(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 359 507**

(51) Int. Cl.:
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06702917 .3**
(96) Fecha de presentación : **13.01.2006**
(97) Número de publicación de la solicitud: **1836795**
(97) Fecha de publicación de la solicitud: **26.09.2007**

(54) Título: **Método para gestionar derechos digitales en un servicio de difusión/multidifusión.**

(30) Prioridad: **14.01.2005 US 643997 P**
09.04.2005 KR 20050029717

(45) Fecha de publicación de la mención BOPI:
24.05.2011

(45) Fecha de la publicación del folleto de la patente:
24.05.2011

(73) Titular/es: **LG ELECTRONICS Inc.**
20 Yeouido-dong
Yeongdeungpo-gu, Seoul 150-721, KR

(72) Inventor/es: **Son, Sung-Mu;**
Shim, Dong-Hee;
Han, Kyu-Sung;
Shon, Min-Jung;
Kim, Te Hyun;
Lee, Seung-Jae y
Chu, Youn Sung

(74) Agente: **Curell Aguilá, Marcelino**

DESCRIPCIÓN

Método para gestionar derechos digitales en un servicio de difusión/multidifusión.

Campo técnico

La presente invención se refiere a la gestión de derechos digitales, y en particular, a un método para gestionar derechos digitales en un servicio de difusión/multidifusión de un terminal de comunicaciones móviles.

Antecedentes de la técnica

En general, un servicio de difusión/multidifusión se refiere a un servicio para proporcionar a un terminal de comunicaciones móviles, una emisión de difusión general por vía aérea o diversa información adicional, o similares. El servicio de difusión/multidifusión es un tipo nuevo de servicio que incluye un servicio de difusión general en el cual un proveedor proporciona información útil a todos los clientes que se abonan a su servicio, y un servicio de multidifusión para proporcionar información solamente a un grupo particular de clientes que se han abonado previamente a un tema o contenido particular.

Como el servicio de difusión/multidifusión puede proporcionar la misma información simultáneamente a múltiples clientes, una gestión eficaz de recursos de la red permite proporcionar una aplicación de gran ancho de banda. Además, puesto que el servicio de difusión/multidifusión proporciona varios tipos de servicios de alta velocidad de acuerdo con una solicitud del cliente, se pueden satisfacer las crecientes demandas y requerimientos de los clientes.

Para proteger de forma segura y gestionar sistemáticamente derechos con respecto al contenido proporcionado por el servicio de difusión/multidifusión, se requieren funciones de protección de servicios y protección de contenidos. La gestión de derechos digitales (DRM), que recientemente se está debatiendo de forma activa, se aplica al servicio de difusión/multidifusión para permitir la protección del contenido proporcionado por el servicio de difusión/multidifusión.

La DRM puede interceptar previamente un uso no autorizado (o ilegal) de contenido convirtiendo el contenido en unos datos cifrados de tipo paquete con el uso de una técnica de cifrado, y seguidamente permitiendo que usuarios que han completado un procedimiento de autenticación y confirmación de autorización obtengan acceso al contenido original.

Por lo tanto, en el método para gestionar derechos digitales del servicio de difusión/multidifusión de la técnica relacionada, cada terminal que utiliza el servicio recibe un objeto derechos (RO) para utilizar el servicio desde un servidor emisor de derechos (Emisor de Derechos: RI), y seguidamente utiliza el RO recibido para decodificar unos datos o contenido del servicio cifrados. En este caso, el RO se puede cifrar utilizando una clave pública de cada terminal.

Es decir, el RI debería transmitir el RO que se cifra utilizando la clave pública de cada terminal, hacia los terminales que utilizan el servicio de difusión/multidifusión. Por ejemplo, si un número K de terminales utiliza el servicio de difusión/multidifusión, el RI genera los RO, cada uno de los cuales se cifra utilizando la clave pública de cada uno del número K de terminales, y debe transmitir repetidamente los RO generados hacia todos los terminales.

