(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 969 760**

(51) Int. Cl.:

H04H 60/23 (2008.01)
H04N 7/167 (2011.01)
H04N 21/254 (2011.01)
H04N 21/4627 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.07.2016 PCT/EP2016/066618**

(87) Fecha y número de publicación internacional: **19.01.2017 WO17009370**

(96) Fecha de presentación y número de la solicitud europea: **13.07.2016 E 16748067 (2)**

(97) Fecha y número de publicación de la concesión europea: **20.12.2023 EP 3323215**

(54) Título: **Autenticación de datos de difusión digital**

(30) Prioridad:

13.07.2015 GB 201512232

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.05.2024

(73) Titular/es:

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

(72) Inventor/es:

WENDLING, BERTRAND y
AUMASSON, JEAN-PHILIPPE

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Autenticación de datos de difusión digital

La presente descripción se refiere a los datos de verificación transmitidos en una señal de difusión digital, en particular, aunque no exclusivamente en una señal de televisión digital, y más específicamente en el contexto de HbbTV.

Antecedentes

Los sistemas modernos de televisión interactiva, como aquellos que implementan el estándar HbbTV, permiten que las aplicaciones interactivas se ejecuten en un terminal de usuario como un televisor o un decodificador. En particular, de acuerdo con el estándar HbbTV, se sigue un enfoque híbrido mediante el cual los datos de la aplicación pueden ser recibidos en una señal de difusión, por aire, por satélite o por cable. Los datos de la aplicación pueden incluir un enlace de Internet o un localizador de recursos universal (URL) a una ubicación desde donde la aplicación interactiva, o el contenido para una aplicación interactiva local, puede ser descargado por el terminal del usuario a través de Internet. Esto se ilustra en la Figura 1. Por ejemplo, en un sistema HbbTV, los datos de la aplicación se proporcionan en forma de tablas formateadas según el estándar de Transmisión Digital de Vídeo (DVB), comúnmente conocidas como Tabla de Información de Aplicación (AIT). Los datos de la aplicación pueden incluir una URL como se mencionó anteriormente, otros datos para ser utilizados por una aplicación y/o un carrusel de datos u objetos para descargar los datos de la aplicación o la propia aplicación desde la señal de difusión. En los sistemas discutidos anteriormente, los datos (por ejemplo, las tablas) se transmiten en texto claro.

En particular, dado que la transmisión de los datos de la aplicación se realiza en texto claro, existe un riesgo de un tipo de ataque de intermediario, en el cual un pirata informático intercepta la señal de difusión y manipula los datos de la aplicación antes de enviarlos. Los datos de la aplicación pueden ser manipulados de tal manera que dirijan a una aplicación residente en un televisor a acceder a información fraudulenta, por ejemplo, haciendo que un usuario divulgue información confidencial al pirata, o descargar una aplicación desde una URL pirata, por ejemplo, para instalar un virus en el televisor. Los datos de la aplicación manipulada son luego enviados o transmitidos por el pirata con el objetivo de llevar a cabo un fraude cuando el televisor o su usuario actúen sobre la información. Esto se ilustra en la Figura 2.

Para aumentar la seguridad de los sistemas de TV interactiva, sería conveniente difundir los datos de la aplicación de tal manera que se protejan contra ataques de intermediarios del tipo descrito anteriormente.

Se describe un decodificador de televisión en el que se verifica una firma clave que ha sido generada para una clave de descifrado pública utilizando una clave de firma privada, utilizando una clave de verificación pública correspondiente a la clave de firma privada, según se describe en el documento EP1 7684048.

Resumen

En resumen, las modalidades descritas se refieren a la autenticación de datos de aplicación transmitidos digitalmente mediante la firma digital de los datos de aplicación. Un certificado asociado con una clave privada utilizada por el emisor del certificado para firmar digitalmente los datos de la aplicación puede ser utilizado por un televisor o cualquier otro terminal de usuario para verificar la firma digital. Se describen modalidades para verificar y generar confianza en el certificado, tanto inicialmente como cuando se emite un nuevo certificado por el emisor. Sin mecanismos para verificar la confianza en el certificado, especialmente cuando un certificado cambia, el sistema seguiría siendo vulnerable a un ataque de intermediario en el que el pirata reemplaza el certificado del emisor con un certificado pirata.

Se apreciará que el emisor del certificado (el propietario de la clave privada correspondiente) puede ser una persona natural o una entidad legal como una difusora. Sin embargo, tal como se utiliza en el presente documento, el término "emisor" puede hacer referencia a una aplicación, servicio, canal de difusión o programa en particular para el cual los datos de la aplicación pueden ser firmados de forma independiente. Asimismo, la referencia a un emisor también abarcaría, por ejemplo, una agrupación de difusoras que hayan acordado utilizar el mismo certificado. El término "propietario", por ejemplo, propietario de una clave privada, se entenderá en consecuencia. Además, se apreciará que la presente descripción es igualmente aplicable a datos de difusión distintos de los datos de la aplicación, por ejemplo, datos de superposición de pantalla que invitan a un usuario a llamar a una línea de ayuda para donaciones, aunque gran parte de la descripción actual se realiza en términos de datos de la aplicación a modo de ejemplo y para mayor claridad y simplicidad.

El término "certificado" se entiende como una clave pública (asociada con una clave privada utilizada por el emisor para firmar datos) junto con al menos una firma digital aplicada a la clave pública. Se puede proporcionar un certificado según varios formatos y estándares, por ejemplo, el estándar X.509. Una firma digital de un mensaje (aquí típicamente un elemento de datos o una clave pública) se genera aplicando una clave privada de un par de claves al mensaje o a un resumen hash del mensaje utilizando un algoritmo de firma, muchos ejemplos de los cuales

son bien conocidos en el arte. Una firma digital de un mensaje puede ser verificada por un algoritmo de verificación de firma (correspondiente al algoritmo de firma) utilizando una clave pública del par de claves para verificar la correspondencia entre la firma y el mensaje o su resumen de hash. La referencia a la verificación de datos utilizando un certificado se entenderá como que comprende la verificación de una firma digital de los datos utilizando una clave pública asociada con el certificado.

La referencia a la firma de un nuevo certificado con una clave privada específica se entenderá como la firma de al menos una clave pública asociada con el nuevo certificado con la clave privada específica (aunque la firma puede generarse al firmar otros datos junto con la clave pública, por ejemplo, información del emisor o información relacionada con una autoridad de certificación externa). El término "firma" se entenderá en consecuencia en este contexto. Donde la clave privada específica está asociada con un certificado existente, este proceso de firma también puede denominarse emitir el nuevo certificado utilizando el certificado existente. La referencia a verificar un primer certificado utilizando un segundo certificado se entenderá como autenticar o verificar la clave pública del primer certificado con la clave pública del segundo certificado aplicando la clave pública del segundo certificado a una firma en el primer certificado, al menos de la clave pública del primer certificado (aunque la firma en algunos casos puede generarse para la clave pública del primer certificado junto con otros datos, por ejemplo, información del emisor o información relacionada con una autoridad de certificación externa).

En la presente descripción, "verificar", "validar" o "autenticar" datos o un certificado utilizando un certificado debe entenderse como una forma abreviada de referirse a un proceso de verificar una firma digital asociada o adjunta a los datos o certificado mediante el procesamiento de la firma digital utilizando una clave pública asociada con el certificado en un algoritmo de verificación de firma. De manera similar, verificar, validar o autenticar una firma digital (de datos, un certificado o de otra manera) debe leerse de manera análoga. La persona experta en el campo de las firmas digitales y los certificados digitales, más generalmente en el campo de la autenticación de datos o documentos digitales, o incluso más generalmente en los campos de seguridad de datos y criptografía, está familiarizada con los términos mencionados anteriormente, así como con los términos "clave pública" y "clave privada" en relación con la criptografía asimétrica.

Según la invención, se proporciona un sistema de recepción de radiodifusión según la reivindicación 1 que comprende un receptor para recibir una señal de radiodifusión digital y un procesador. El procesador está configurado para verificar un certificado digital actual extraído de una señal de difusión digital utilizando un certificado digital anterior previamente almacenado como confiable. Los certificados digitales actuales y anteriores están asociados con firmas digitales con las cuales los datos recibidos con la señal de difusión han sido firmados. El certificado digital actual ha sido firmado con una clave privada asociada a un certificado anterior.

Al firmar un certificado actual con una clave privada asociada a un certificado anterior, al emitirse el certificado actual, la confianza acumulada en el certificado anterior puede transferirse al certificado actual verificando el certificado actual utilizando el certificado anterior (siempre y cuando al menos uno de los certificados anteriores almacenados como confiables por el sistema sea parte de un conjunto de certificados anteriores con los que el certificado actual ha sido firmado). De esta manera, se reduce o elimina el período requerido para confiar en un nuevo certificado después de un cambio de certificado y se reduce o incluso elimina el riesgo de un ataque de intermediario utilizando un certificado pirata como consecuencia.

