

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 422 191**

51 Int. Cl.:

H04N 5/00 (2011.01)

H04N 21/462 (2011.01)

H04N 7/16 (2011.01)

H04N 7/173 (2011.01)

H04N 21/454 (2011.01)

H04N 21/266 (2011.01)

H04N 21/2347 (2011.01)

H04N 21/81 (2011.01)

H04N 21/234 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **08.03.2001 E 01916529 (9)**

97 Fecha y número de publicación de la concesión europea: **08.05.2013 EP 1266524**

54 Título: **Verificación opcional de contenido de televisión interactiva**

30 Prioridad:

08.03.2000 US 521251

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

09.09.2013

73 Titular/es:

**OPENTV, INC. (100.0%)
275 Sacramento Street
San Francisco, CA 94111, US**

72 Inventor/es:

DUREAU, VINCENT

74 Agente/Representante:

TOMAS GIL, Tesifonte Enrique

ES 2 422 191 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Verificación opcional de contenido de televisión interactiva

5 Antecedentes de la invención

1. Campo de la invención

10 [0001] La invención se refiere a sistemas de televisión interactiva y más particularmente a un sistema y un método para inhibir de manera selectiva la verificación del contenido de televisión interactiva que es fiable mientras que el contenido que no es fiable se verifica.

2. Descripción de la técnica relacionada

15 [0002] Una red de televisión interactiva puede implementar una variedad de medidas para mantener la seguridad y calidad de los programas transmitidos. Diferentes redes pueden no implementar las mismas medidas, de modo que las diferentes redes pueden tener diferentes niveles de seguridad o de calidad.

20 [0003] Algunas redes pueden tener niveles muy bajos de seguridad y/o de calidad. Por ejemplo, en una red de televisión horizontal "en abierto", muchos proveedores de servicio pueden estar autorizados para transmitir contenido de televisión interactiva directamente a un usuario sin control del operador de red y sin ninguna garantía de que el contenido cumple con el nivel de calidad previsto por el fabricante del receptor de televisión interactiva. En otro ejemplo, los medios compartidos tales como Internet o las redes de cable pueden permitir que terceras partes modifiquen fácilmente el contenido que se transmite desde una parte emisora a una parte receptora. En estas redes, no se puede confiar en que el contenido que llega a un receptor cumpla con los estándares de seguridad y/o de calidad del receptor, ya sea porque un tercero lo haya manipulado o porque inicialmente no se haya transmitido con el nivel de calidad previsto.

30 [0004] Otras redes pueden tener niveles de seguridad y/o de calidad mucho más altos. Por ejemplo, una red puede estar completamente controlada por un operador de red o sus asociados (p. ej., una red vertical por satélite de TV de pago). El contenido transmitido por esta red se puede verificar antes de que se transmita, de modo que tendrá el nivel de calidad previsto por el receptor. Además, puede ser extremadamente costoso para un tercero manipular el contenido transmitido por este tipo de red, de modo que se puede asumir que el contenido no ha sido modificado por un tercero. Por lo tanto, se puede confiar en que el contenido que llega al receptor cumple con los estándares de calidad y de seguridad aplicables.

35 [0005] Para garantizar que el contenido de televisión interactiva que se entrega a un receptor cumple con las necesidades de calidad y de seguridad apropiados de este receptor, el contenido puede ser verificado por el receptor. La verificación puede garantizar que una pieza de contenido fue creada por un productor particular (es decir, autenticándola), que la pieza de contenido no ha sido manipulada durante la transmisión, que la pieza de contenido contiene los derechos de acceso apropiados o que la pieza de contenido cumple con una especificación particular (p. ej., especificación de programación). La verificación puede implicar firmas o credenciales de procesamiento que acompañan a una pieza particular de contenido (p. ej., en la autenticación), comparando estructuras de datos con una especificación (p. ej., en la verificación de código de bytes con una especificación de programación) u otras operaciones que consumen tiempo y recursos.

45 [0006] Puede ocurrir que no siempre sea deseable verificar cada pieza de contenido. Mientras que el contenido de una red de baja seguridad puede requerir autenticación para garantizar que no se ha manipulado, el contenido de una red de alta seguridad puede no necesitar autenticación porque hay poco riesgo de que el contenido haya sido producido por una fuente desautorizada o se haya manipulado. Además, si la calidad del contenido pudiera garantizarse antes de la transmisión, no habría necesidad de verificar la calidad del contenido en el receptor. En situaciones en las que hay alguna garantía de calidad y/o de seguridad, la verificación del contenido sería una pérdida de tiempo y de recursos. Por lo tanto sería deseable proporcionar un sistema y un método para distribuir contenido de televisión interactiva que permita que se realicen procedimientos de verificación de modo selectivo.

55 [0007] La EP 0.752.786 se refiere a un sistema y a un método para autenticar aplicaciones transmitidas en un sistema de información interactiva. Un programa interactivo ejecutable se combina con datos de audio/vídeo para la transmisión. El programa se divide en módulos y se crea un módulo de directorio que enlaza los módulos de programa. La seguridad para la aplicación ejecutable está provista mediante la anexión de un certificado firmado para los respectivos módulos de directorio.

60 [0008] El documento WO 98/21683 describe un sistema para proteger un ordenador de las descargas hostiles. Este ordenador está conectado a una red informática interna, dicha red está conectada a una red informática externa. Un sistema de seguridad de red interna examina las descargas recibidas de la red informática externa e impide que las descargas que parecen sospechosas lleguen a la red informática interna. El sistema de seguridad de red interna recibe las políticas de seguridad de una consola de gestión de seguridad que se encuentra en la red informática interna.

65

Resumen de la invención

[0009] La invención comprende un sistema y un método para controlar la verificación del contenido de televisión interactiva que puede incluir tanto información fiable como no fiable. El contenido fiable puede incluir información recibida de una fuente fiable. El contenido fiable también puede incluir información que, aunque se recibe desde una fuente no fiable, se identifica en sí como información fiable. "Fiable" se utiliza en este caso para referirse a contenido y/o fuentes de contenido para los que el receptor tiene la garantía de que no hay necesidad de verificar el contenido. Por ejemplo, puede haber garantía de que el contenido es auténtico o de que el contenido satisface un nivel de calidad previsto por el receptor, de modo que no es necesario verificar estas calidades.

