador (es decir, un contador), un módulo procesador (es decir, un procesador), y/o un módulo reloj (es decir, un reloj) o módulo temporizador (es decir, un temporizador). Uno o más programas que puedan implementar o utilizar las diversas técnicas descritas en la presente memoria pueden utilizar una interfaz de programación de aplicaciones (API), controles reutilizables, y elementos similares. Dichos programas pueden implementarse en un lenguaje de programación de alto nivel de procedimiento u orientado al objeto para comunicarse con un sistema informático. Sin embargo, el/los programa/s pueden implementarse en un lenguaje de ensamblaje o de máquina, si se desease. En cualquier caso, el lenguaje puede ser un lenguaje compilado o interpretado, y combinado con implementaciones de hardware.

Se ha de comprender que muchas de las unidades funcionales descritas en esta especificación han sido etiquetadas como módulos, para poder enfatizar más específicamente su independencia de implementación. Por ejemplo, se puede implementar un módulo como un circuito de hardware que comprende circuitos integrados a escala muy grande (VLSI) o disposiciones de puerto personalizados, semiconductores disponibles en comercios, tal y como chips lógicos, transistores, u otros componentes discretos. También se puede implementar un módulo en dispositivos de hardware programables, tal y como disposición de puertos programables de campo, lógica de disposición programable, dispositivos de lógica programable o similares.

También se pueden implementar módulos en software para que diversos tipos de procesadores los ejecuten. Un módulo identificado de código ejecutable puede, por ejemplo, comprender uno o más bloques físicos o lógicos de instrucciones de ordenador, que pueden, por ejemplo, estar organizadas como un objeto, procedimiento o función. Sin embargo, los ejecutables de un módulo identificado no necesitan estar ubicados juntos físicamente, pero pueden comprender instrucciones dispares almacenadas en diferentes ubicaciones que, cuando se juntan de forma lógica, comprenden el módulo y logran el propósito establecido para el módulo.

De hecho, el módulo de código ejecutable puede ser una única instrucción, o muchas instrucciones, y puede incluso estar distribuida entre varios segmentos de código diferentes, entre diferentes programas, y a lo largo de diversos dispositivos de memoria. De manera similar, los datos operacionales se pueden identificar e ilustrar en la presente memoria dentro de módulos, y pueden estar realizados de cualquier forma apropiada y organizados dentro de cualquier tipo de estructura de datos apropiada. Los datos operacionales se pueden recolectar como un único conjunto de datos, o pueden estar distribuidos a lo largo de diferentes ubicaciones, que incluyen diferentes dispositivos de almacenamiento, y pueden existir, al menos parcialmente, simplemente como señales electrónicas

en un sistema o red. Los módulos pueden ser pasivos o activos, incluyendo los agentes capaces de operar para realizar determinadas funciones.

A lo largo de esta especificación se hace referencia a "un ejemplo" o "ejemplar" con el significado de que un detalle, estructura o característica específica descrita en conexión con el ejemplo está incluida en al menos una realización de la presente invención. Por lo tanto, las apariciones de las frases "en un ejemplo" o la palabra "ejemplar" en diversos lugares a lo largo de esta especificación no necesariamente se refieren siempre a la misma realización.

Tal y como se utiliza aquí, una pluralidad de elementos, elementos estructurales, elementos composicionales, y/o materiales se pueden presentar en una lista común para mayor conveniencia. Sin embargo, estas listas han de ser interpretadas como si cada miembro de esta lista estuviese identificado individualmente como un miembro separado y único. Por lo tanto, ningún miembro individual de dicha lista ha de ser interpretado como el equivalente de facto de cualquier otro miembro de la misma lista simplemente por estar incluido en un grupo común sin ninguna indicación que diga lo contrario. Además, en la presente memoria se hace referencia a diversas realizaciones y ejemplos de la presente invención junto con alternativas para los diversos componentes de los mismos. Se ha de comprender que dichas realizaciones, ejemplos y alternativas no han de ser interpretadas como equivalentes de facto entre sí, sino que han de ser consideradas como representaciones separadas y autónomas de la presente invención.

Además, los detalles, estructuras, o características descritas pueden combinarse de cualquier manera apropiada en una o más realizaciones. En la descripción anterior, se ofrecen numerosos detalles específicos, tales como ejemplos de diseños, distancias, ejemplos de redes, etc., para ofrecer una comprensión pormenorizada de las realizaciones de la invención. Un experto en la técnica pertinente reconocerá, sin embargo, que la invención puede llevarse a la práctica sin uno o más de los detalles específicos, o con otros métodos, componentes, diseños, etc. En otras instancias, no se muestran o describen en detalle estructuras, materiales u operaciones bien conocidas para evitar confundir aspectos de la invención.

A pesar de que los ejemplos anteriores son ilustrativos de los principios de la presente invención en una o más aplicaciones específicas, será evidente para aquellos con experiencia ordinaria en la técnica que se pueden realizar numerosas modificaciones en cuanto a forma, uso y detalles de implementación sin ejercitar facultades inventivas, y sin alejarse de los principios y conceptos de la invención. En consecuencia, no se pretende limitar la invención, excepto por las reivindicaciones que se detallan a continuación.