Además, de acuerdo con la modalidad, se puede construir y mantener la confianza sin la necesidad de que los certificados o claves criptográficas se carguen previamente en el sistema en la etapa de fabricación para autenticar los datos recibidos por el dispositivo del usuario. Por lo tanto, puede que no sea necesario contar con una autoridad de certificación global que proporcione confianza en los certificados para permitir la autenticación de los datos recibidos.

Según la invención, el procesador está configurado para:

extraer el certificado digital actual de la señal de difusión;
realizar una primera determinación si el certificado digital extraído ha sido previamente almacenado como confiable;
si la primera determinación es negativa, realizar una segunda determinación si se ha almacenado un certificado digital anterior del mismo emisor como confiable;
si la segunda determinación es positiva, utilizar el certificado digital anterior almacenado para realizar una tercera determinación si el certificado extraído es válido verificando el certificado digital extraído utilizando una clave pública respectiva asociada con el certificado digital anterior almacenado como confiable; y,
si la tercera determinación es positiva, almacenar el certificado digital extraído como confiable.

El procesador está, en algunas modalidades, adicionalmente configurado para:

extraer los datos de la señal de difusión;
si la primera determinación es positiva, utilizar la clave pública asociada con el certificado digital extraído para verificar la firma digital de los datos; y,

si la tercera determinación es positiva, utiliza la clave pública asociada con el certificado digital extraído para verificar la firma digital de los datos.

Los datos pueden ser firmados utilizando una clave privada y el certificado digital actual puede estar asociado con la clave privada para identificar al propietario de la clave privada (emisor del certificado) y con una clave pública para verificar la firma digital. El certificado digital actual puede haber sido emitido utilizando una o más claves privadas asociadas con certificados digitales anteriores emitidos por el emisor, lo cual puede incluir la firma digital de la clave pública asociada por separado con cada una de las una o más claves privadas.

Los datos pueden ser extraídos en respuesta a una solicitud de un usuario u otro disparador, o los datos pueden ser extraídos periódicamente para ser almacenados en el sistema, por ejemplo, en la memoria de un televisor o decodificador. Donde el certificado actual ya ha sido almacenado, el certificado extraído puede ser utilizado ya sea utilizándolo directamente o utilizando la versión almacenada del mismo, por supuesto.

El procesador puede estar configurado para realizar una tercera determinación positiva si una clave pública asociada con cualquiera de una pluralidad de certificados digitales anteriores que se han almacenado como confiables verifica correctamente la firma digital actual. Si el sistema ha estado fuera de línea durante algún tiempo, por ejemplo, porque el usuario ha estado de vacaciones, es posible que se haya perdido un cambio intermedio de certificado. Al permitir la autenticación utilizando cualquiera de una serie de certificados anteriores, la confianza acumulada en los certificados anteriores no se pierde en tales casos, siempre y cuando uno de los certificados anteriores almacenados como confiables se haya utilizado para firmar el certificado actual. Con este fin, el certificado digital actual puede haber sido firmado digitalmente con una pluralidad de claves privadas asociadas con respectivos certificados anteriores para crear firmas digitales respectivas (que pueden ser referidas colectivamente como una firma), de modo que la firma digital (es decir, cada firma respectiva) pueda ser verificada con cualquiera de una pluralidad de claves públicas respectivas asociadas con los respectivos certificados anteriores. Por ejemplo, el certificado digital actual puede estar asociado con una pluralidad de firmas digitales, cada una asociada con un certificado anterior respectivo, de manera que, si se utiliza cualquiera de estos certificados anteriores para la autenticación del certificado actual, una de las firmas digitales validará / descifrará correctamente y el certificado actual será reconocido como confiable.

En algunas modalidades, si la segunda determinación es negativa y no se ha extraído previamente ningún certificado del mismo emisor por el sistema (o más generalmente, cada vez que se extrae un certificado por primera vez para un emisor, por ejemplo, independientemente de cualquier otra determinación), el certificado extraído puede ser almacenado como confiable. Esto proporciona una forma de confiar inicialmente en un certificado ya sea en un modo de inicio del sistema cuando no hay certificados confiables anteriores en el sistema, o cuando se extrae por primera vez un certificado para un nuevo emisor (difusora, canal, servicio, ...). Para que un ataque de intermediario sea exitoso en estas circunstancias, tendría que estar sincronizado precisamente con el momento de la primera extracción del certificado, cuya probabilidad se espera que sea baja en la mayoría de las circunstancias.

El sistema puede configurarse para generar una señal de advertencia de certificado, lo cual podría resultar en la visualización de una advertencia, el bloqueo de datos de aplicación, otros contenidos o su uso, u otras acciones en respuesta a la advertencia. Se puede generar una advertencia de certificado si la segunda determinación es negativa, por ejemplo.

El sistema puede configurarse para extraer periódicamente el certificado actual de la señal de difusión y almacenar el certificado extraído como confiable si ha sido extraído de manera consistente durante un número predeterminado de veces y/o durante un tiempo predeterminado. La consistencia puede ser medida por cualquier criterio adecuado, por ejemplo, que cada certificado extraído sea idéntico al previamente extraído. De esta manera, la confianza en el certificado puede ser establecida si se recibe de manera constante en la señal de difusión durante un período prolongado de tiempo, por ejemplo, un día, unos días, una semana, semanas, un mes o varios meses. Sin embargo, se puede observar que, siempre y cuando un certificado anterior confiable que también se utiliza para firmar el certificado actual esté almacenado por el sistema, no será necesario seguir esta operación extendida de construcción de confianza cuando ocurra un cambio de certificado.

El sistema puede implementar un entorno interactivo HbbTV y/o puede comprender un receptor de televisión. Sin embargo, se apreciará que la presente descripción no se limita a sistemas de televisión digital, sino que también es aplicable a otros tipos de sistemas de difusión digital, que pueden ser susceptibles a un ataque de intermediario.

En una modalidad, se proporciona un sistema para firmar datos que se van a difundir junto con un certificado digital en una señal de difusión digital, por ejemplo, una señal de televisión digital. El sistema comprende un sistema de recepción de transmisiones según se describe anteriormente y un procesador configurado para firmar datos a difundir con una firma digital utilizando una clave privada, en donde el certificado digital está asociado con la clave privada propiedad del propietario de la clave privada (el emisor del certificado) y con una clave pública para verificar la firma digital. El procesador está adicionalmente configurado para firmar el certificado digital con una firma digital utilizando una o más claves privadas anteriores asociadas con certificados anteriores respectivos del emisor.

Como se explicó anteriormente, al emitir un certificado actual utilizando uno o más certificados anteriores del mismo emisor, los terminales receptores como televisores o decodificadores pueden transferir la confianza que tienen en los certificados anteriores al certificado actual sin necesidad de un período prolongado para volver a generar confianza, lo cual podría representar una oportunidad para un ataque de intermediario que introduzca un certificado pirata.

En otra modalidad, se proporciona un sistema de difusión para difundir datos de aplicación firmados y que comprende un sistema para firmar datos de aplicación como se describe anteriormente y un transmisor para transmitir una señal de difusión digital que incluye los datos firmados y el certificado digital.

Se entenderá, por supuesto, que los datos firmados y el certificado digital pueden difundirse juntos sustancialmente al mismo tiempo, por ejemplo, en los mismos o en flujos de datos paralelos. Alternativamente, los datos firmados y el certificado digital pueden difundirse de forma independiente, en diferentes momentos y/o intervalos diferentes. Cuando sea necesario para emparejar la firma y el certificado, se puede asociar un identificador, por ejemplo, que identifique al emisor del certificado, con ambos para que el certificado se pueda utilizar para verificar la firma correcta. Alternativamente, el sistema receptor puede utilizar otros medios para relacionar el certificado con las firmas, por ejemplo, el certificado puede estar adjunto o transmitido junto con la firma y los datos firmados.

Como se mencionó anteriormente, los datos pueden incluir datos de aplicación para ser utilizados por una aplicación o para cargar la propia aplicación. Los datos de la aplicación pueden incluir una URL u otra información de contacto para ser utilizada por la aplicación o para iniciar la aplicación. Los datos pueden difundirse en forma de una tabla DVB y/o pueden incluir datos en forma de un objeto o carrusel de datos; datos necesarios para ejecutar o iniciar una aplicación en forma de un objeto o carrusel de datos; o una tabla que incluye una URL con un enlace a una ubicación donde encontrar una aplicación relacionada. Los datos pueden estar en forma de una tabla de información de aplicación (AIT) de DVB y/o pueden incluir uno o más de los siguientes: datos de audio, datos de vídeo, subtítulos, datos de superposición de pantalla y contenido relacionado con datos de audio y vídeo transmitidos o bajo demanda.

En otros aspectos, se proporciona un método según la reivindicación 13.