[0010] En una forma de realización, se proporciona un método que comprende: recepción del contenido de televisión interactiva en un receptor de televisión interactiva, donde dicho contenido de televisión interactiva comprende una primera parte que es fiable y una segunda parte que no es fiable; recepción de una notificación vía los medios que entregan el contenido de televisión interactiva en dicho receptor de televisión interactiva, donde dicha notificación identifica dicha primera parte de dicho contenido de televisión interactiva como contenido fiable, el contenido fiable representa el contenido que se puede aceptar para procesamiento sin realizar uno o más procedimientos de verificación; determinación de que dicha primera parte representa contenido fiable en respuesta a la recepción de dicha notificación; determinación de que dicha segunda parte representa contenido no fiable en respuesta a la determinación de que no se ha recibido una notificación que identifique la segunda parte como contenido fiable, el contenido no fiable representa contenido que debe ser verificado por dicho o dichos procedimientos de verificación para ser aceptado para procesamiento; en respuesta a la determinación de que la segunda parte representa contenido no fiable, dicho receptor: realiza uno o más procedimientos de verificación con respecto a dicha segunda parte de dicho contenido de televisión interactiva; aceptación de la segunda parte para procesamiento en respuesta a la verificación de la segunda parte por uno o más procedimientos de verificación; y rechazo de la segunda parte en respuesta a que la segunda parte no se ha verificado por uno o más procedimientos de verificación; dicho receptor inhibe la ejecución de dicho o dichos procedimientos de verificación con respecto a dicha primera parte de dicho contenido de televisión interactiva y acepta la primera parte para procesamiento, en respuesta a la detección de dicha notificación que indica que la primera parte representa contenido fiable; donde dicha notificación es fiable en respuesta a la determinación de que la notificación está firmada, la notificación se recibe vía un canal de entrega fiable o la notificación se verifica.

[0011] Se proporciona también un sistema que comprende: un receptor de televisión interactiva que tienen uno o más receptores de señal configurados para recibir contenido de televisión interactiva y una notificación vía los medios que entregan el contenido de televisión interactiva, donde dicho contenido de televisión interactiva comprende una primera parte que es fiable y una segunda parte que no es fiable, y donde dicha notificación identifica dicha primera parte de dicho contenido de televisión interactiva como contenido fiable, el contenido fiable representa contenido que se puede aceptar para procesamiento sin realizar uno o más procedimientos de verificación; una memoria, donde dicha memoria se configura para almacenar dicha notificación; y una unidad de verificación de datos acoplada a dichos receptores de señal y dicha memoria; donde dicha unidad de verificación de datos se configura para: determinar que dicha primera parte representa contenido fiable en respuesta a la recepción de dicha notificación; determinar que dicha segunda parte representa contenido no fiable en respuesta a la determinación de que no se ha recibido una notificación que identifique la segunda parte como contenido fiable, el contenido no fiable representa contenido que debe ser verificado por dicho o dichos procedimientos de verificación para ser aceptado para procesamiento; en respuesta a la determinación de que la segunda parte representa contenido no fiable: llevar a cabo uno o más procedimientos de verificación con respecto a dicha segunda parte de dicho contenido de televisión interactiva; aceptar la segunda parte para procesamiento en respuesta a que la segunda es verificada por uno o más procedimientos de verificación; y rechazar la segunda parte en respuesta a que la segunda parte no es verificada por uno o más procedimientos de verificación; inhibir la ejecución de dicho o dichos procedimientos de verificación con respecto a dicha primera parte de dicho contenido de televisión interactiva y aceptar la primera parte para procesamiento, en respuesta a la detección de dicha notificación que indicaba que la primera parte representa contenido fiable; donde dicha notificación es fiable en respuesta a la determinación de que la notificación está firmada, la notificación es recibida vía un canal de entrega fiable o la notificación es verificada.

[0012] La identificación del contenido fiable puede ser a través de la identificación de una o más de las fuentes fiables de contenido o a través de la identificación de piezas particulares de contenido en las que se puede confiar. El contenido fiable se puede identificar bien positivamente (p. ej., "la aplicación A es fiable") o negativamente (p. ej., "todas las aplicaciones excepto la aplicación B son fiables"). La autenticidad de la notificación en sí se puede garantizar mediante la entrega a través de medios fiables, la identificación como contenido fiable o la verificación de la notificación (p. ej., usando una firma). La notificación puede incluir una fecha de caducidad después de la cual la notificación ya no es válida. La notificación también puede incluir un identificador y un número de versión. Cuando se recibe una notificación que tiene el mismo identificador y un número de versión posterior a una notificación precedente, la notificación posterior reemplaza a la precedente.

[0013] La notificación se puede transmitir al receptor con el contenido fiable o se puede transmitir antes de la transmisión del contenido fiable. La notificación también puede ser recuperada por el receptor cuando se ha recibido contenido particular. La notificación se puede transmitir al receptor usando los mismos medios que se usan para el contenido de televisión interactiva o se puede entregar por medios diferentes. Si la notificación debe ser transmitida con el contenido fiable, se puede incluir en la información de sistema para la transmisión (p. ej., descriptores asociados a la

transmisión). La notificación también se puede incluir en los datos firmados para una aplicación o módulo particular. Si la notificación se debe transmitir aparte del contenido fiable, se puede introducir, por ejemplo, en un mensaje de gestión de derechos de acceso (EMM) condicional o se puede transmitir (bien empujada o sacada) sobre una conexión punto a punto.

[0014] En una forma de realización, un receptor de televisión interactiva se configura para recibir contenido de televisión interactiva. Está provista una notificación para el receptor. La notificación identifica como fiable parte del contenido de televisión interactiva que se entrega al receptor. El receptor está configurado para verificar el contenido que no es fiable, pero está configurado para inhibir la verificación del contenido fiable. El receptor evita así la reverificación del contenido que ya es fiable. (En otro ejemplo, el receptor se puede configurar por defecto para que no verifique ningún contenido a menos que se identifique como no fiable).

[0015] El receptor se emplea en un sistema de televisión interactiva. El receptor se acopla a una o más fuentes de contenido de televisión interactiva a través de mecanismos de entrega tales como redes de difusión o conexiones punto a punto. Las fuentes proporcionan contenido fiable y/o no fiable al receptor. Las notificaciones se pueden entregar al receptor a través de los mismos mecanismos de entrega que se usan para el contenido de televisión interactiva en sí o se puede entregar mediante un mecanismo separado. Después de que se haya verificado el contenido o de que se haya inhibido la verificación del contenido, el contenido es procesado por el receptor y enviado a una televisión (o control remoto u otro dispositivo) para su presentación a un usuario.

Breve descripción de los dibujos

[0016] Se harán aparentes otros objetos y ventajas de la invención tras la lectura de la siguiente descripción detallada y en referencia a los dibujos anexos en los que:

La fig. 1 es un diagrama de bloques funcional que ilustra la distribución del contenido de televisión interactiva desde una variedad de fuentes hacia un receptor de televisión interactiva.

La fig. 2 es un diagrama de bloques de un receptor de televisión interactiva usado en una forma de realización.

La fig. 3 es un diagrama de flujos que ilustra el método por el que el receptor funciona en una forma de realización.