REIVINDICACIONES

1. Un dispositivo de cliente (220) operativo de autentificación de un localizador uniforme de recursos de contenidos, URL, para transmisión continua adaptativa dinámica por protocolo de transferencia de hipertexto, HTTP, DASH, con circuitos de ordenador configurados para:

obtener un indicador de clave de autentificación de URL y un indicador de firma de URL de contenidos de un servidor;

generar una firma de URL calculada para una descripción de presentación de medios, MPD, (242) a partir del indicador de clave de autentificación de URL;

solicitar el segmento DASH cuando la firma de URL calculada coincide con la firma de URL de contenidos recibida, autenticando de esta manera el URL de contenidos, en donde la firma de URL de contenidos recibida se deriva en el servidor a partir del URL de contenidos que está dentro del URL de segmento DASH; y

recibir el segmento DASH utilizando el URL de contenidos autenticado.

2. El dispositivo de cliente (220) de la reivindicación 1, en el que los circuitos de ordenador configurados para recibir el indicador de clave de autentificación de URL y el indicador de firma de URL de contenidos también están configurados para:

recibir el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos por medio de un fichero de metadatos (242) de descripción de presentación de medios, MPD.

3. El dispositivo de cliente (220) de la reivindicación 1, en el que el indicador de clave de autentificación de URL incluye una clave de autentificación de URL, o el indicador de firma de URL de contenidos incluye una firma de URL de contenidos.

4. El dispositivo de cliente (220) de la reivindicación 1, en el que se utiliza un descriptor URL Authenticity para declarar un marco de autentificación por medio del indicador de clave de autentificación de URL, en el que el descriptor URL Authenticity incluye un elemento URL Digest o un elemento URL Signature, en donde los circuitos de ordenador también están configurados para:

construir un URL de firma utilizando una plantilla a partir del elemento URL Digest, y descargar una firma de URL de contenidos a partir del URL de firma; o

construir un URL de clave de autentificación a partir del elemento URL Signature, descargar una clave de autentificación de URL a partir del URL de clave de autentificación,

construir un URL de firma utilizando una plantilla a partir del elemento URL Signature; y descargar una firma de URL de contenidos a partir del URL de firma.

5. El dispositivo de cliente (220) según una de las reivindicaciones 1 a 4, en el que se utiliza el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos para autentificar un URL base para una MPD DASH, periodo, conjunto de adaptación, o nivel de representación, o se utiliza el indicador de clave de autentificación URL, o el indicador de firma de URL de contenidos para autentificar un URL de segmento de la MPD.

6. El dispositivo de cliente (220) según una de las reivindicaciones 1 a 5, en el que se utiliza el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos para autentificar una lista de reproducción DASH, incluida una pluralidad de URL de segmentos DASH, en el que se utiliza el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos para autentificar cada URL específico de una lista de reproducción en la lista de reproducción DASH.

7. El dispositivo de cliente (220) según una de las reivindicaciones 1 a 5, en el que se utiliza el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos para generar una plantilla DASH para una pluralidad de URL de segmentos DASH, en el que el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos indican una regla predeterminada para autentificar cada URL específico de una plantilla.

8. El dispositivo de cliente (220) según una de las reivindicaciones 1 a 7, en el que los circuitos de ordenador configurados para recibir el indicador de clave de autentificación de URL y el indicador de firma de URL de contenidos también se pueden configurar para: recibir el indicador de clave de autentificación de URL o el indicador de firma de URL de contenidos por medio de un contenedor con formato de fichero de medios base de la Organización Internacional de Normalización (ISO-BMFF) en el segmento DASH; en el que el indicador de clave de autentificación de URL incluye una clave de autentificación de URL, o el indicador de firma de URL de contenidos incluye una firma de URL de contenidos, en el que el segmento DASH incluye un segmento de inicialización o un

contenedor moov para el ISO-BMFF, o el segmento DASH incluye un segmento de medio o un contenedor moof para el ISO-BMFF.

9. El dispositivo de cliente (220) según una de las reivindicaciones 1 a 7, en el que el dispositivo de cliente incluye un terminal móvil (MT), un equipo de usuario (UE), o una estación móvil (MS); y el dispositivo de cliente incluye una antena, una cámara, una pantalla táctil, un altavoz, un micrófono, un procesador de gráficos, un procesador de aplicaciones, una memoria interna, o un puerto de memoria no volátil.

10. Un método para proveer autentificación de un localizador uniforme de recursos de contenidos, URL, para transmisión continua adaptativa dinámica por protocolo de transferencia de hipertexto, HTTP, DASH, en un dispositivo de cliente (220), que comprende:

recibir un indicador de clave de autentificación de URL y una firma de URL de contenidos de un servidor (218);

calcular una firma de URL calculada para una descripción de presentación de medios, MPD, (242) utilizando el indicador de clave de autentificación de URL; y

solicitar el segmento DASH cuando la firma de URL calculada coincide con la firma de URL de contenidos recibida; y

recibir un segmento DASH utilizando el URL de contenidos autentificado.