Breve descripción de la figura

Se describirán ahora modalidades, a modo de ejemplo e ilustración, con referencia a los dibujos adjuntos, en los cuales:

La Figura 1 ilustra un sistema de televisión interactivo que comprende una difusora y un televisor ilustrativo como receptor;
La Figura 2 ilustra un ataque de hombre en el medio en el sistema de televisión interactiva.
La Figura 3 ilustra una televisión interactiva que comprende datos firmados digitalmente y un ataque de intermediario en dicho sistema;
La Figura 4 ilustra una difusora en el sistema de televisión interactiva;
La Figura 5 ilustra un receptor en el sistema de televisión interactiva;
La Figura 6 ilustra un proceso de firma digital implementado por la difusora;
La Figura 7 ilustra una visión general de un proceso de verificación de firma implementado por el receptor;
La Figura 8 ilustra un proceso de verificación de firma con verificación de certificado sincrónico;
La Figura 9 ilustra un proceso de verificación de certificado asíncrono;
La Figura 10 ilustra detalles del procesamiento de certificados en la Figura 9; y
La Figura 11 ilustra la operación de los procesos descritos a medida que un certificado cambia varias veces a lo largo del tiempo.

Descripción detallada

Con referencia a la Figura 3, una difusora 100 transmite, junto con datos audiovisuales y canales de televisión, datos como datos de aplicación y certificados con los cuales se han firmado los respectivos elementos de datos, como se explica en detalle a continuación. Principalmente, la descripción se realiza en términos de un certificado actual, que es el certificado actual para un emisor dado (propietario de una clave privada correspondiente). Se entenderá que en la práctica una difusora puede transmitir un número de certificados actuales para emisores respectivos (como se define anteriormente). Se entenderá que los certificados se procesan por separado para cada emisor y que la descripción a continuación se realiza principalmente en términos de un único certificado actual, con el fin de brindar claridad y simplicidad en la presentación.

Un receptor 200, en algunas modalidades un televisor o decodificador, recibe la señal de difusión y extrae datos y certificados de la señal de difusión. Los datos y certificados se extraen, dependiendo de la modalidad, en respuesta a un evento desencadenante como una entrada del usuario, o periódicamente para que se almacenen en caché y estén listos para su uso en el receptor 200, o ambos. Los datos pueden incluir datos superpuestos para superponer en los datos audiovisuales recibidos, o datos de aplicación como páginas HTML con aplicaciones incrustadas o URL

para ser utilizados por aplicaciones cargadas en el receptor 200 para acceder a información a través de Internet (u otra red de comunicaciones) 300, o para iniciar una aplicación, por ejemplo, utilizando un URL. El receptor 200 autentica los datos extraídos utilizando certificados extraídos o almacenados y también verifica la confianza en los certificados utilizados para la autenticación, como se describe en detalle a continuación.

Un pirata 400 llevando a cabo un ataque de intermediario se muestra con líneas discontinuas en la Figura 3. El pirata 400 recibe los datos de difusión y el certificado, y transmite un certificado pirata y datos manipulados firmados con el certificado pirata al receptor 200. Por ejemplo, los datos pueden incluir una URL para una aplicación de malware que reemplace una aplicación proporcionada por la difusora. Si el atacante tiene éxito, el receptor 200 autenticaría los datos piratas utilizando el certificado pirata y luego accedería a la aplicación de malware a través de Internet 300 en lugar de la aplicación de la difusora. Para protegerse contra este tipo de ataque, la difusora 100 ha firmado digitalmente el certificado actual con uno o más certificados anteriores que pueden ser confiables para el receptor 200 y, correspondientemente, el receptor 200 utiliza certificados previamente confiables para validar el certificado actual, por ejemplo, para distinguir un cambio por parte de la difusora 100 a un nuevo certificado de un certificado modificado debido a un ataque de intermediario. Esto se describirá en detalle a continuación.

Con referencia a la Figura 4, la difusora 100 comprende un subsistema de gestión de contenido 102 que incluye un procesador 104 y un subsistema de difusión 106. El subsistema de gestión de contenido 102 está configurado para preparar contenido y datos para la difusión por el subsistema de difusión 106, incluyendo la firma digital de los datos y el certificado utilizado para firmar los datos, como se describe en detalle a continuación. Se apreciará que la difusora 100, el subsistema de gestión de contenido 102 y el subsistema de difusión 106 incluirán en la práctica muchos más componentes, incluyendo arreglos de servidor-cliente, bancos de memoria, interfaces de red, interfaces de usuario para permitir la intervención del usuario, acondicionadores de señal, multiplexores, equipos de difusión, etc., cuyos detalles y funciones serán bien conocidos por una persona experta en la materia y que se omiten en la presente discusión por claridad de presentación. Por ejemplo, una arquitectura típica puede involucrar una infraestructura de cabecera conectada a una variedad de servidores de datos y proporcionando señales para su difusión a través de un medio de transmisión adecuado, como aire, satélite o cable. En algunas modalidades, la difusora 100 puede estar dispuesta para difundir señales y poner datos y otras aplicaciones disponibles a través de Internet 300 mediante la implementación de un estándar HbbTV, por ejemplo, HbbTV 1.5 o 2.0 (ver por ejemplo la Especificación HbbTV 2.0, 01-05-2015, disponible en línea en https://www.hbbtv.org/pages/about hbbtv/HbbTV_specification_2_0.pdf). En algunas de estas modalidades, los datos de la aplicación, como las URL de la aplicación, los carruseles de objetos o datos, se transmiten en formato DVB AIT.

En algunas modalidades, el subsistema de gestión de contenido 102, específicamente el procesador 104, está configurado para firmar digitalmente datos de aplicación y crear certificados con una clave pública para la verificación de firmas creadas con una clave privada correspondiente de acuerdo con, por ejemplo, el estándar FIPS 186-4 (ver http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf). Los certificados se generan y formatean, en algunas modalidades, de acuerdo con el estándar X.509, como se especifica en el RFC5280 (disponible en línea en https://tools.ietf.org/html/rfc5280). En algunas modalidades, las firmas digitales se crean utilizando los algoritmos DSA o ECDSA (ver http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).

Con referencia a la Figura 5, el receptor 200, por ejemplo, un televisor o un decodificador, comprende una parte receptora 202 para recibir la señal de difusión, decodificar y demultiplexar la señal de difusión y extraer diversos datos y flujos de audio/video de la señal de difusión, como será bien conocido por la persona experta en la materia. El receptor puede estar configurado para recibir señales de difusión por aire, de uno o más satélites o a través de cable. El receptor 200 además comprende una interfaz de red 204 para la conexión con internet, una red de área amplia y/o una red de área local, por ejemplo, a través de una conexión cableada, Wi-Fi, Bluetooth u otra conexión. El receptor, en algunas modalidades, implementa un enfoque híbrido, por ejemplo, implementando el estándar HbbTV, con audio/datos y otros datos recibidos tanto de una señal de difusión como a través de una red como Internet. Una memoria 206 almacena datos (datos de audio/video y datos relacionados como superposiciones de pantalla, subtítulos, diferentes flujos de audio, datos de aplicaciones, datos de usuario, etc.) recibidos a través de la señal de difusión o conexión de red y datos procesados. Un procesador 208 procesa flujos de datos recibidos para extraer y procesar datos, audio/video, aplicaciones u otros datos, y almacena los datos en la memoria 206. El procesador 208 está adicionalmente configurado para verificar y establecer confianza en los certificados recibidos a través de la señal de difusión, como se describe en detalle a continuación.

Se entenderá que el receptor 200 en la práctica tendrá muchos otros componentes, que no son centrales para la presente descripción y por lo tanto se han omitido en aras de la claridad de la presentación y la concisión. Tales componentes variarán dependiendo del tipo específico de receptor (TV, radio, híbrido que incluye conexión de red integrada, decodificador, televisor, etc.), pero pueden incluir un generador de pantalla; una pantalla; una segunda pantalla u otro dispositivo auxiliar; un módulo de red para acceder a dicho dispositivo de "segunda pantalla", por ejemplo, una tableta o un teléfono móvil, a través de Bluetooth o Wi-Fi; circuitos de procesamiento de entrada de usuario, un dispositivo de entrada de usuario como un control remoto o un teclado; componentes de procesamiento adicionales, detallados, separados e interactivos, como un procesador de vídeo dedicado, un módulo de seguridad y/o acceso condicional dedicado; y así sucesivamente. Se entenderá en general que los componentes descritos anteriormente con referencia a la Figura 5 (así como las Figuras 3 y 4) se describen como agrupaciones funcionales

/ lógicas y que en la práctica pueden implementarse en diversas estructuras, hardware, microprograma y software, combinados entre sí o divididos entre diferentes unidades de procesamiento físicas, procesadores y/o dispositivos.