La fig. 4 es un diagrama que ilustra los componentes de datos de una notificación en una forma de realización.

La fig. 5 es un diagrama que ilustra los componentes de datos de una notificación en una forma de realización alternativa.

[0017] Aunque la invención puede tener varias modificaciones y formas alternativas, las formas de realización específicas de la mismas se muestran a modo de ejemplo en los dibujos y se describirán en la presente en detalle. Debe entenderse, no obstante, que los dibujos y la descripción detallada de los mismos no tiene intención de limitar la invención a la forma particular descrita, sino que, al contrario, la intención es cubrir todas las modificaciones, equivalentes y alternativas que caigan dentro del espíritu y del alcance de la presente invención, tal y como se define por las reivindicaciones anexas.

Descripción detallada de la forma de realización preferida

[0018] A continuación se describe una forma de realización de la invención. En esta forma de realización, un receptor de televisión interactiva acepta una señal de televisión interactiva vía uno o más medios, tales como redes de cable o redes de difusión por satélite. El receptor también puede aceptar contenido de conexiones punto a punto u otras fuentes de contenido. El contenido de televisión interactiva transmitido vía estos medios puede contener programas de televisión o contenido de audio-vídeo similar, al igual que contenido interactivo tal como señales de control o aplicaciones interactivas. El receptor de televisión interactiva también está configurado para recibir notificaciones, ya sea vía los medios que entregan el contenido de televisión interactiva o a través de un mecanismo de entrega separado. Estas notificaciones identifican una o más piezas de contenido de televisión interactiva fiable que se transmiten o se transmitirán al receptor. Estas piezas de contenido fiable no tienen que ser verificadas independientemente por el receptor porque, como indica la notificación, el receptor tiene alguna garantía de que cumplen con los requisitos de seguridad y/o de calidad del receptor y, por lo tanto, no necesitan ser verificadas.

[0019] En referencia a la fig. 1, se muestra un diagrama de bloques funcional que ilustra la distribución de contenido de televisión interactiva desde una variedad de fuentes hacia un receptor de televisión interactiva. Esta figura representa un receptor de televisión interactiva 12 que está acoplado a diferentes fuentes de contenido de televisión interactiva. Aunque el contenido se puede entregar a través de muchos mecanismos de entrega diferentes, se muestran tres mecanismos a modo de ejemplo en la figura. Primero, el contenido de las fuentes 14 y 15 se entregan al receptor 12 a través de una red de transmisión de difusión. Esta red consiste esencialmente en una estación de difusión 16 que ensambla el contenido de las fuentes 14 y 15 y procesa (p. ej., digitaliza, comprime y paquetiza) el contenido y una red

de transmisión por satélite 17 que recibe el contenido de la emisora de difusión 16 y lo transmite al receptor 12. (Debería puntualizarse que el receptor 12 puede ser sólo uno de los muchos receptores a los que se distribuye este contenido). El segundo mecanismo de entrega es una conexión punto a punto directa entre el receptor 12 y la fuente de 18, que puede ser algún tipo de servidor. Esta conexión se puede hacer vía una línea telefónica ordinaria. El tercer mecanismo de entrega es también una conexión punto a punto, pero la transmisión del contenido desde la fuente 19 al receptor 12 se hace vía una o más redes compartidas (p. ej., a través de Internet).

[0020] Se muestran diferentes mecanismos de entrega en la fig. 1 para ilustrar los diferentes niveles de seguridad con los que se puede entregar el contenido de televisión interactiva al receptor 12. Un mecanismo de entrega, la conexión punto a punto directa a una fuente de contenido, puede comprender comunicación vía una línea telefónica ordinaria. Este tipo de conexión es iniciado típicamente por el receptor para recuperar información desde un servidor de datos y normalmente es seguro. El contenido entregado por este mecanismo normalmente es, por lo tanto, fiable. Otro mecanismo de entrega, la conexión punto a punto a través de una o más redes, puede comprender una conexión típica entre nodos en Internet. Debido a que los datos se pueden dirigir a través de muchas redes compartidas diferentes en este caso, se pueden leer, almacenar y escribir muchas veces según se transmiten desde la fuente 19 al receptor 12. Por lo tanto hay muchas oportunidades para que los datos se corrompan o para que un tercero modifique los datos. En términos generales, este es, por lo tanto, un mecanismo de entrega de baja seguridad, por lo tanto, el contenido de televisión interactiva recibido vía este mecanismo normalmente no es fiable.

[0021] El tercer mecanismo de entrega es una red de difusión por satélite. Esta red puede, por ejemplo, comprender una red de TV de pago vertical. En este tipo de red, el contenido se comprueba típicamente antes de su difusión y, en este tipo de sistema, es difícil que un tercero modifique el contenido según se difunde, de modo que se puede asumir que el contenido recibido vía este mecanismo es fiable. Por otro lado, la red de difusión por satélite puede comprender una red de televisión horizontal "en abierto". En este tipo de red, el contenido puede no comprobarse antes de su difusión y puede ser muy fácil que un tercero modifique el contenido antes de que llegue al receptor. En este tipo de red de difusión de baja seguridad, el contenido entregado al receptor no es fiable.

[0022] En referencia a la fig. 2, se muestra un diagrama de bloques de un receptor 22. El contenido de televisión interactiva se entrega al receptor 22 a través de un receptor de señal tal como el sintonizador 31. En este ejemplo, una señal de difusión se alimenta al sintonizador 31. El sintonizador 31 selecciona un canal en el que se transmite contenido interactivo de difusión y pasa el contenido a la unidad de procesamiento 32. (Debería señalarse que el contenido de televisión interactiva también se puede entregar al receptor 22 a través de otros receptores de señal, tal como el módem 38). En el caso de una transmisión por satélite digital, el contenido se formatea en paquetes, de modo que la unidad de procesamiento 32 desmultiplexa los paquetes de la señal de difusión y reconstruye los paquetes en lo que es típicamente un programa de televisión comprimido y/o una aplicación interactiva incorporada en el contenido recibido. La descompresión es realizada por la unidad de descompresión 33. La información de audio y de vídeo asociada al programa de televisión incorporado en la señal se dirige entonces a la unidad de visualización 34, que puede desempeñar otro procesamiento y conversión de la información en un formato de televisión adecuado, tal como audio/vídeo NTSC o HDTV. Las aplicaciones reconstruidas desde la señal de difusión se dirigen a la memoria de acceso aleatorio (RAM) 37 y son ejecutadas por unidad de control 35.