11. El método de la reivindicación 10, en el que recibir el indicador de clave de validación de URL también comprende:

recibir el indicador de clave de validación de URL por medio del fichero de metadatos de descripción de presentación de medios (MPD).

12. El método de la reivindicación 10, en el que el indicador de clave de autentificación de URL incluye un URL de indicador de clave que indica a la clave de autentificación de URL, o un URL de indicador de firma que indica a la firma de URL de contenidos, y que además comprende:

obtener la clave de autentificación de URL utilizando el URL de indicador de clave; u

obtener la firma de URL de contenidos utilizando el URL de indicador de firma.

13. El método de la reivindicación 10, en el que el indicador de clave de autentificación de URL incluye una regla de construcción de URL que provee una plantilla para construir los URL de clave de autentificación, o una regla de construcción de URL que provee una plantilla para construir los URL para la firma de URL de contenidos, y que además comprende:

construir los URL de clave de autentificación utilizando la regla de construcción de URL; o

construir los URL de firmas de URL de contenidos utilizando la regla de construcción de URL.

14. Un programa de ordenador que comprende un código de programa de ordenador adaptado para ejecutar el método según una de las reivindicaciones 10 a 13.

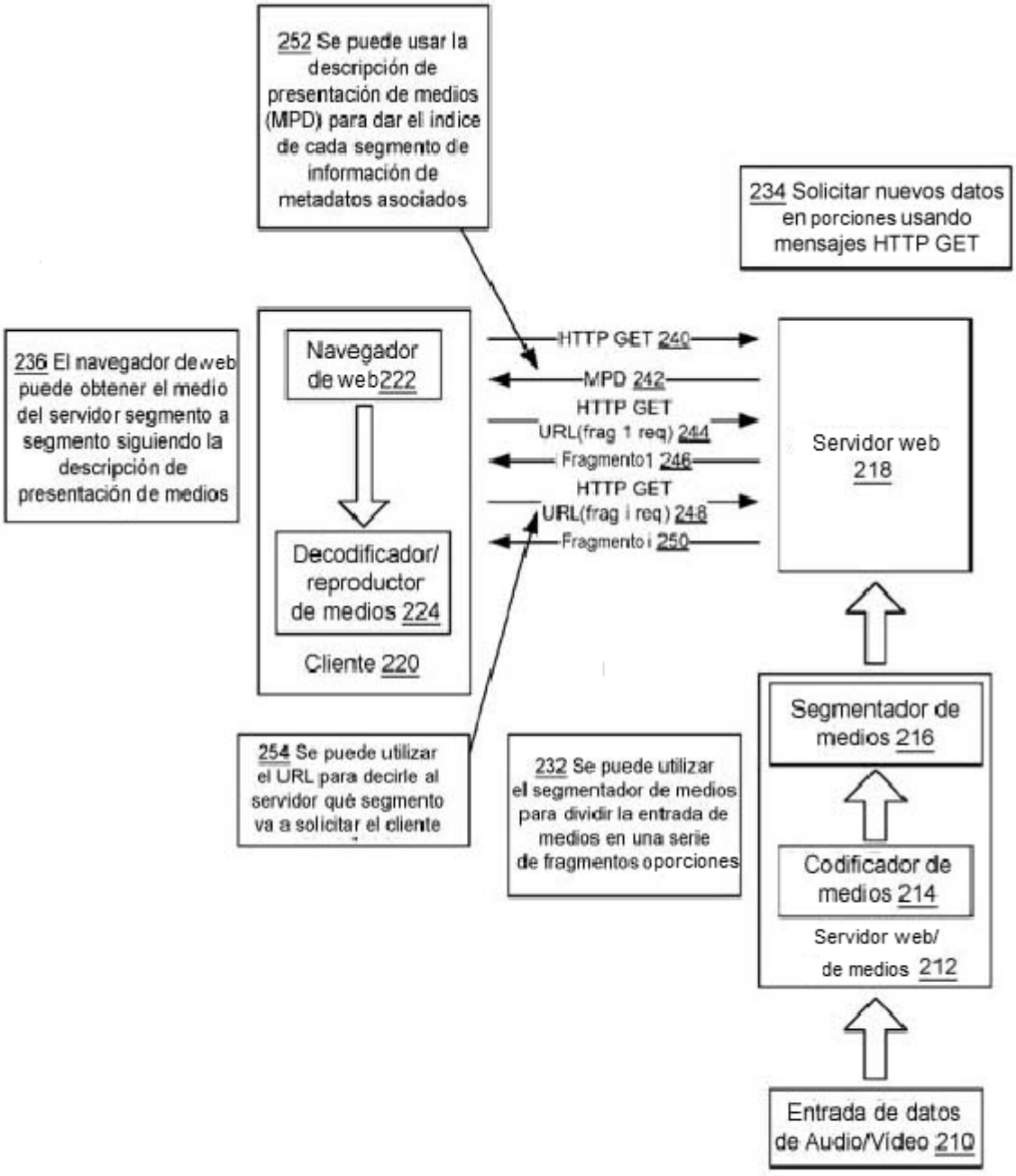
252 Se puede usar la descripción de presentación de medios (MPD) para dar el índice de cada segmento de información de metadatos asociados
234 Solicitar nuevos datos en porciones usando mensajes HTTP GET
236 El navegador de web puede obtener el medio del servidor segmento a segmento siguiendo la descripción de presentación de medios
Navegador de web 222
Decodificador/ reproductor de medios 224
Cliente 220
HTTP GET 240
MPD 242
HTTP GET URL(frag 1 req) 244
Fragmento1 246
HTTP GET URL(frag i req) 248
Fragmento i 250
Servidor web 218
254 Se puede utilizar el URL para decirle al servidor qué segmento va a solicitar el cliente
232 Se puede utilizar el segmentador de medios para dividir la entrada de medios en una serie de fragmentos o porciones
Segmentador de medios 216
Codificador de medios 214
Servidor web/ de medios 212
Entrada de datos de Audio/Vídeo 210