En algunas modalidades, cuando el receptor 200 es adquirido por el usuario, no hay certificados ni claves criptográficas precargadas en el receptor en la etapa de fabricación o venta al por menor que puedan ser utilizados para autenticar los datos de la aplicación recibidos por el dispositivo del usuario. El receptor 200, una vez conectado a una red de difusión, construye su propia confianza en los datos recibidos. Como se describirá en detalle a continuación, en algunas modalidades esto se realiza adquiriendo certificados transmitidos, por ejemplo, a través del aire, y almacenándolos en el receptor 200. Puede haber muchos canales/servicios o paquetes de canales/servicios o uno por país, dependiendo de la configuración específica de la red de difusión, de manera que el receptor 200 típicamente no puede confiar globalmente en una autoridad de certificación externa. El receptor 200, en algunas modalidades, confiará en un certificado cuando el mismo certificado se utilice durante un período de tiempo predefinido, o si un certificado recién introducido está firmado con el anterior, como se detalla a continuación.

Pasando ahora a algunos procesos implementados por los componentes descritos anteriormente, y comenzando con los procesos de extremo de cabeza (o aguas arriba) en el lado de la difusora 100, se describe ahora un proceso para preparar datos para su difusión de manera que puedan ser autenticados por el receptor 200, haciendo referencia a la Figura 6. En el paso 112, un certificado actual (que es un certificado con una clave pública que se utilizará para verificar los datos de difusión en el receptor) se firma a sí mismo con una o más claves privadas asociadas con certificados anteriores (es decir, claves que han sido utilizadas por la difusora 100 -el canal, programa, servicio, etc.- en el pasado para firmar datos transmitidos mientras se utilizaba un certificado anterior respectivo) para permitir la transferencia de confianza de certificados anteriores a actuales por parte del receptor 200, como se describe en detalle a continuación. En las modalidades en las que el certificado actual está firmado con dos o más claves privadas asociadas con certificados anteriores respectivos, esto permite ventajosamente que el receptor 200 transfiera la confianza de un certificado anterior más antiguo al certificado actual si se perdió un certificado intermedio, por ejemplo, cuando el receptor 200 estuvo apagado durante algún tiempo. En algunas de estas modalidades, el certificado actual se firma por separado con cada una de estas claves privadas (por ejemplo, las claves privadas asociadas con los últimos seis certificados anteriores) para crear un número correspondiente de firmas respectivas que se utilizan para emitir el certificado actual (se incluyen en el certificado actual).

En el paso 114, se utiliza la clave privada asociada con el certificado actual para firmar los datos que se van a difundir, de manera que luego estén listos para su difusión. Los datos se transmiten luego en el paso 116. El proceso puede volver al paso 114 para preparar datos adicionales para la difusión utilizando la clave privada asociada con el certificado actual, o al paso 112 para cambiar periódicamente la clave privada y el certificado, por ejemplo, una vez al mes, momento en el cual el certificado actual se convierte en un certificado anterior según se utiliza aquí, y se utiliza un nuevo certificado actual para verificar los datos de difusión. Esto ayuda a prevenir un ataque de intermediario incluso si el pirata 400 puede modificar la señal durante un largo período de tiempo, ya que el pirata 400 puede no ser capaz de firmar un certificado pirata utilizando la clave privada de un certificado válido anterior, a menos que el pirata haya obtenido de alguna manera acceso a dicha clave privada.

Se entenderá que, en particular, el orden de los pasos 112 y 114 puede invertirse, aunque típicamente será eficiente emitir un certificado de corriente solo una vez, mientras se puede utilizar para firmar muchas instancias de datos durante su período de validez. Se entenderá además que el paso 112, 114 y 116, y en particular los pasos 114 y 116, pueden ser llevados a cabo por diferentes entidades que cooperan para transmitir datos que pueden ser autenticados. Con respecto al paso 116, se entenderá que, si bien, en algunas modalidades, los datos pueden siempre transmitirse junto con el certificado asociado a su firma digital, esto no es necesariamente así y, en algunas modalidades, el certificado actual solo puede difundirse una vez o unas pocas veces después de un cambio de certificado o, en general, puede difundirse periódicamente de forma independiente de los datos que se han firmado.

Con referencia a la Figura 7, se describe ahora un proceso general para la autenticación de los datos recibidos por el receptor 200. En el paso 212, se extraen los datos firmados digitalmente y el certificado correspondiente de una señal de difusión. Como se describe anteriormente, esto se puede hacer al mismo tiempo tanto para los datos como para el certificado, o los dos pueden extraerse de forma independiente, como se describe anteriormente en relación con la preparación y transmisión de datos firmados por la difusora. Sin embargo, se puede observar que la extracción de datos y el certificado en el paso 212 pueden estar desacoplados, incluso si ambos siempre se transmiten juntos. En el paso 214, el receptor 200 verifica si el certificado extraído es confiable y, en caso afirmativo, utiliza el certificado para verificar la firma de los datos con el certificado, extraído o almacenado, según corresponda, en el paso 216. Si el resultado de la verificación es positivo, se concede acceso a los datos (por ejemplo, mostrando los datos o utilizándolos para acceder y/o cargar una aplicación), de lo contrario, se puede negar el acceso y/o generar una advertencia de fallo de autenticación, por ejemplo, para mostrarla. Si el certificado extraído no es confiable, se activa una acción de advertencia de certificado en el paso 218, como se describe más adelante.

Ahora se describe un proceso para extraer y verificar un certificado al mismo tiempo que los datos asociados, con referencia a la Figura 8. En el paso 220, se extraen los datos firmados y la firma correspondiente de la señal de difusión. En el paso 222 se determina si el certificado extraído ha sido previamente confiable (por ejemplo, si coincide con un certificado previamente almacenado como confiable o se identifica de otra manera, por ejemplo,

mediante un código de identificación), y, en caso afirmativo, el certificado se utiliza en el paso 224 para verificar la firma de los datos y autenticar los datos como se describe anteriormente. Si la determinación es negativa, entonces se determina, en el paso 226, si se ha confiado en una versión anterior del certificado (por ejemplo, previamente almacenada como confiable por el receptor 200, como estar presente en una lista de certificados almacenados previamente). Si es así, el certificado extraído se verifica en el paso 228 con uno o más certificados anteriores, de lo contrario se activa una acción de advertencia de certificado en el paso 230.

Centrándonos en más detalle en el paso 228, el receptor 200 examina la firma (o firmas) generada por la difusora 100 al emitir el certificado actual (y recibida junto con el certificado / adjunta a él), intentando verificar cada firma con el certificado anterior o más certificados para el mismo emisor almacenados como previamente confiables y/o en una lista de certificados previamente confiables mantenida por el receptor 200, en algunas modalidades comenzando con el certificado anterior más reciente. Si alguno de estos certificados anteriores verifica una de las firmas del certificado actual extraído (es decir, la clave pública asociada con al menos uno de los certificados anteriores verifica correctamente una de las firmas), se considera que el certificado extraído es válido. Si, en el paso 232 se ha determinado que el certificado extraído es válido, la firma de los datos se verifica como se describe anteriormente con referencia, por ejemplo, al paso 216, y el certificado actual se almacena como confiable en el paso 234. En modalidades que mantienen una lista de certificados anteriores confiables, la lista se actualiza en el paso 236 con el certificado anterior ahora agregado a la lista (habiendo sido reemplazado por el certificado actual). De lo contrario, si la determinación en el paso 232 es negativa, el proceso vuelve al paso 230 para activar una acción de advertencia de certificado.

Una acción de advertencia de certificado, como la activada en el paso 216 o 230, comprende, según la modalidad y el diseño de la interfaz de usuario, uno o más de los siguientes:

- generando una señal para provocar la visualización de un mensaje de advertencia, enviando dicha señal a través de una red y/o mostrando el mensaje de advertencia;
- en el caso de datos para el lanzamiento de una aplicación, bloquear el acceso o el lanzamiento de la aplicación;
- en el caso de datos para ser utilizados por una aplicación, bloqueando el acceso a los datos;
- en caso de que el contenido se muestre junto con, por ejemplo, un flujo de audio/video, bloqueando la visualización del contenido;
- Si el receptor 200 está en modo de configuración, marque o guarde el certificado como confiable: el modo de configuración puede estar activo si, por ejemplo,

    - el certificado es la primera instancia de un certificado extraído para el emisor del certificado;
    - el receptor 200 ha sido iniciado por primera vez;
    - el certificado es el primer certificado, para el emisor o en general, recibido después de un reinicio;
    - ocurrió un primer o reinicio dentro de un período predeterminado antes de que se extrajera el certificado;
    - el receptor 200 o, específicamente, su función de gestión de certificados ha sido reiniciada manualmente por un usuario o de otra manera.