Sin embargo, en el método para gestionar los derechos digitales en el servicio de difusión/multidifusión, si existen muchos terminales que utilizan el servicio, el RI debe generar/gestionar los RO cifrados que utilizan las claves públicas de cada terminal de uno en uno, lo cual da como resultado un aumento de la carga de operaciones así como un funcionamiento y una gestión ineficaces de la red.

La versión preliminar 2.0 de la especificación DRM de la *Open Mobile Alliance* (OMA) se refiere a aspectos generales del Protocolo de Adquisición de Objetos de Derechos (ROAP) en la normativa de la OMA.

Exposición de la invención

Problema técnico

Un aspecto importante de la presente invención es que los presentes inventores reconocieron ciertas deficiencias de la técnica relacionada, tal como se ha mencionado anteriormente. Como consecuencia, los presentes inventores proporcionaron una solución a dichas deficiencias, de la manera siguiente.

Un objetivo de la presente invención es proporcionar un método para gestionar derechos digitales de un servicio de difusión/multidifusión capaz de gestionar eficazmente derechos digitales con respecto a un grupo de terminales de comunicaciones móviles que utilizan el mismo servicio.

Otro objetivo de la presente invención es proporcionar un método para gestionar derechos digitales de un servicio de difusión/multidifusión capaz de gestionar eficazmente derechos digitales para un grupo de terminales de comunicaciones móviles que utilizan el mismo paquete de servicios.

Solución técnica

Según un primer aspecto de la presente invención, según la reivindicación 1, se proporciona un método de gestión de derechos digitales para un servicio de difusión general-multidifusión, en el que el método se realiza por medio de un terminal.

Según un segundo aspecto de la presente invención, se proporciona según la reivindicación 6 un método de gestión de derechos digitales para un servicio de difusión general-multidifusión, en el que el método se realiza mediante una red.

En las reivindicaciones subordinadas, se mencionan varias formas de realización de los métodos y mejoras de los mismos.

Descripción de los dibujos

Los dibujos adjuntos, que se incluyen para proporcionar una mayor comprensión de la invención y se incorporan a la presente memoria constituyendo parte de la misma, ilustran formas de realización de la invención y junto con la descripción sirven para explicar los principios de la invención.

En los dibujos:

la figura 1 es un diagrama de bloques que ilustra una construcción de un sistema de servicios de difusión/multidifusión según la presente invención;

la figura 2 es una vista ejemplificativa que ilustra ejemplos de agrupamientos de servicios;

la figura 3 es una vista ejemplificativa que ilustra un esquema de funcionamiento ejemplificativo basado en dominios de servicios según la presente invención;

la figura 4 es un diagrama de flujo de señales que ilustra una primera forma de realización para un método destinado a gestionar derechos digitales según la presente invención;

la figura 5 es un diagrama de flujo de señales que ilustra una segunda forma de realización para un método destinado a gestionar derechos digitales según la presente invención;

la figura 6 representa una jerarquía de claves para protección de servicios según la presente invención;

la figura 7 ilustra la diferencia entre la Protección de Servicios y la Protección de Contenido según la presente invención;

la figura 8 presenta una jerarquía de claves ejemplificativa para la protección de servicios y la protección de contenido según la presente invención;

la figura 9 muestra bloques ejemplificativos de la función de protección de servicios e interfaces entre ellos según la presente invención;

la figura 10 muestra una tabla que explica las interfaces y establece correspondencias de las mismas con puntos de referencia de BCAST según la presente invención.

Modo de poner en práctica la invención

A continuación, se explicarán, haciendo referencia a los dibujos adjuntos, formas de realización de un método ejemplificativo para gestionar derechos digitales en un servicio de difusión/multidifusión según la presente invención.

En general, en la gestión de derechos digitales, para compartir un objeto derechos de contenido y una clave de cifrado de contenido, varios dispositivos (que incluyen un terminal) utilizan un concepto al que se hace referencia como dominio.