FIG. 1

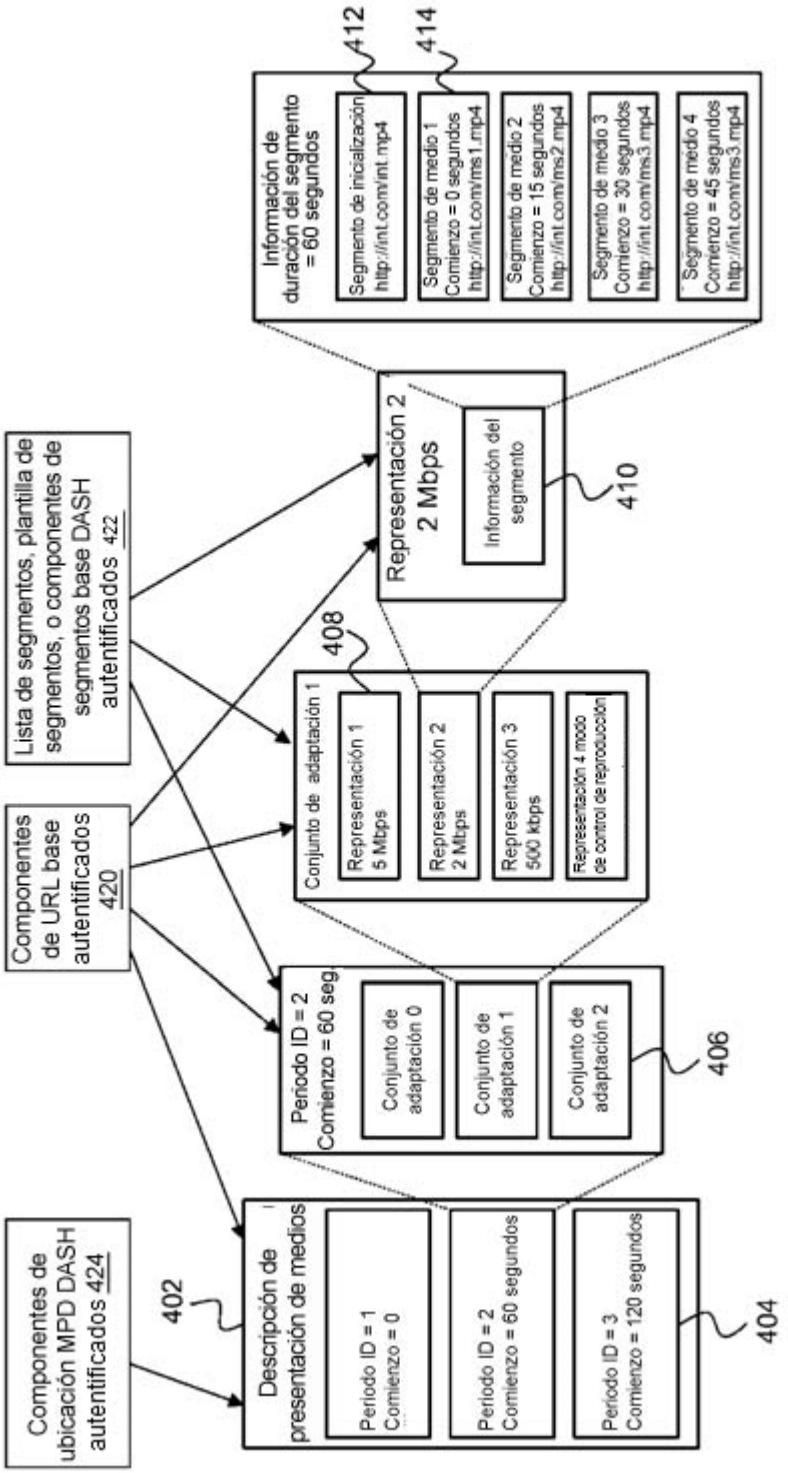
Componentes de ubicación MPD DASH autentificados 424
402
Descripción de presentación de medios
Periodo ID = 1 Comienzo = 0
Periodo ID = 2 Comienzo = 60 segundos
Periodo ID = 3 Comienzo = 120 segundos
404
Componentes de URL base autentificados 420
Lista de segmentos, plantilla de segmentos, o componentes de segmentos base DASH autentificados 422
Periodo ID = 2 Comienzo = 60 seg
Conjunto de adaptación 0
Conjunto de adaptación 1
Conjunto de adaptación 2
406
Conjunto de adaptación 1
Representación 1 5 Mbps
Representación 2 2 Mbps
Representación 3 500 kbps
Representación 4 modo de control de reproducción
408
Representación 2 2 Mbps
Información del segmento
410
Información de duración del segmento = 60 segundos
Segmento de inicialización http://int.com/mt.mp4
Segmento de medio 1 Comienzo = 0 segundos http://int.com/ms1.mp4
Segmento de medio 2 Comienzo = 15 segundos http://int.com/ms2.mp4
Segmento de medio 3 Comienzo = 30 segundos http://int.com/ms3.mp4
Segmento de medio 4 Comienzo = 45 segundos http://int.com/ms3.mp4
412
414