[0023] La unidad de control 35 puede comprender un microprocesador, un micro controlador, un procesador de señal digital (DSP) o algún otro tipo de dispositivo procesador de instrucciones de software. La memoria 36 puede incluir unidades de memoria que sean estáticas (por ejemplo, SRAM), dinámicas (por ejemplo, DRAM), volátiles o no volátiles (por ejemplo, FLASH), según sea necesario para soportar las funciones del receptor. El código de sistema se almacena típicamente en la memoria FLASH. Cuando se aplica potencia al receptor, la unidad de control 35 ejecuta el código de sistema operativo que se almacena en la memoria 36. El código de sistema operativo se ejecuta continuamente cuando el receptor está alimentado de la misma manera que el código de sistema operativo de un ordenador personal (PC) típico y permite que el receptor ejecute la información de control y el código de aplicación.

[0024] La unidad de control 35 sirve como una unidad de verificación de datos para el contenido entregado al receptor. La verificación del contenido recibido puede comprender varios procedimientos diferentes. Por ejemplo, los procedimientos de verificación realizados por el receptor pueden incluir la verificación de código o el análisis de fichero de códigos. La verificación de código comprende la comprobación de la conformidad del código de aplicación con respecto a una especificación de programación antes de la ejecución. Esto evita la comprobación del tiempo de ejecución y permite que el código de aplicación se ejecute más rápidamente. Los procedimientos de verificación pueden incluir también autenticación. La autenticación puede comprender firmas de desenscriptación para comprobar la validez de la fuente de contenidos u otros atributos. La verificación también puede incluir la comprobación de los derechos de acceso asociados al contenido recibido. Estos derechos pueden incluir, por ejemplo, los derechos de una aplicación para acceder a recursos físicos tales como módems o unidades de disco duro para recursos virtuales tales como archivos almacenados u otro contenido recibido. Incluso también, la verificación puede incluir la comprobación de los derechos de terceros en relación con el contenido recibido (p. ej., los derechos de aplicaciones recibidas anteriormente para acceder al contenido recibido). Cabe señalar que los procedimientos recogidos en este documento están destinados a ser ejemplos de procedimientos que pueden ser innecesarios para contenido fiable y, por lo tanto, pueden evitarse cuando el contenido fiable es identificado por el sistema. Estos procedimientos pueden incluir también

procedimientos sin verificación. Por motivos de brevedad, no obstante, tales procedimientos se denominarán generalmente, en este caso, procedimientos de verificación.

[0025] La unidad de control 35 está configurada para verificar selectivamente el contenido de televisión interactiva recibido basado en las notificaciones que identifican contenido particular como fiable o no fiable. Las notificaciones que se reciben a través del canal de difusión, la conexión de módem u otros medios se almacenan en la memoria del receptor. Según se entrega el contenido de televisión interactiva al receptor, la unidad de control 35 determina si el contenido debería o no ser verificado, basado en la identificación de las notificaciones de contenido particular como fiable o no fiable. En una forma de realización, el receptor verifica el contenido recibido por defecto. Esto es, a menos que una notificación identifique el contenido particular como fiable, éste será verificado por el receptor antes de su uso. En otros ejemplos, el receptor puede estar configurado para asumir que todo el contenido es fiable, de modo que ningún contenido recibido será verificado a menos que se identifique específicamente como no fiable.

[0026] El receptor se aloja típicamente en un descodificador conectado a un televisor del usuario. Debe observarse que el receptor puede comprender cualquier unidad de procesamiento para recibir y procesar el contenido de televisión interactiva. El receptor puede ser en un alojamiento de descodificador que se encuentra físicamente en la parte superior de un televisor, puede estar en alguna otra ubicación externa al televisor (p. ej., en el lateral o en la parte trasera del televisor o en una ubicación remota del televisor) o puede estar incorporado en el propio televisor. De forma similar, el televisor al que se dirige la salida del receptor puede comprender un monitor de televisión o de vídeo que utiliza cualquier formato de televisión adecuado (p. ej., NTSC o HDTV) o se puede sustituir por otros dispositivos, tales como un grabador de vídeo.

[0027] En referencia a la fig. 3, se muestra un diagrama de flujos que ilustra el método empleado por el receptor. En este método, se proporciona una notificación para que el receptor identifique el contenido que es fiable y por lo tanto no requiera verificación por el receptor. Cuando el contenido es recibido por el receptor, el receptor determina si el contenido es fiable, de acuerdo con la notificación. Si el contenido es fiable, entonces es usado por el receptor sin más verificación. Si el contenido no es fiable, el receptor ejecuta los procedimientos de verificación normales en el contenido. Si el contenido se puede verificar usando estos procedimientos, el contenido es usado entonces por el receptor. Si el contenido no se puede verificar usando los procedimientos de verificación normales, se descarta (es decir, no se usa).

[0028] La notificación se puede entregar con el contenido fiable o se puede entregar antes de la transmisión del contenido fiable. La manera particular en la que se entrega la notificación puede variar de una forma de realización a otra. Por ejemplo, en un ejemplo, la notificación puede ser entregada al receptor a través de un canal seguro (p. ej., un acceso EMM condicional o una conexión punto a punto directa entre el emisor y el receptor). Debido a que el canal es seguro, no hay necesidad de encriptar la notificación o proporcionar una credencial para su uso en la verificación de la notificación. En otra forma de realización, la notificación se puede entregar a través de un canal que no sea seguro. En este caso, la notificación puede estar firmada o puede proporcionar otros medios para verificar su autenticidad. En otro ejemplo, la notificación puede estar incluida en datos firmados dentro de una aplicación o módulo, de modo que cuando la aplicación o el módulo se verifican, la notificación también se verifica. La notificación puede entonces indicar que el contenido subsiguiente es fiable. Se observa que múltiples notificaciones pueden ser activamente usadas por el receptor para determinar si el contenido recibido es o no fiable.

[0029] En referencia a la fig. 4, se muestra un diagrama que ilustra los componentes de datos de una notificación en un ejemplo. El componente primario de la notificación 40 es la información 41 que identifica qué contenido es fiable. El contenido fiable se puede identificar de numerosas y diferentes maneras. Por ejemplo, el contenido puede ser identificado por su fuente o por referencia al contenido en sí. La fuente del contenido puede ser un proveedor de servicios, un programa, un canal, un bouquet (una colección de canales) o una red (una colección de bouquets). Si el contenido es identificado por su fuente, todo el contenido recibido desde la fuente fiable es fiable para el receptor hasta que la notificación expire o se reemplace o revoque. El contenido fiable también se puede identificar por referencia al contenido particular que es fiable, independientemente de su fuente. En este caso, la notificación puede identificar aplicaciones particulares, partes de aplicaciones, módulos, programas, flujos de datos u otro contenido. Si el contenido fiable es identificado por la fuente o por referencia al contenido particular, se pueden utilizar valores comodín en la identificación. Por ejemplo, todas las aplicaciones de un productor particular que tengan una identidad que empiece por un número particular son fiables.