El uso de un dominio permite que el contenido y objetos de derechos de contenido sean compartidos entre varios dispositivos cuyo propietario es un usuario, y un dispositivo al cual no se le permite acceder a un emisor de contenidos o un emisor de derechos podría utilizar un dispositivo con permisos de acceso para obtener el contenido y objetos de derechos de contenido. Por ejemplo, un dispositivo portátil reproductor de música que no tiene

capacidades de Internet inalámbrica se puede conectar a un ordenador personal (PC) que permita el acceso a Internet para así obtener contenido y objetos de derechos de contenido. Por lo tanto, el emisor de derechos gestiona el dominio para procesar solicitudes de unión y solicitudes de abandono del dispositivo que pertenece al dominio.

La presente invención puede proporcionar un cierto tipo de dominio de difusión. Todos los terminales que se abonan a un servicio o a un agrupamiento de servicios comparten una clave de grupo común. Se cifrarían entonces Claves de Cifrado de Servicios (SEK) o Claves de Cifrado de Programas (PEK) utilizando esta clave de grupo común. A este tipo de dominio de difusión se le denomina dominio de servicios. A saber, a un conjunto (o grupo) de terminales que se abonan a un servicio o agrupamiento de servicios, y que comparten una clave cifrada común se le hace referencia como dominio de servicios. En este caso, a un conjunto (o grupo) combinado selectivamente de uno o más servicios se le hace referencia como agrupamiento de servicios.

Terminales en un dominio de servicios pueden compartir contenido y servicios con cualquier otro terminal dentro del mismo dominio de servicios, sujetos a permisos especificados por los proveedores de contenidos o servicios. La ventaja de los dominios de servicios es que comunicar cambios de la SEK consume muy poco ancho de banda.

En la presente invención, el RI transmite a los terminales, un mensaje de claves con respecto a un dominio de servicios, el cual es un grupo de terminales que utilizan el mismo servicio o agrupamiento de servicios.

En este caso, el mensaje de claves se refiere a unos medios para proporcionar información sobre los derechos a utilizar el dominio de servicios (al unirse) que se envían desde el Emisor de Derechos (RI) hacia el terminal (dispositivo). Un ejemplo no limitativo puede ser un objeto derechos de dominio de servicios (es decir, Objeto Derechos: RO). En lo sucesivo, la presente invención simplemente se referirá a un "objeto derechos" meramente por comodidad. Resulta evidente que también pueden utilizarse otros tipos de mensajes de claves u otros medios de información.

Cada terminal que ha recibido el objeto derechos de dominio (RO), decodifica el RO de dominio correspondiente al dominio del mismo utilizando una clave de dominio perteneciente al mismo. En este caso, el RI emite un número de objetos de derechos que es igual al número de dominios de servicios, con independencia del número de terminales que usen el servicio o agrupamiento de servicios. Los terminales que pertenecen al mismo dominio comparten entre ellos la misma clave de dominio.

En la presente invención, el RI recibe una clave pública desde un terminal que solicita un registro de servicio, cifra una clave de dominio correspondiente a un dominio que el terminal pretende utilizar, utilizando la clave pública para seguidamente transmitir la clave de dominio cifrada. El RI seguidamente transmite el objeto derechos de dominio (RO) cifrado utilizando la clave de dominio. En este caso, el RO de dominio contiene una clave de cifrado de datos de servicios para decodificar los datos del servicio cifrados, recibidos desde un servidor de difusión/multidifusión.

En la presente invención, el RI recibe una clave pública desde un terminal que solicita un registro de servicio. El RI seguidamente cifra una clave de dominio correspondiente al dominio, que desea utilizar el terminal, utilizando la clave pública. El RI seguidamente transmite la clave de dominio cifrada hacia el terminal. Además, el RI cifra un RO de dominio que contiene una clave de cifrado de mensaje de claves utilizando la clave de dominio para seguidamente transmitir el RO de dominio cifrado hacia el terminal. El RI también cifra una clave de cifrado de datos de servicios para decodificar datos de servicios recibidos desde un servidor de difusión/multidifusión utilizando la clave de cifrado de mensaje de claves para seguidamente transmitir la clave de cifrado de datos de servicios, cifrada, hacia el terminal.