FIG. 2

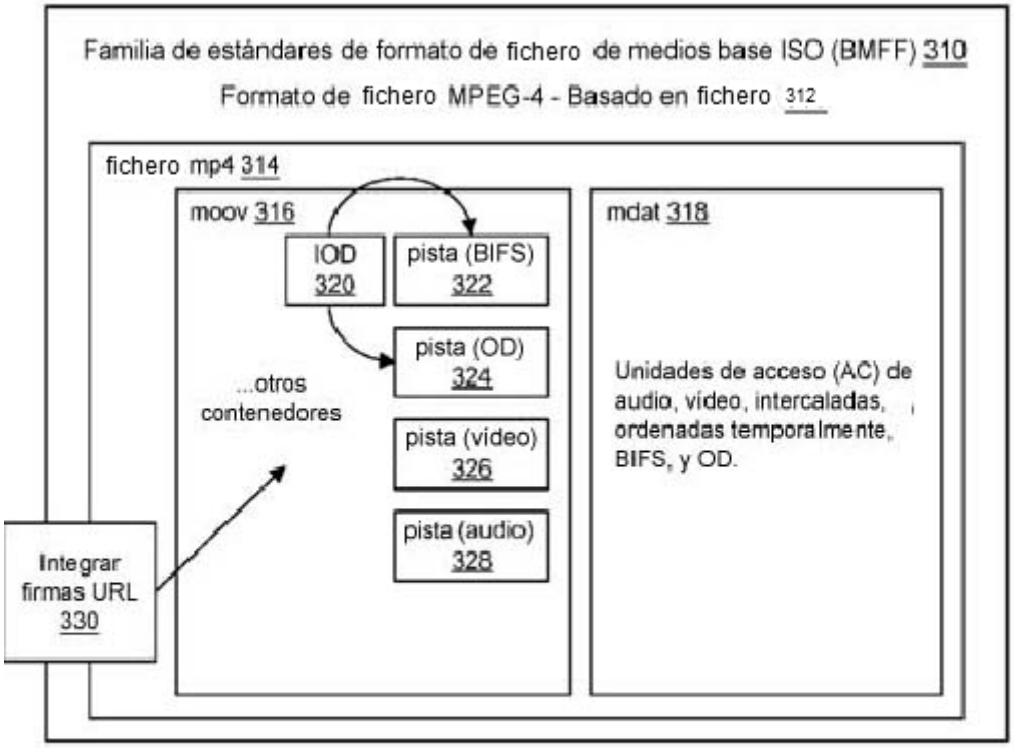
Familia de estándares de formato de fichero de medios base ISO (BMFF) 310
Formato de fichero MPEG-4 - Basado en fichero 312
fichero mp4 314
moov 316
IOD 320
pista (BIFS) 322
pista (OD) 324
...otros contenedores
pista (video) 326
pista (audio) 328
mdat 318
Unidades de acceso (AC) de audio, vídeo, intercaladas, ordenadas temporalmente, BIFS, y OD.
Integrar firmas URL 330