[0030] La identificación del contenido fiable puede ser positiva o negativa. Esto es, una notificación puede identificar contenido que sea fiable o puede identificar contenido que no sea fiable. Al identificar explícitamente el contenido que no es fiable, el contenido restante se puede identificar como fiable. En cualquier caso, el contenido fiable es identificado por la notificación. De forma similar, el receptor puede utilizar un valor predeterminado positivo o negativo para los procedimientos de verificación. En otras palabras, el receptor se puede configurar para verificar todos los contenidos recibidos a menos que algún contenido sea identificado como que no requiere verificación (es decir, el contenido es fiable) o se puede configurar para que no verifique ningún contenido recibido a menos que algún contenido sea identificado como que requiere verificación (es decir, el contenido no es fiable).

[0031] Como se puede observar en la fig. 4, la notificación también puede incluir distintos componentes además de la información que identifica el contenido fiable. En este ejemplo, la notificación también incluye una identidad de

notificación 42, una versión de notificación 43, una expiración 44 y un certificado 45. Además, la notificación 40 incluye una firma 47 para verificar la notificación.

[0032] La expiración 44, la identidad de notificación 42 y la versión de notificación 43 se utilizan para limitar el tiempo de vida de la notificación. La expiración 44 da una fecha y/o un momento en el que la notificación expira. La identificación de la notificación del contenido fiable es válida sólo hasta la fecha de caducidad. En un sistema que por defecto verifica todos los contenidos, el contenido que es identificado por la notificación como fiable no se verifica si se recibe antes de la fecha de caducidad, pero sí se verifica si se recibe después de la fecha de caducidad. Aunque no se representa en la figura, se contempla que la notificación también puede incluir una hora de inicio en la que la notificación se convierte inicialmente en válida. La identidad de notificación 42 y la versión de notificación 43 también pueden limitar el tiempo de vida de una notificación particular. Una notificación posterior que tiene una identidad de notificación idéntica a una notificación previa reemplazará la notificación previa si la notificación posterior tiene un número de versión posterior. En este caso, la primera notificación no se convierte necesariamente en inválida en su totalidad, sino que es sustituida por la segunda notificación de reemplazo. Si no se recibe ninguna notificación posterior, la notificación previa permanecerá válida indefinidamente (a menos que expire o se termine de otro modo). La notificación posterior puede modificar sólo partes de la notificación previa mientras el resto se mantiene o puede proporcionar una identificación completamente diferente del contenido fiable.

[0033] La notificación 40 incorpora la firma 47 para permitir la verificación de la autenticidad de la notificación. Una firma utiliza medios tales como encriptación mediante clave pública para permitir la verificación del contenido asociado. Los sistemas de encriptación mediante clave pública pueden emplear varios algoritmos de encriptación. Sea cual sea el algoritmo que se seleccione para un sistema de encriptación mediante clave pública particular, el sistema utiliza un par de claves de encriptación, una de ellas se denomina clave privada y una de ellas se denomina clave pública. La clave privada es mantenida en secreto por su propietario, mientras que la clave pública está libremente disponible. Un mensaje u otro archivo que esté encriptado con la clave pública sólo puede ser descifrado con la clave privada. Asimismo, un archivo que esté encriptado con la clave privada sólo puede ser descifrado con la clave pública. Cuando un mensaje está encriptado con una de las claves, se convierte en un conjunto aparentemente aleatorio de caracteres. Así, cuando un mensaje encriptado con una clave pública se envía al titular de la clave privada, el emisor puede tener la certeza de que, aunque el mensaje sea interceptado, sólo el receptor deseado (que posee la clave privada) puede descifrar éste y leer el mensaje. Cuando un mensaje está firmado, en lugar de encriptado, el mensaje permanece en forma legible, pero hay una firma encriptada anexa al mensaje. Aunque cualquiera que vea el mensaje puede leerlo, la firma puede utilizarse para verificar que el mensaje se originó con el titular de la clave privada. Además, debido a que el algoritmo que encripta la firma depende en parte del mensaje que precede a la firma, cualquier cambio en el mensaje hará que la firma no sea verificable. Por lo tanto, la firma puede utilizarse para garantizar que el mensaje no se ha modificado.

[0034] En referencia a la fig. 5, se ilustra una notificación en un ejemplo alternativo. La notificación 50 incluye información 51, una identidad de notificación 52, una versión de notificación 53, una expiración 54 y un certificado 55. La notificación 50 incluye la firma 56 del autor de la notificación y el certificado 55 incluye la firma 57 de una parte fiable. El certificado 55 se usa como medio para garantizar que la notificación 50 fue creada por una parte autorizada. El certificado 55 es la clave pública del autor de la notificación, firmada por alguna parte fiable. Una parte fiable es una parte que puede certificar la autenticidad de la clave. La firma de la parte fiable está encriptada e incorporada a la clave. La clave pública de la parte fiable es bien conocida. Esto es, está almacenada en el receptor y siempre está disponible para el receptor. Toda la notificación 50 se firma 57 entonces con la clave privada de la parte autorizada para garantizar que ninguno de los datos de la notificación 50 se pueda modificar. El uso del certificado 55 en la notificación 50 proporciona unos medios para verificar que la información 51 es autorizada. La notificación 50 es por lo tanto adecuada para permitir que la notificación identifique el contenido fiable producido por un tercero en lugar de una parte fiable.

[0035] Debe observarse que los certificados y firmas usados en las notificaciones anteriormente descritas están concebidos para garantizar la autenticidad de las notificaciones. En algunos ejemplos, las notificaciones pueden ser entregadas al receptor por medios de entrega seguros, en cuyo caso las firmas y/o los certificados pueden no ser necesarios.

[0036] Como se ha indicado anteriormente, la verificación del contenido de televisión interactiva puede incluir muchos y diferentes tipos de procedimientos. Por ejemplo, la verificación puede incluir la autenticación del contenido. El contenido de televisión interactiva puede comprender varios tipos de datos, tales como flujos de datos de audio y/o de vídeo o módulos de datos de aplicaciones, cada uno de los cuales puede estar acompañado por algún tipo de firma que se puede usar para verificar los datos. El contenido de televisión interactiva también puede incluir algún tipo de credencial. En los sistemas típicos del estado de la técnica, si el contenido de televisión interactiva se transmite con una firma o credencial, el receptor puede automáticamente verificar la firma o credencial a la recepción o uso del contenido. Como se ha explicado anteriormente, esto puede implicar el uso de algoritmos de encriptación mediante clave pública para verificar la firma o para ejecutar procesos relacionados con la credencial (p. ej., modificación de unos derechos de acceso de la aplicación). Consecuentemente, una parte de la potencia de procesamiento del receptor puede ser consumida por la verificación y otros procesos, independientemente de si el contenido se entregó o no a través de un medio seguro. El presente sistema y método se puede emplear, por lo tanto, para identificar el contenido recibido como

fiable o no fiable y, si es fiable, para inhibir los procesos que de otra manera se llevarían a cabo. Como resultado, la potencia de procesamiento del receptor no se desperdicia en procedimientos innecesarios.