Con referencia a la Figura 9, se describe ahora un proceso asíncrono para verificar certificados que puede ejecutarse de forma independiente a la extracción de datos firmados. Un proceso de este tipo puede ejecutarse periódicamente y mantener un almacén o lista de un certificado actual confiable y de certificados anteriores confiables, de manera que la verificación en el paso 214, anteriormente mencionado, pueda simplificarse a una prueba de si el certificado extraído ha sido almacenado o marcado como confiable previamente por el receptor 200. Por supuesto, este proceso se puede combinar con el proceso recién descrito con referencia a la Figura 8. Específicamente, en el paso 238, se extraen los certificados de la señal de difusión y cada certificado extraído se procesa en el paso 240 para verificar la confianza en él. Se entenderá que en algunas modalidades se extrae y procesa un certificado antes de que se procese y extraiga el siguiente, efectivamente entrelazando los pasos 238 y 240. El proceso espera durante un período de tiempo en el paso 242 y luego ocurre otra ronda de procesamiento. De esta manera, los certificados se extraen y procesan periódicamente, por ejemplo, una vez al día. Se entenderá que son posibles varios horarios, por ejemplo, escalonando la extracción y el procesamiento por emisores, manteniendo una lista de emisores para los cuales se deben extraer certificados (por ejemplo, para que solo se extraigan certificados de emisores para los cuales ya se solicitó información / certificados, por ejemplo, cuando una demanda del usuario activó el paso 220 y los siguientes pasos en el pasado), y así sucesivamente.

El procesamiento en el paso 240 de uno de los certificados extraídos puede comprender uno o más, según la modalidad, de los pasos del proceso ahora descritos con referencia a la Figura 10, donde se observará en particular que el orden y la combinación de los pasos pueden variar de una modalidad a otra. En el paso 244 se determina si el certificado extraído es confiable, como se describe anteriormente, y si es así, el procesamiento de ese certificado se detiene en el paso 246 y el proceso vuelve a procesar el siguiente certificado. Si la extracción es la primera vez que se extrae un certificado para el emisor, como se determina en el paso 248, por ejemplo, mediante una referencia cruzada con una lista de emisores para los cuales se ha extraído al menos un certificado en el pasado, entonces el certificado extraído se almacena como confiable en el paso 250 y el proceso vuelve para el siguiente certificado que se va a procesar y/o extraer. De lo contrario, en el paso 252, se determina si el certificado extraído ha sido firmado

por la difusora 100 con un certificado anterior del mismo emisor (como se describe anteriormente, por ejemplo). Si la determinación es positiva, el certificado extraído se almacena como confiable en el paso 254 y se actualiza una lista de certificados previamente confiables para el emisor en consecuencia en el paso 256, como se describe anteriormente, y el proceso vuelve para el siguiente certificado a ser procesado y/o extraído.

Si la determinación en el paso 252 también es negativa, el paso 258 prueba si el certificado es el mismo que el último extraído para el mismo emisor (por ejemplo, verificando en una lista que contiene para cada emisor el último certificado extraído) y, de ser así, incrementa un contador de extracción mantenido para el certificado extraído en el paso 260 (entendiéndose que si un emisor emite varios certificados, por ejemplo, para diferentes servicios o canales, este paso puede modificarse para verificar la última extracción de un certificado del mismo emisor para, por ejemplo, el mismo servicio o canal). El paso 262 verifica si el contador cumple una condición de umbral y, si es así, almacena el certificado extraído como confiable en el paso 264 y actualiza una lista de certificados anteriores en el paso 266, por ejemplo, como se describe anteriormente, y el proceso vuelve para el siguiente certificado a ser procesado y/o extraído. De lo contrario, si no se cumplen las condiciones de umbral, el procesamiento se detiene para este certificado en el paso 268 y el proceso vuelve a procesar el siguiente certificado extraído (o a extraer el siguiente certificado para su procesamiento, de acuerdo con la modalidad específica). Si la determinación en el paso 258 es negativa (es decir, ha habido un cambio en el certificado del emisor / se ha emitido un nuevo certificado por el emisor), el contador de extracción se reinicia en el paso 270 y el proceso vuelve al siguiente certificado a ser procesado y/o extraído.

Se describe ahora el funcionamiento del sistema y los procesos, con referencia a la Figura 11, a un nivel alto tomando como ejemplo un certificado para un emisor dado que cambia periódicamente, como cuando el emisor utiliza una nueva clave privada y emite correspondientemente un nuevo certificado, por ejemplo, una vez al mes. En un primer paso 500, en el pasado, se confiaba y utilizaba un certificado anterior N-3 para verificar los datos firmados con una clave privada correspondiente. El Certificado N-3 fue incluido así en una lista de certificados previamente confiables. En el paso 502 se ha introducido un nuevo certificado N-2 que se utiliza para firmar datos. La confianza se ha transferido del certificado N-3 al certificado N-2 y el certificado N-2 se agrega a la lista de certificados previamente confiables. En el paso 504, se introduce un nuevo certificado N-1, se transfiere la confianza a él desde el certificado N-2 (o N-3) y se agrega el certificado N-1 a la lista. En el paso 506, se ha recibido un certificado de corriente N. El certificado actual está firmado por la difusora 100 con los certificados N-1, N-2 y N-3, de modo que el receptor 200 puede confiar en el certificado actual en base a cualquiera de estos certificados anteriores, como se describe anteriormente, y utilizar el certificado actual para autenticar los datos actuales en el paso 508. Un receptor 200 que ha perdido el certificado N-1, por ejemplo, debido a un largo apagado, aún puede transferir confianza desde un certificado más antiguo (N-2 o N-3) y así utilizar el certificado actual para la autenticación.

Se apreciará que el número de certificados anteriores que se deben mantener en la lista será determinado por una serie de factores de diseño, incluyendo un equilibrio entre la duración que un dispositivo puede estar apagado sin tener que pasar por un procedimiento de configuración para establecer la confianza en los certificados de un emisor dado, la longitud de las listas de certificados y los datos de firma, y el riesgo de ataque si los certificados antiguos se ven comprometidos. El número de certificados anteriores que se utilizan para la firma de un certificado actual / transferencia de confianza puede, por ejemplo, establecerse en 2, 3, 4, 5, 6 o más alto. Asimismo, se apreciará que el momento en el que se añade un certificado actual a la lista de certificados anteriores puede variar de una modalidad a otra. Por ejemplo, en algunas modalidades, un certificado actualmente confiable se agrega a la lista de certificados anteriores confiables tan pronto como ha sido verificado y es confiable, de modo que esté listo en esa lista para verificar un nuevo certificado que se reciba en el futuro. En algunas modalidades, el certificado actual puede ser agregado a esta lista solo una vez que un nuevo certificado se convierte en el certificado actual (En cuyo caso, el certificado actual, N en el ejemplo anterior, es verificado por los certificados N-2 o N-3, pendiente de agregar el certificado N-1 a la lista). Se apreciará que los tiempos intermedios y alternativos también son posibles en varias modalidades.

Diversas modificaciones, combinaciones y yuxtaposiciones de las características descritas anteriormente, que se encuentren dentro del alcance de las reivindicaciones adjuntas, ocurrirán a una persona experta en la materia. Se entenderá que si bien las modalidades descritas se describen en diferentes agrupaciones y módulos, algunas modalidades reflejan las agrupaciones descritas en términos de implementación física, posiblemente con la implementación en hardware dedicado de algunas o todas las agrupaciones y módulos, mientras que otras modalidades reagrupan las funcionalidades descritas en diferentes disposiciones físicas y se debe entender que los módulos y agrupaciones descritos son agrupaciones lógicas con el propósito de claridad en la explicación de las funciones asociadas, más que con el propósito de limitación. Por lo tanto, las funciones descritas pueden agruparse de manera diferente en agrupaciones lógicas o físicas y pueden implementarse en uno o más de software, microprograma, software intermedio o hardware según varias modalidades. Asimismo, se entenderá que los pasos del proceso descritos pueden ser reorganizados, combinados u omitidos en cierta medida y que dichos cambios serán evidentes para la persona experta que lea la descripción anterior. Se entenderá que la descripción anterior se ha realizado con el propósito de explicar diversas modalidades y técnicas reveladas, y no con el propósito de limitar el alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema de recepción de difusión que comprende un receptor (200) para recibir una señal de difusión digital y un procesador (208) configurado para:

extraer un certificado digital actual de la señal de difusión, en donde el certificado digital actual ha sido firmado digitalmente con una o más claves privadas asociadas con los respectivos certificados digitales anteriores emitidos por el emisor del certificado actual; y verificar el certificado digital actual extraído de la señal de difusión digital utilizando un certificado digital anterior almacenado previamente como confiable mediante la verificación del certificado digital extraído utilizando una clave pública respectiva asociada con el certificado digital anterior almacenado como confiable, en donde los certificados digitales actual y anterior están asociados con firmas digitales con las cuales los datos transmitidos con la señal de difusión han sido firmados,
en donde el procesador (208) está configurado para:

- realizar una primera determinación antes de verificar el certificado digital actual para determinar si el certificado digital actual extraído ha sido previamente almacenado como confiable;

si la primera determinación es negativa, realizar una segunda determinación de si se ha almacenado un certificado digital anterior emitido por el emisor como confiable;
si la segunda determinación es positiva, utilizar el certificado digital confiable previamente almacenado para realizar una tercera determinación de si el certificado digital extraído es válido, verificando el certificado digital extraído actual utilizando una clave pública respectiva asociada con el certificado digital confiable previamente almacenado; y si la tercera determinación es positiva, almacenar el certificado digital extraído actual como confiable.