FIG. 3

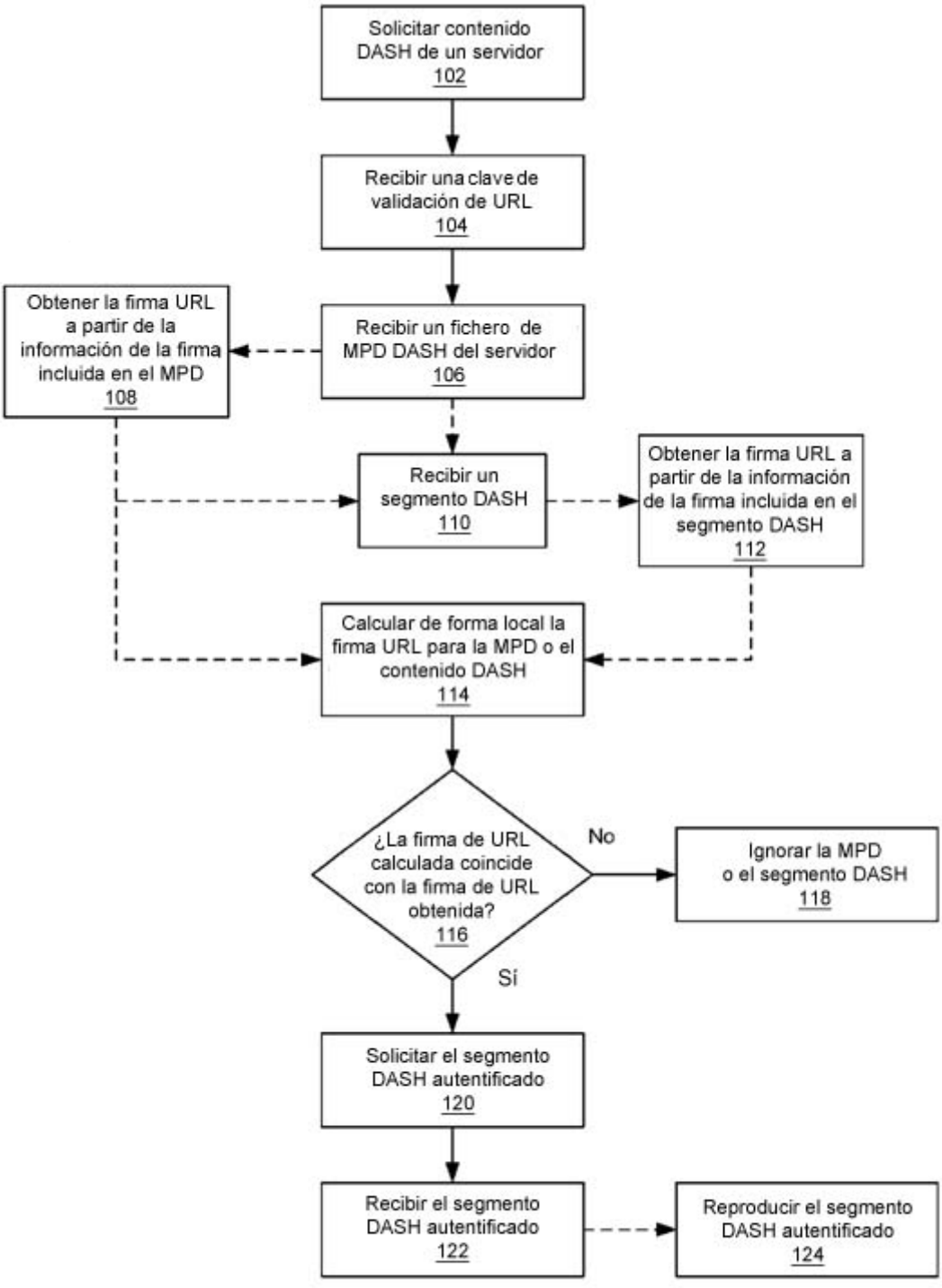
Solicitar contenido DASH de un servidor 102
Recibir una clave de validación de URL 104
Recibir un fichero de MPD DASH del servidor 106
Obtener la firma URL a partir de la información de la firma incluida en el MPD 108
Recibir un segmento DASH 110
Obtener la firma URL a partir de la información de la firma incluida en el segmento DASH 112
Calcular de forma local la firma URL para la MPD o el contenido DASH 114
¿La firma de URL calculada coincide con la firma de URL obtenida? 116
No
Ignorar la MPD o el segmento DASH 118
Sí
Solicitar el segmento DASH autentificado 120
Recibir el segmento DASH autentificado 122
Reproducir el segmento DASH autentificado 124

FIG. 4

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:mpeg:dash:schema:sea:2013"
  attributeFormDefault="unqualified"
  elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:mpeg:dash:schema:sea:2013" xmlns:dash="urn:mpeg:dash:schema:mpd:2011">