5 [0037] Otro tipo de operación que, en el caso de contenido fiable, se puede evitar en el presente sistema es la verificación del código. La verificación del código se refiere a la calidad del contenido más que a la seguridad del contenido. La verificación del código está generalmente destinada a garantizar que la representación binaria del código, tal como una clase o interfaz, sea estructuralmente correcta. Por ejemplo, los procedimientos de verificación de código pueden incluir la comprobación de cada instrucción para asegurarse de que tiene un código de operación válido o la comprobación de cada instrucción de derivación para asegurarse de que deriva al principio de la instrucción y no al medio de una instrucción. La verificación de código se realiza frecuentemente en applets o aplicaciones de Java antes de ejecutarla, de modo que es necesario hacer estas comprobaciones estructurales durante la ejecución de los applets o aplicaciones. La verificación de código que se realiza antes del tiempo de ejecución permite que el código verificado se ejecute más rápidamente. Aunque la verificación de código puede aumentar la velocidad de ejecución de un applet o aplicación, las comprobaciones estructurales realizadas en la verificación no se eliminan, simplemente se realizan antes del tiempo de ejecución en vez de durante el tiempo de ejecución. El receptor todavía tiene que dedicar valiosos y limitados recursos a la verificación. El presente sistema permite que la verificación de procedimientos salga completamente del receptor. Esto es, si el código de aplicación (contenido de televisión interactiva) se ha verificado antes de su entrega al receptor y hay alguna garantía de que la verificación del código entregado siga siendo válida (es decir, el código es fiable), no es necesario verificarlo nuevamente en el receptor. La inhibición de la verificación de código, por lo tanto, evita desperdiciar los recursos de procesamiento del receptor en esta innecesaria verificación. (Debe señalarse que el presente sistema se puede utilizar para evitar la verificación de código innecesaria, independientemente de que la verificación se produzca antes del tiempo de ejecución o en el tiempo de ejecución).

25 [0038] Los ejemplos anteriores tienen la intención de ilustrar algunos de los procedimientos que se pueden evitar por varias formas de realización del presente sistema. La referencia a estos procedimientos como procedimientos de verificación no está destinada a limitar los tipos de procedimientos que pueden estar implicados, sino simplemente para proporcionar una etiqueta conveniente a los procedimientos que se pueden evitar usando el presente sistema. Así, puede haber otros muchos tipos de procedimientos que son no necesarios, pero que se realizan en el contenido de televisión interactiva por defecto. Si se puede determinar antes de transmitir el contenido particular que es innecesario ejecutar estos procedimientos, este contenido se puede considerar fiable y el receptor de televisión interactiva puede estar configurado para inhibir los procedimientos en cuanto al contenido fiable. Consecuentemente, el presente sistema se puede utilizar para evitar la amplia gama de procedimientos que puede no ser necesario realizar, mejorando así la eficiencia de los sistemas de televisión interactiva a los que se incorpora.

35 [0039] Aunque la presente invención se ha descrito con referencia a las formas de realización particulares, se entenderá que las formas de realización son ilustrativas y que el alcance de la invención no se limita a estas formas de realización. Son posibles muchas variaciones, modificaciones, adiciones y mejoras de las formas de realización descritas.

REIVINDICACIONES

1. Método que comprende:

5 recepción del contenido de televisión interactiva en un receptor de televisión interactiva (12, 22), donde dicho contenido de televisión interactiva comprende una primera parte que es fiable o una segunda parte que no es fiable,

10 recepción de una notificación (40, 50) **a través de los medios que entregan el contenido de televisión interactiva** en dicho receptor de televisión interactiva (12, 22), dicha notificación está separada de la primera parte y de la segunda parte y donde dicha notificación identifica dicha primera parte de dicho contenido de televisión interactiva como contenido fiable, el contenido fiable es el contenido dado para el cual el receptor ha recibido una notificación que identifica el contenido dado como uno que cumple con los estándares de seguridad y/o de calidad del receptor y el contenido no fiable es el contenido para el cual el receptor no ha recibido tal notificación;

15 determinación de que dicha primera parte es contenido fiable sobre la base de dicha notificación;

20 determinación de que dicha segunda parte es contenido no fiable sobre la base de una determinación de que no se ha recibido una notificación que identifique la segunda parte como contenido fiable;

sobre la base de la determinación de que la segunda parte representa contenido no fiable, dicho receptor:

25 realiza uno o más procedimientos de verificación con respecto a dicha segunda parte de dicho contenido de televisión interactiva para verificar que la segunda parte cumple con dichos estándares de seguridad y/o de calidad del receptor;

30 usa la segunda parte para el procesamiento en respuesta a la verificación de la segunda parte por uno o más procedimientos de verificación; y

rechaza la segunda parte en respuesta a que la segunda parte no ha sido verificada por uno o más procedimientos de verificación;

35 dicho receptor impide la ejecución de dicho o dichos procedimientos de verificación con respecto a dicha primera parte de dicho contenido de televisión interactiva y utiliza la primera parte para el procesamiento, en respuesta a la detección de dicha notificación que indica que la primera parte representa contenido fiable.

2. Método según la reivindicación 1 donde dicho o dichos procedimientos de verificación comprenden uno o varios de:

40 autenticación de dicho contenido de televisión interactiva;

verificación de que dicho contenido de televisión interactiva no ha sido manipulado durante la transmisión;

45 verificación de que dicho contenido de televisión interactiva posee los derechos de acceso apropiados; y

verificación de que dicho contenido de televisión interactiva cumple con una especificación predeterminada.

3. Método según la reivindicación 1 que comprende además la transmisión de dicho contenido de televisión interactiva a dicho receptor de televisión interactiva (12, 22) y la transmisión de dicha notificación (40, 50) a dicho receptor de televisión interactiva (12, 22).

4. Método según la reivindicación 1 donde dicha primera parte de dicho contenido de televisión interactiva comprende contenido asociado a una fuente identificada (14, 15, 18, 19).

5. Método según la reivindicación 4 donde dicha fuente (14, 15, 18, 19) se selecciona del grupo que consiste en: un paquete, una red, un canal y un programa.

6. Método según la reivindicación 4 donde dicha fuente (14, 15, 18, 19) comprende un proveedor de servicios.

7. Método según la reivindicación 1 donde dicha primera parte de dicho contenido de televisión interactiva comprende piezas identificadas de contenido.

8. Método según la reivindicación 7 donde dichas piezas de contenido comprenden al menos una parte de una aplicación televisiva interactiva.