2. Un sistema según la reivindicación 1, en donde el procesador (208) está configurado para:

extraer los datos de la señal de difusión, en donde los datos están firmados con una firma digital utilizando una clave privada y el certificado digital actual está asociado con la clave privada y con una clave pública para verificar la firma digital;
si la primera determinación es positiva, utiliza la clave pública asociada con el certificado digital extraído para verificar la firma digital de los datos; y, si la tercera determinación es positiva, utiliza la clave pública asociada con el certificado digital extraído para verificar la firma digital de los datos.

3. Un sistema según la reivindicación 1 o 2, en donde el procesador (208) está configurado para realizar una tercera determinación positiva si una clave pública asociada con cualquiera de una pluralidad de certificados digitales anteriores que se han almacenado como confiables verifica correctamente el certificado actual.

4. Un sistema según la reivindicación 1, 2 o 3, en donde el procesador (208) está configurado para:
si la segunda determinación es negativa y ningún certificado emitido por el emisor se ha extraído previamente por el sistema, almacenar el certificado extraído como confiable.

5. Un sistema según la reivindicación 1, 2, 3 o 4, en donde el procesador (208) está configurado para:
si la segunda determinación es negativa, generar una señal de advertencia de certificado.

6. Un sistema según cualquiera de las reivindicaciones anteriores, en donde el procesador (208) está configurado para:
extraer periódicamente el certificado actual de la señal de difusión y almacenar el certificado extraído como confiable si ha sido extraído de manera consistente durante un número predeterminado de veces y/o durante un tiempo predeterminado.

7. Un sistema según cualquiera de las reivindicaciones anteriores, en donde el sistema implementa un entorno interactivo HbbTV.

8. Un sistema para recibir y difundir datos de aplicación firmados junto con un certificado digital en una señal de difusión digital, el sistema comprende un sistema receptor de difusión según la reivindicación 1, un transmisor para transmitir la señal de difusión digital que comprende los datos firmados y el certificado digital, y un procesador (208) configurado para:
firmar los datos a difundir con una firma digital utilizando una clave privada propiedad del emisor del certificado digital, en donde el certificado digital está asociado con la clave privada y con una clave pública para verificar la firma digital; firmar el certificado digital con una firma digital utilizando una o más claves privadas anteriores asociadas con certificados anteriores emitidos por el emisor.

9. Un sistema como se reivindicó en la reivindicación 8, en donde la señal de difusión digital comprende una señal de televisión digital.

10. Un sistema según cualquier reivindicación anterior, en donde el certificado digital ha sido firmado digitalmente con una pluralidad de claves privadas asociadas con certificados anteriores respectivos, de manera que la firma digital puede ser verificada con cualquiera de una pluralidad de claves públicas respectivas asociadas con los certificados anteriores respectivos.

11. Un sistema según cualquiera de las reivindicaciones anteriores, en donde los datos comprenden datos de aplicación para ser utilizados por una aplicación, una URL o información de contacto para ser utilizados por la aplicación o para iniciar la aplicación.

12. Un sistema según cualquiera de las reivindicaciones anteriores, en donde los datos se transmiten en forma de una tabla DVB.

13. Un método de recepción de difusión que utiliza un receptor (200) para recibir una señal de difusión digital, el método comprende:

extraer un certificado digital actual de la señal de difusión, en donde el certificado digital actual ha sido firmado digitalmente con una o más claves privadas asociadas con certificados digitales anteriores emitidos por el emisor del certificado actual; y verificar el certificado digital actual extraído de la señal de difusión digital utilizando un certificado digital anterior almacenado previamente como confiable mediante la verificación del certificado digital extraído utilizando una clave pública respectiva asociada con el certificado digital anterior almacenado como confiable, en donde el certificado digital actual y el certificado digital anterior están asociados con firmas digitales con las cuales se ha transmitido datos con la señal de difusión, en donde se realiza una primera determinación de si el certificado digital actual extraído ha sido almacenado previamente como confiable, antes de verificar el certificado digital actual,
y en donde:

si la primera determinación es negativa, se realiza una segunda determinación de si se ha almacenado como confiable un certificado digital anterior emitido por el emisor;
si la segunda determinación es positiva, utilizar el certificado digital confiable previamente almacenado para realizar una tercera determinación de si el certificado digital actual extraído es válido, verificar el certificado digital actual extraído utilizando una clave pública respectiva asociada con el certificado digital confiable previamente almacenado; y si la tercera determinación es positiva, almacenar el certificado digital actual extraído como confiable.

14. Un método de recibir y difundir datos de aplicación firmados para difundirse junto con un certificado digital en una señal de difusión digital, el método comprende el método según la reivindicación 13 y además comprende:

firmar los datos a difundir con una firma digital utilizando una clave privada propiedad del emisor del certificado digital, en donde el certificado digital está asociado con la clave privada y con una clave pública para verificar la firma digital;
firmar el certificado digital con una firma digital utilizando una o más claves privadas anteriores asociadas con los respectivos certificados anteriores emitidos por el emisor; y transmitir la señal de difusión digital que comprende los datos firmados y el certificado digital.