  <!—URL Authenticity signaling -->

  <xs:complexType name="URLAuthenticity">
    <xs:attribute name="keyUriTemplate" type="xs:anyURI" use="required"/>
    <xs:attribute name="authSchemeIdUri" type="xs:anyURI" use="required"/>
    <xs:attribute name="authUrlTemplate" type="xs:anyURI" use="required"/>
    <xs:attribute name="authTagLength" type="xs:unsignedInt"/>
    <xs:attribute name="validityExpires" type="xs:dateTime" use="required"/>
    <xs:attribute name="inbandAuthTag" type="xs:boolean"/>
  </xs:complexType>
</xs:schema>
```

FIG. 5
(Tabla 2)

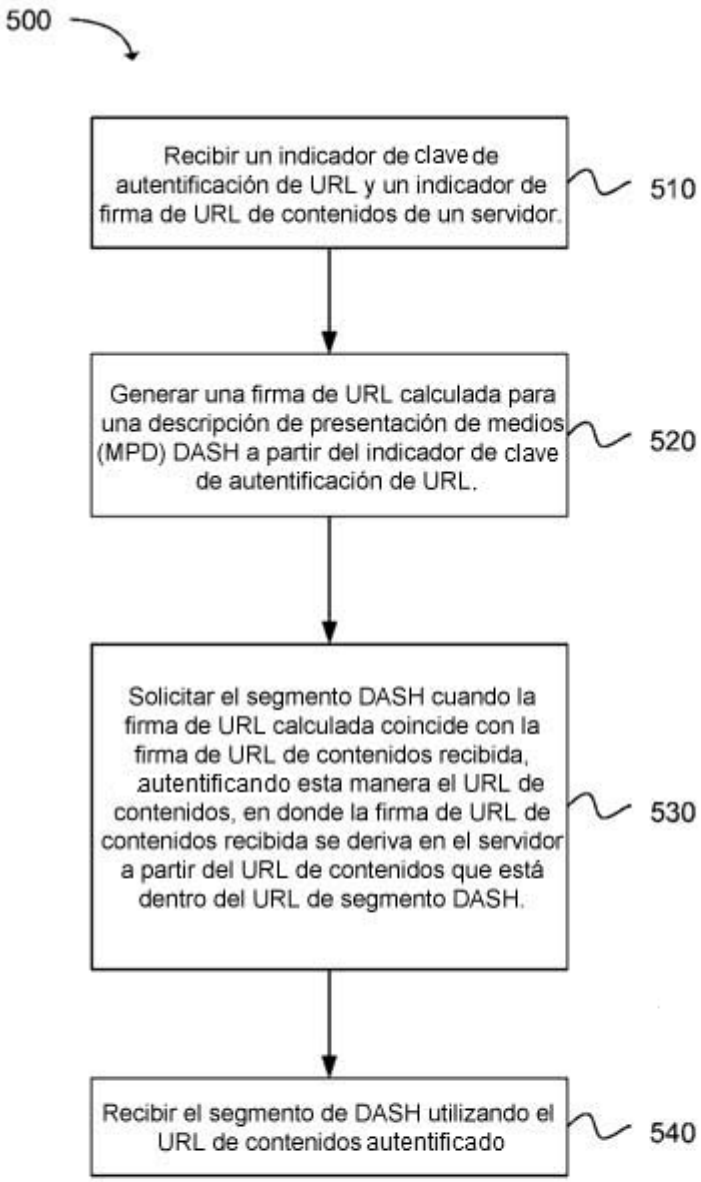
500
Recibir un indicador de clave de autentificación de URL y un indicador de firma de URL de contenidos de un servidor.
510
Generar una firma de URL calculada para una descripción de presentación de medios (MPD) DASH a partir del indicador de clave de autentificación de URL.
520
Solicitar el segmento DASH cuando la firma de URL calculada coincide con la firma de URL de contenidos recibida, autentificando esta manera el URL de contenidos, en donde la firma de URL de contenidos recibida se deriva en el servidor a partir del URL de contenidos que está dentro del URL de segmento DASH.