9. Método según la reivindicación 7 donde dicha primera parte de dicho contenido de televisión interactiva se identifica por uno o más caracteres comodín.
- 5 10. Método según la reivindicación 1 donde dicha primera parte de dicho contenido de televisión interactiva se identifica por la identificación explícita de dicha segunda parte de dicho contenido de televisión interactiva.
11. Método según la reivindicación 1 donde dicha notificación es transmitida a dicho receptor (12, 22) antes de transmitir dicho contenido de televisión interactiva a dicho receptor (12, 22).
- 10 12. Método según la reivindicación 1 donde dicha notificación es transmitida a dicho receptor (12, 22) con dicho contenido de televisión interactiva.
13. Método según la reivindicación 1 donde dicha notificación es recibida a través de un canal de entrega fiable que comprende un acceso condicional EMM.
- 15 14. Método según la reivindicación 1 donde dicha notificación es recibida a través de un canal de entrega fiable que comprende un canal punto a punto.
15. Método según la reivindicación 14 donde dicha notificación es impulsada hacia dicho receptor sobre dicho canal punto a punto.
- 20 16. Método según la reivindicación 14 donde dicha notificación es sacada por dicho receptor sobre dicho canal punto a punto.
- 25 17. Método según la reivindicación 1 donde dicha notificación está contenida en datos firmados asociados a una aplicación.
18. Método según la reivindicación 1 donde dicha notificación posee un tiempo de caducidad asociado a esta última, donde dicha notificación es válida antes de dicha fecha de caducidad e inválida después de dicho tiempo de caducidad.
- 30 19. Método según la reivindicación 1 donde dicha notificación posee un número de versión asociado a ésta, donde una notificación que posee un número de versión posterior reemplaza a una notificación que posee un número de versión anterior.
- 35 20. Sistema que comprende:
- un receptor de televisión interactiva (12, 22) que posee
 - uno o más receptores de señal (31) configurados para recibir el contenido de televisión interactiva y una notificación a través de los mismos medios que el contenido de televisión interactiva, donde dicho contenido de televisión interactiva comprende una primera parte que es fiable o una segunda parte que no es fiable, dicha notificación está separada de la primera parte y de la segunda parte y donde dicha notificación identifica la primera parte de dicho contenido de televisión interactiva como contenido fiable, el contenido fiable es contenido dado para el cual el receptor ha recibido una notificación que identifica el contenido dado como que cumple con los estándares de seguridad y/o de calidad del receptor, y el contenido no fiable es contenido para el cual el receptor no ha recibido tal notificación;
 - una memoria (36), donde dicha memoria está configurada para memorizar dicha notificación; y
 - una unidad de verificación de datos (35) acoplada a dicho receptor de señal y a dicha memoria;
 - donde dicha unidad de verificación de datos está configurada para:
 - determinar que dicha primera parte es contenido fiable sobre la base de dicha notificación;
 - determinar que dicha segunda parte es contenido no fiable sobre la base de una determinación de que no se ha recibido una notificación que identifique la segunda parte como contenido fiable;
 - sobre la base de la determinación de que la segunda parte representa contenido no fiable:
 - ejecutar uno o más procedimientos de verificación con respecto a dicha segunda parte de dicho contenido de televisión interactiva para verificar que la segunda parte cumple con dichos estándares de seguridad y/o de calidad del receptor;
 - utilizar la segunda parte para el procesamiento en respuesta a la verificación de la segunda parte por uno o más procedimientos de verificación; y

rechazar la segunda parte en respuesta a que la segunda parte no ha sido verificada por uno o más procedimientos de verificación;

5 inhibir la ejecución de dicho o dichos procedimientos de verificación con respecto a dicha primera parte de dicho contenido de televisión interactiva y utilizar la primera parte para el procesamiento, en respuesta a la detección de dicha notificación que indica que la primera parte representa contenido fiable.

10 21. Sistema según la reivindicación 20 donde dicho contenido de televisión interactiva se entrega a un primer receptor de señal de dicho o dichos receptores de señal por un primer medio y dicha notificación se entrega a un segundo receptor de señal de dicho o dichos receptores de señal por un segundo medio.

15 22. Sistema según la reivindicación 20 donde dicha notificación comprende una primera versión de dicha notificación, y donde cuando dicha unidad de verificación de datos recibe una segunda versión de dicha notificación, dicha unidad de verificación de datos está configurada para reemplazar dicha primera versión de dicha notificación en dicha memoria por dicha segunda versión de dicha notificación para identificar dicha primera parte de dicho contenido de televisión interactiva sobre la base de dicha segunda versión de dicha notificación.

20 23. Sistema según la reivindicación 20 que comprende además un transmisor de televisión interactiva y un medio de transmisión, donde dicho transmisor de televisión interactiva está acoplado a dicho receptor de televisión interactiva por dicho medio de transmisión y donde dicho transmisor de televisión interactiva está configurado para transmitir dichos datos de televisión interactiva a dicho receptor de televisión interactiva a través de dicho medio de transmisión.

25 24. Sistema según la reivindicación 20 que comprende además una fuente de notificación acoplada a dicho receptor de televisión interactiva, donde dicha fuente de notificación está configurada para transmitir dicha notificación a dicho receptor de televisión interactiva.

25 25. Sistema según la reivindicación 20 donde dicha notificación comprende datos firmados por una parte fiable.

30 26. Sistema según la reivindicación 20 donde dicha notificación está integrada en un certificado asociado a dicha primera parte de dicho contenido de televisión interactiva.

35 27. Sistema según la reivindicación 20 donde dicha notificación está contenida en una credencial, donde dicha credencial está firmada por un autor de dicha credencial, y donde dicha credencial contiene un certificado para verificar la firma de dicho productor y garantizar a dicho productor un derecho para proporcionar contenido fiable.

40 28. Método según la reivindicación 1 o sistema según la reivindicación 20, donde dicha notificación identifica además una tercera parte de contenido de televisión interactiva como contenido fiable, dicha tercera parte es contenido que aún no ha sido recibido por el receptor, y donde el método o sistema comprende además:

recepción posterior del tercer contenido; y

45 dicho receptor inhibe la ejecución de dicho o dichos procedimientos de verificación con respecto a la tercera parte y acepta la tercera parte para el procesamiento, en respuesta a la determinación de que dicha notificación recibida previamente indica que la tercera parte representa contenido fiable.