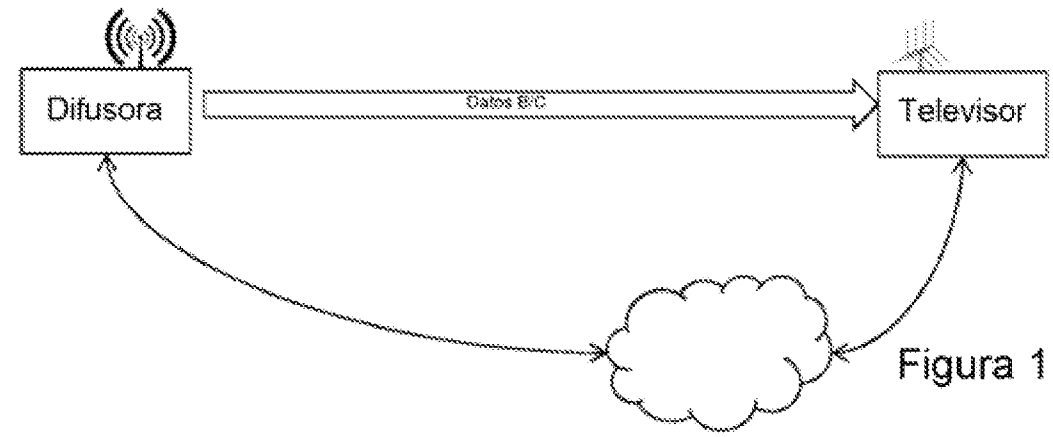

Figura 1

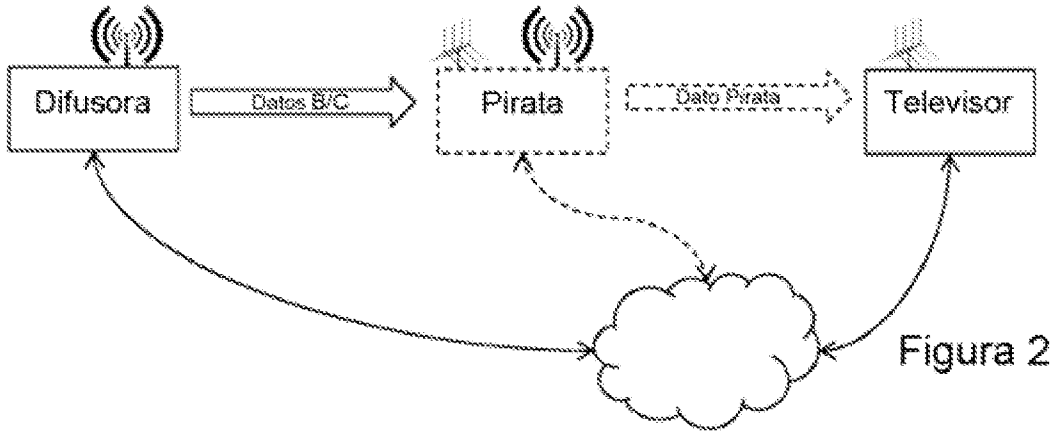

Figura 2

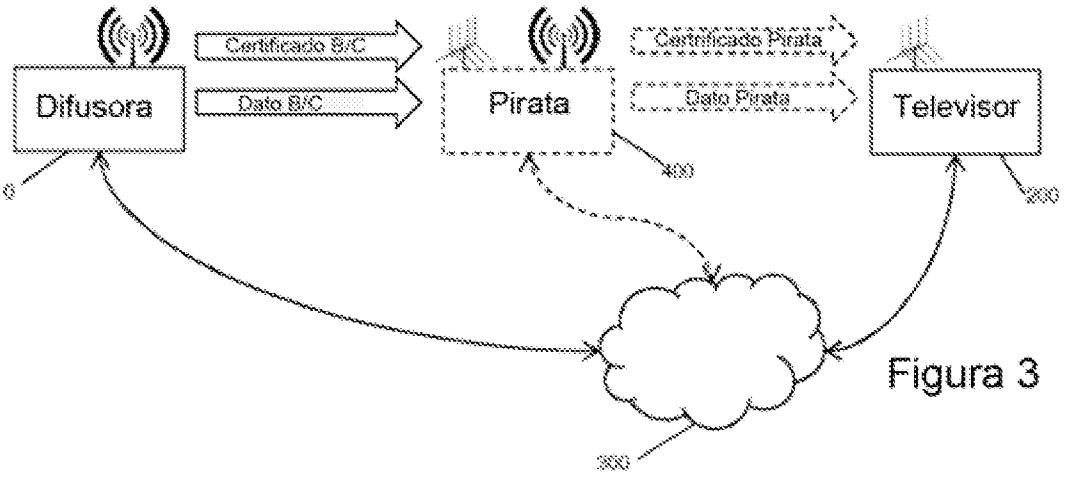

Figura 3

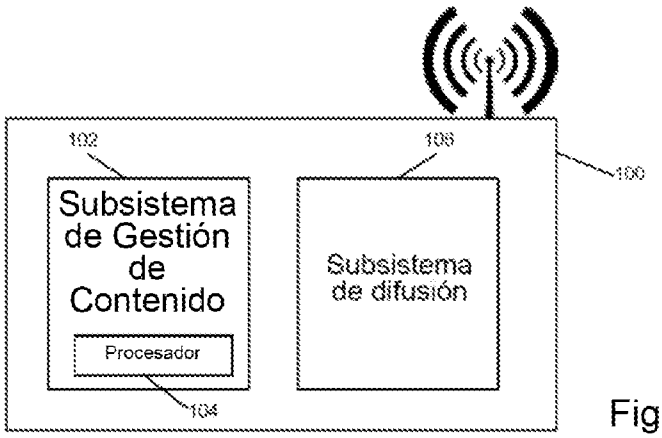

Figura 4

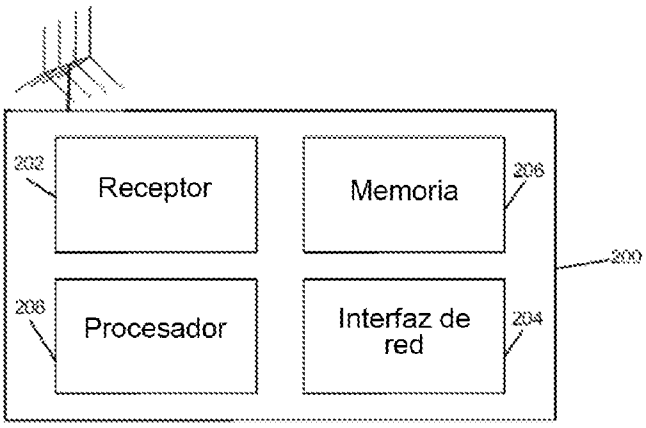

Figura 5

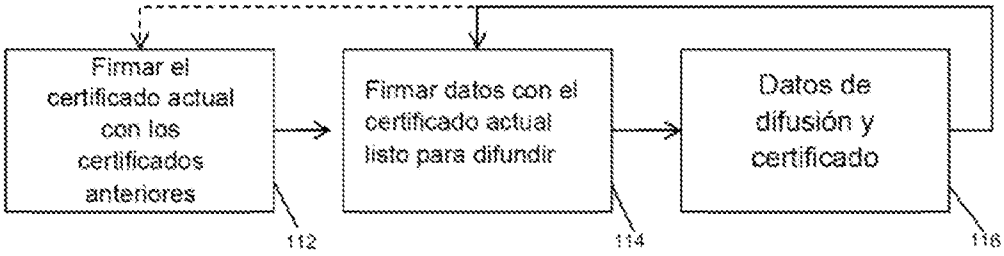

Figura 6

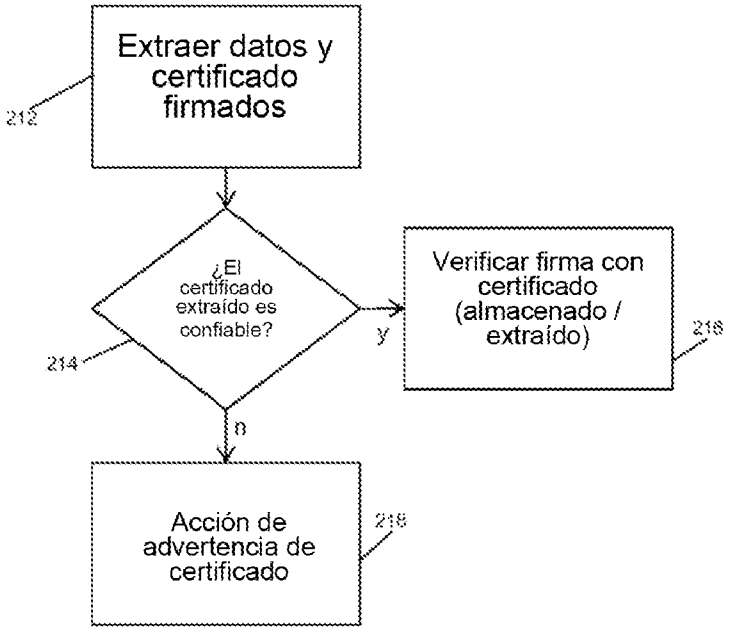

Figura 7

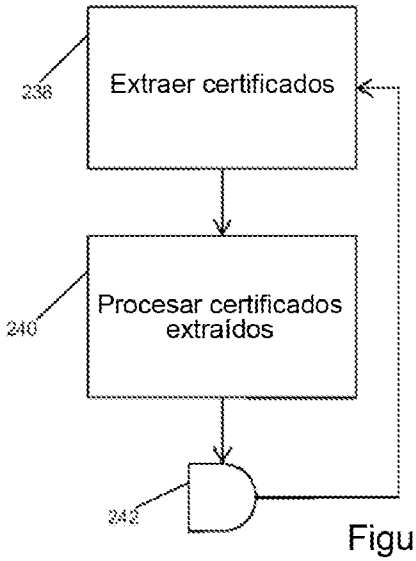

Figura 9

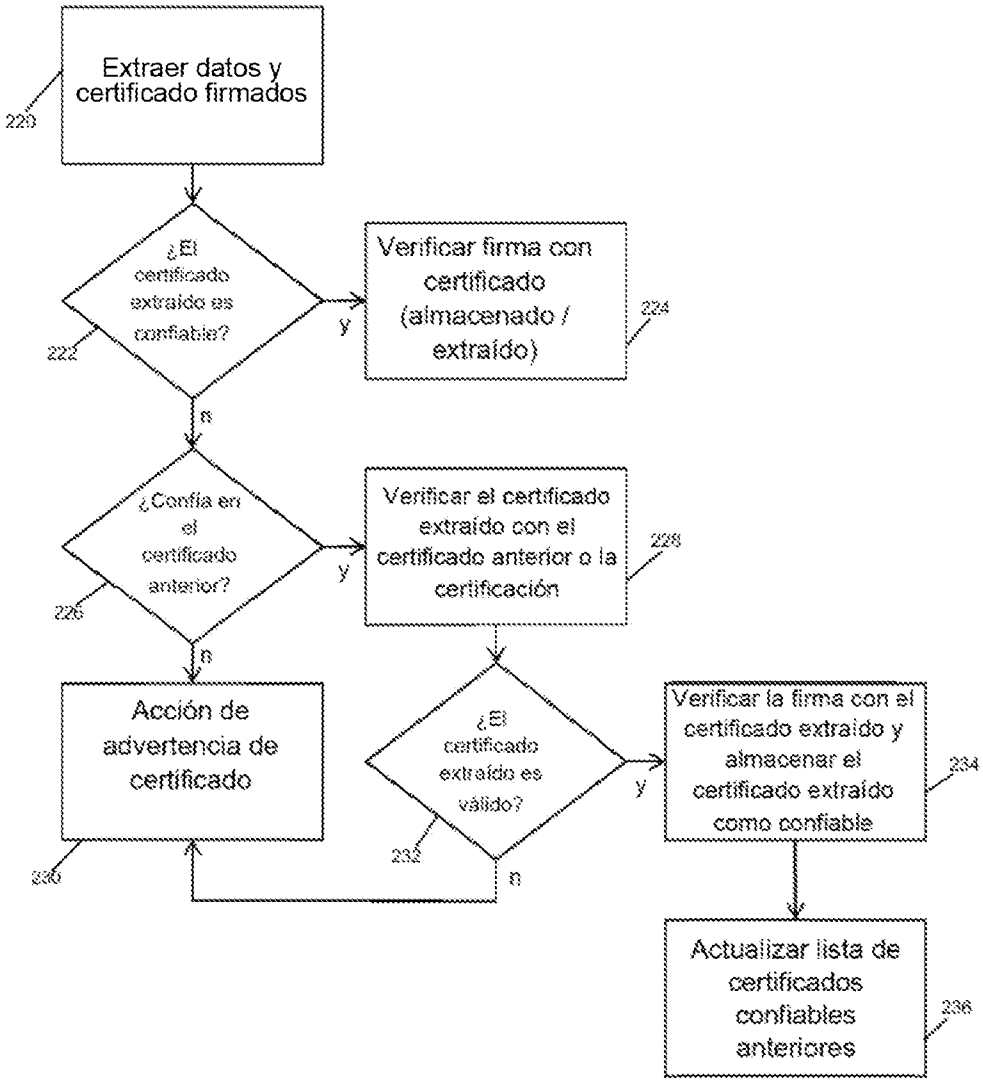
Extraer datos y certificado firmados
220
¿El certificado extraído es confiable?
222
y
Verificar firma con certificado (almacenado / extraído)
224
n
¿Confía en el certificado anterior?
226
y
Verificar el certificado extraído con el certificado anterior o la certificación
228
n
Acción de advertencia de certificado
230
¿El certificado extraído es válido?
232
y
Verificar la firma con el certificado extraído y almacenar el certificado extraído como confiable
234
n
Actualizar lista de certificados confiables anteriores
236