530
Recibir el segmento de DASH utilizando el URL de contenidos autentificado
540

FIG. 6

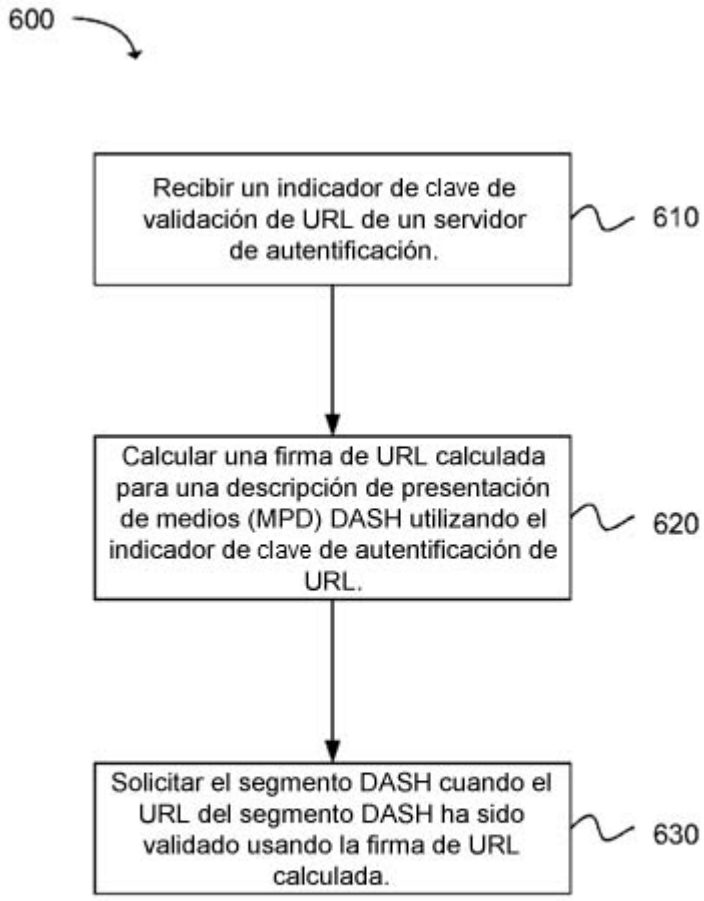
600
Recibir un indicador de clave de validación de URL de un servidor de autentificación.
610
Calcular una firma de URL calculada para una descripción de presentación de medios (MPD) DASH utilizando el indicador de clave de autentificación de URL.
620
Solicitar el segmento DASH cuando el URL del segmento DASH ha sido validado usando la firma de URL calculada.
630

FIG. 7

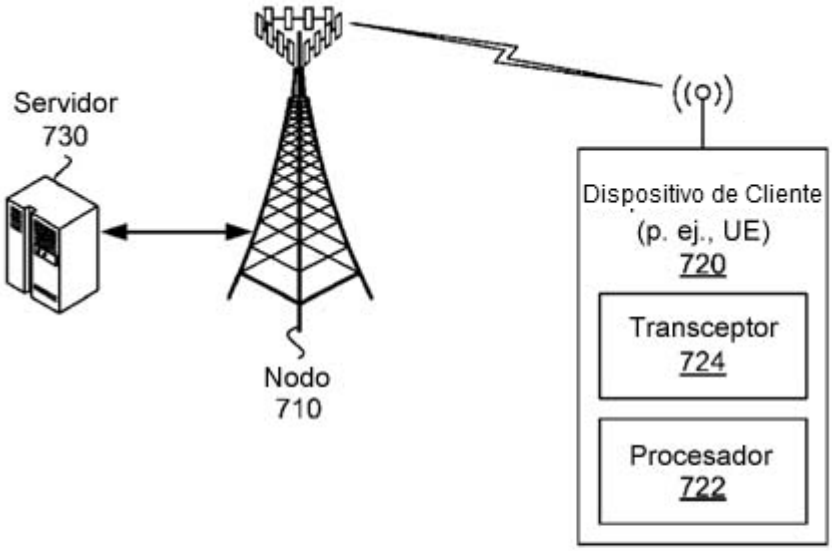
Servidor
730
Nodo
710
Dispositivo de Cliente
(p. ej., UE)
720
Transceptor
724
Procesador
722

FIG. 8

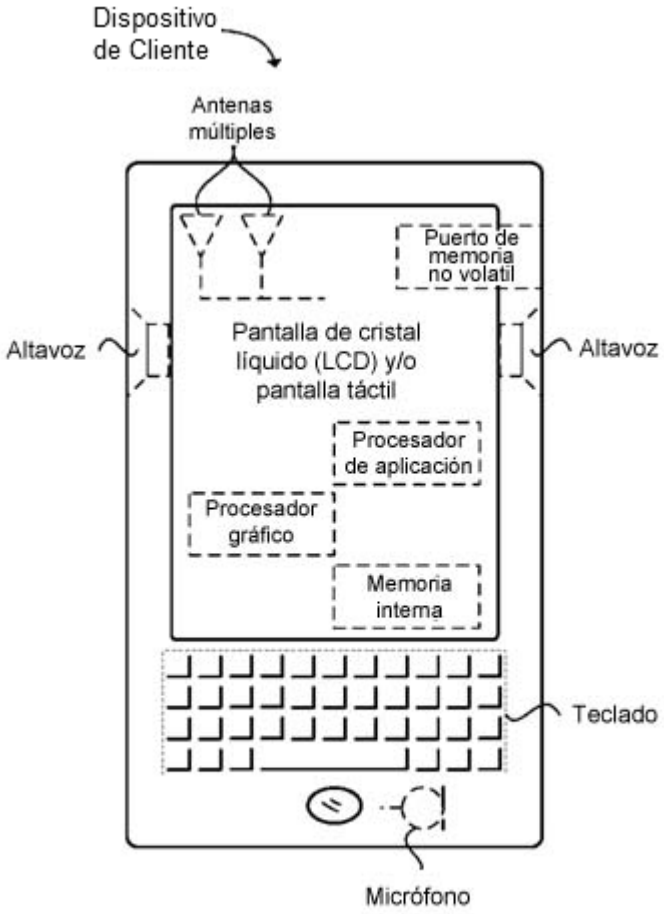
Dispositivo de Cliente
Antenas múltiples
Puerto de memoria no volatil
Altavoz
Pantalla de cristal líquido (LCD) y/o pantalla táctil
Altavoz
Procesador de aplicación
Procesador gráfico
Memoria interna
Teclado
Micrófono

FIG. 9