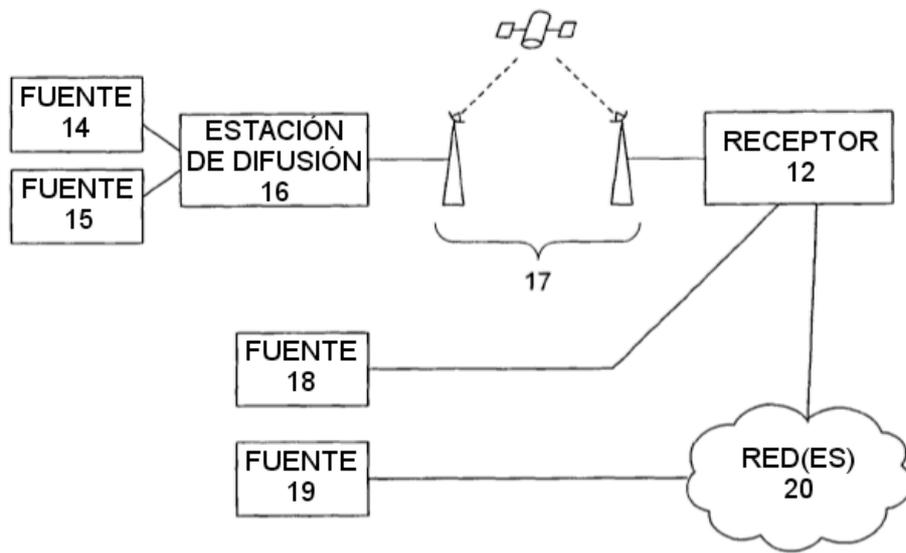


Fig. 1

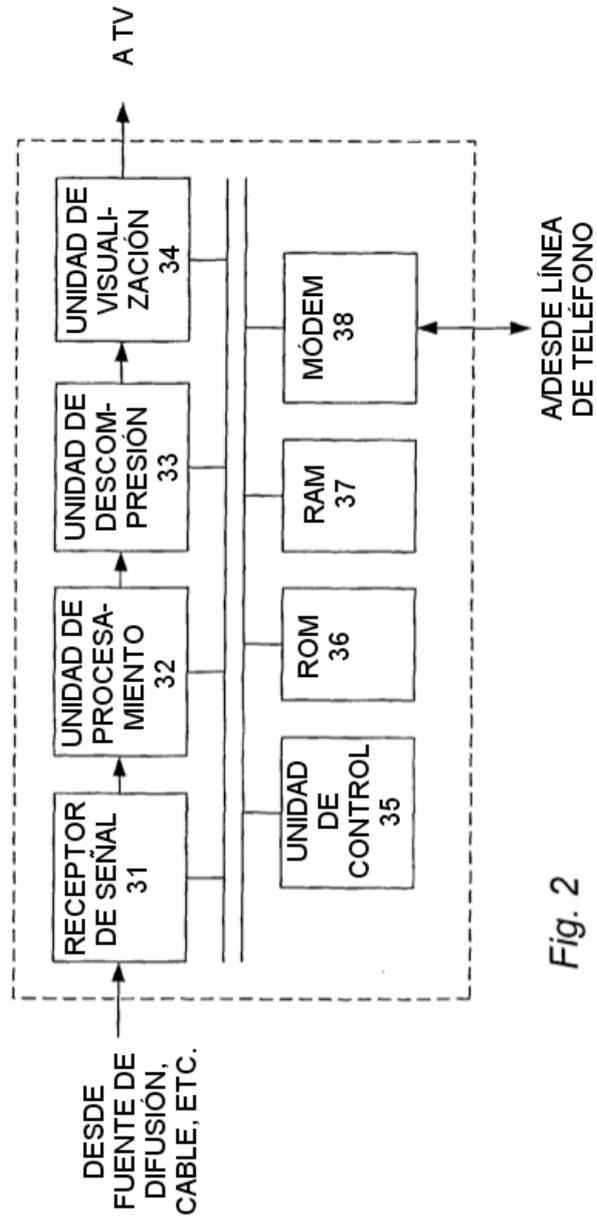


Fig. 2

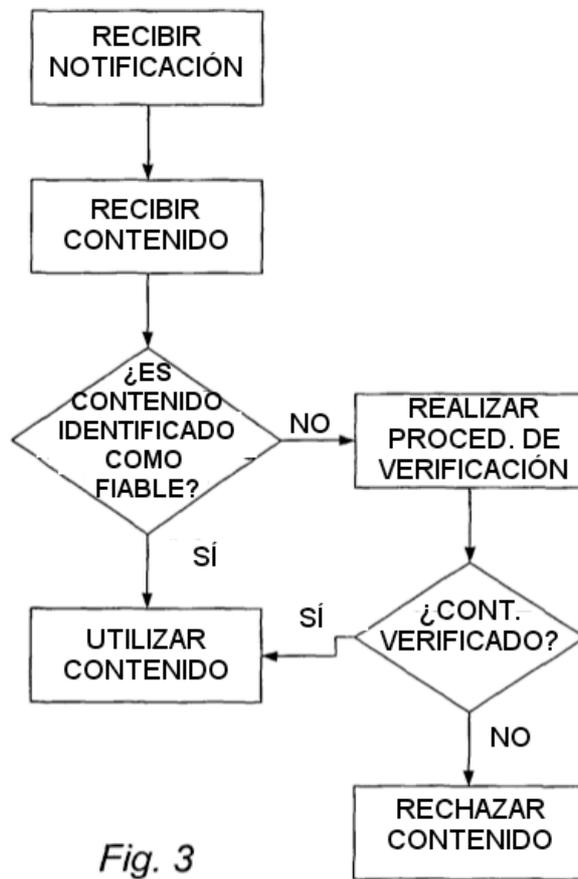


Fig. 3

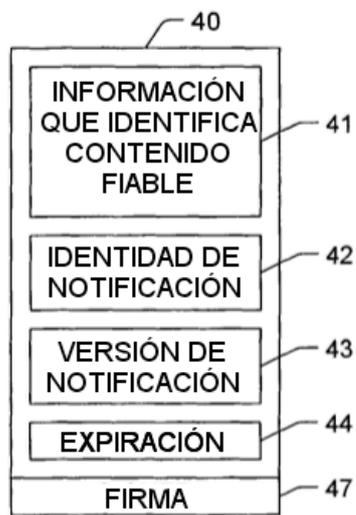


Fig. 4

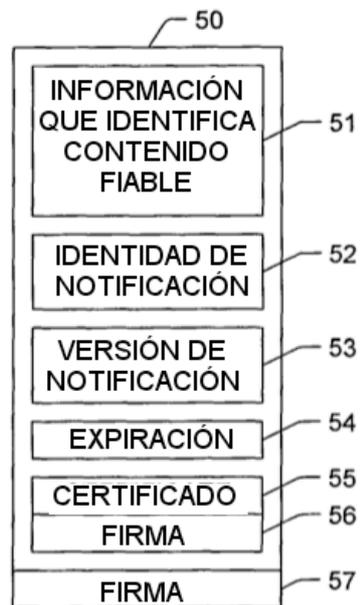


Fig. 5