Figura 8

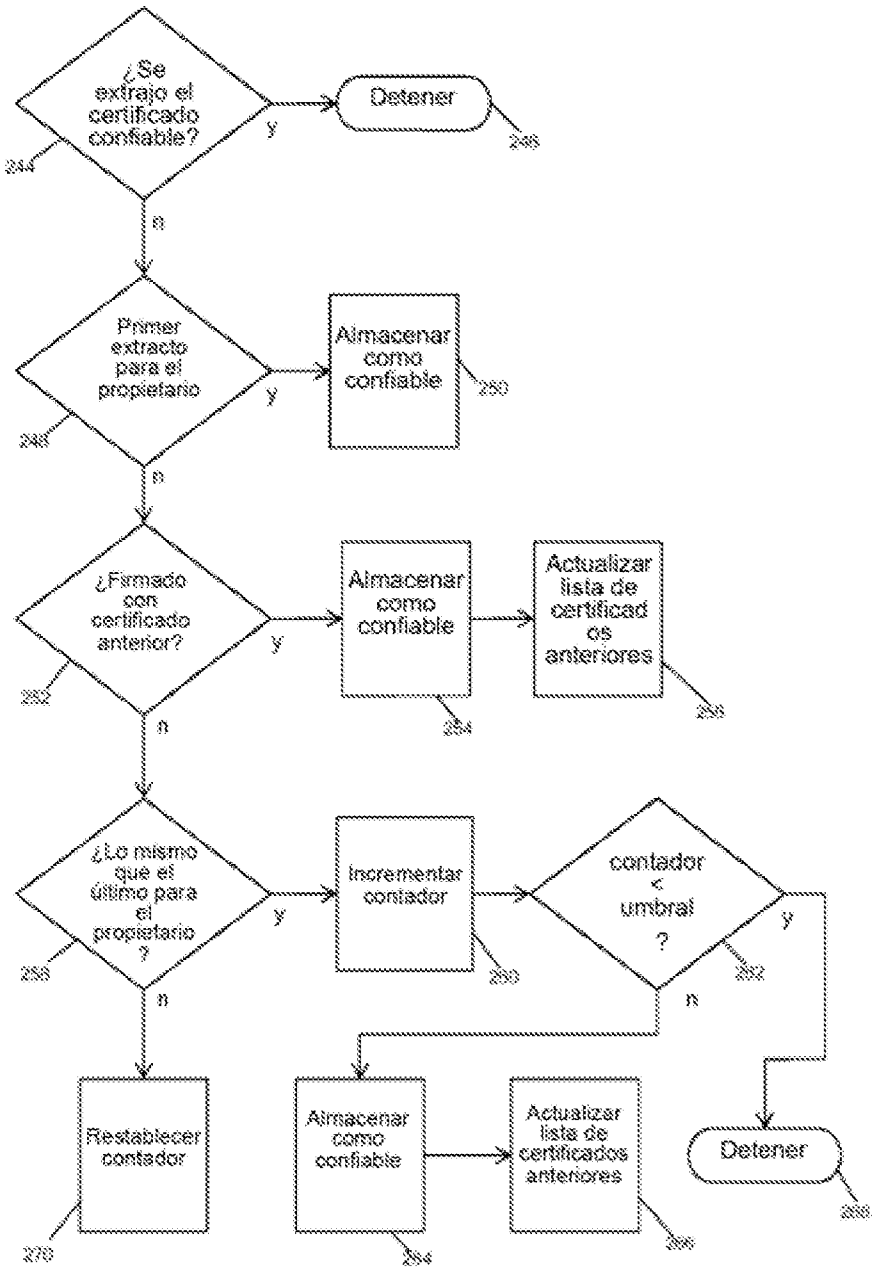
¿Se extrajo el certificado confiable?
y
Detener
246
244
n
Primer extracto para el propietario
y
Almacenar como confiable
250
248
n
¿Firmado con certificado anterior?
y
Almacenar como confiable
Actualizar lista de certificados anteriores
254
256
252
n
¿Lo mismo que el último para el propietario ?
y
Incrementar contador
contador < umbral ?
y
260
262
258
n
Restablecer contador
Almacenar como confiable
Actualizar lista de certificados anteriores
Detener
270
264
266
268

Figura 10

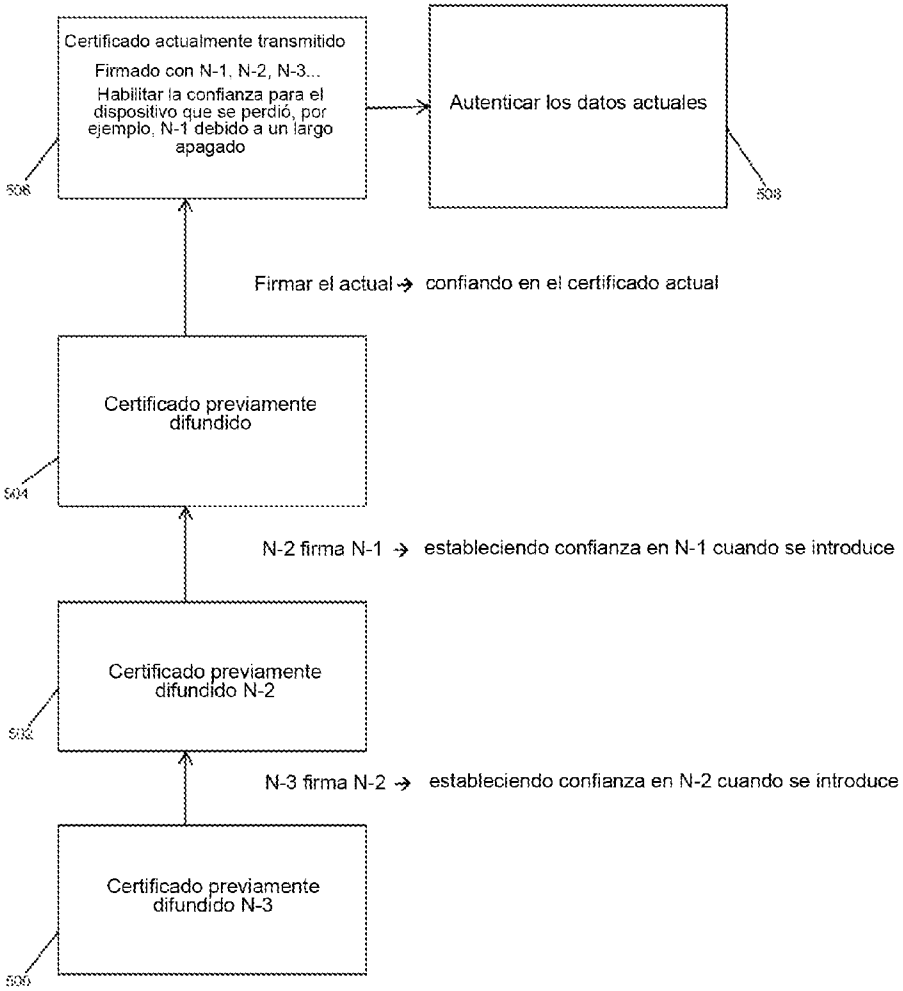
Certificado actualmente transmitido
Firmado con N-1, N-2, N-3...
Habilitar la confianza para el dispositivo que se perdió, por ejemplo, N-1 debido a un largo apagado
Autenticar los datos actuales
508
508
Firmar el actual → confiando en el certificado actual
Certificado previamente difundido
504
N-2 firma N-1 → estableciendo confianza en N-1 cuando se introduce
Certificado previamente difundido N-2
502
N-3 firma N-2 → estableciendo confianza en N-2 cuando se introduce
Certificado previamente difundido N-3
506

Figura 11