La figura 1 es un diagrama de bloques que ilustra una construcción ejemplificativa de un sistema de servicios de difusión/multidifusión según la presente invención. El sistema de servicios de difusión/multidifusión puede comprender de forma genérica terminales 10, un servidor de difusión/multidifusión (BCAST) 20 para proporcionar un servicio a los terminales 10, y un emisor de derechos (RI) 30 para gestionar un objeto derechos (RO) para permitir así que los terminales 10 usen el servicio.

En este caso, el RI 30 puede transmitir el RO a los terminales 10, o el servidor de BCAST 20 puede recibir el RO desde el RI 30 para seguidamente transmitir el RO recibido hacia los terminales 10.

La figura 2 es una vista ejemplificativa que ilustra un concepto de agrupamientos de servicios.

Haciendo referencia a la figura 2, se considera que un agrupamiento de servicios 1 es un paquete que contiene un servicio 1 y un servicio 2, un agrupamiento de servicios 2 es un paquete que contiene el servicio 1 y un servicio 3, un agrupamiento de servicios 3 contiene el servicio 1, y un agrupamiento de servicios 4 es un paquete que contiene el servicio 3 y un servicio 4. Un terminal que está abonado al agrupamiento de servicios 1 puede utilizar los servicios 1 y 2, y un terminal que está abonado al agrupamiento de servicios 4 puede utilizar los servicios 3 y 4. Debería observarse que un grupo de múltiples terminales puede utilizar uno o más servicios dentro de un agrupamiento de servicios.

Por tanto, el RI 30 no emite el RO con respecto a cada terminal 10, sino que emite el RO con respecto a un dominio de servicios al que pertenece el terminal 10. Es decir, el RO de dominio que reciben desde el RI 30 los terminales 10 que pertenecen al mismo dominio de servicios es el mismo. El RO de dominio se cifra utilizando la clave de dominio correspondiente a cada dominio, y por consiguiente los terminales que pertenecen al mismo dominio pueden compartir la clave de dominio para decodificar el RO.

La figura 3 ilustra un esquema de funcionamiento ejemplificativo basado en dominios de servicios según la presente invención. En este caso, un primer terminal 11 y un segundo terminal 12 abonados a un primer agrupamiento de servicios, y un tercer terminal 13 abonado a un segundo agrupamiento de servicios.

En primer lugar, el primer terminal 11 y el segundo terminal 12 reciben una clave de dominio para el primer dominio de servicios desde el RI (no mostrado) para tener de este modo la clave de dominio, y el tercer terminal 13 recibe y tiene una clave de dominio para el segundo dominio de servicios.

El RI o servidor de difusión/multidifusión 20 puede transmitir un RO de dominio de servicios a cada terminal 11, 12 y 13. La figura 3 muestra un ejemplo en el que el servidor de difusión/multidifusión 20 recibe el RO de cada dominio de servicios desde el RI (no mostrado) para seguidamente transmitir el RO recibido a cada terminal 11, 12 y 13.

Cada terminal 11, 12 y 13 que ha recibido el RO de dominio, seguidamente decodifica el RO de dominio utilizando la clave de dominio que tiene cada terminal 11, 12 y 13. Es decir, de entre los dos RO de dominio que se recibieron, el primer terminal 11 y el segundo terminal 12 pueden decodificar el primer RO de dominio de servicios, mientras que el tercer terminal 13 puede decodificar el segundo RO de dominio de servicios.

Tal como se ha mencionado anteriormente, en la presente invención, el RI o el servidor de difusión/multidifusión emite un cierto número de RO de dominio que es igual al número de los dominios de servicios independientemente del número de terminales que usen el servicio, y cada terminal decodifica solamente el RO de dominio que puede decodificar utilizando su clave de dominio de los RO de dominio. Por lo tanto, el sistema de servicios según la presente invención puede mantener la seguridad para un servicio (contenido), y utilizar eficazmente una red entre el servidor y el terminal al mismo tiempo.

La figura 4 es un diagrama de flujo de señales que ilustra una primera forma de realización de un método ejemplificativo para gestionar derechos digitales (derechos de autor) según la presente invención. En particular, la figura 4 ilustra un proceso para recibir un RO de dominio y datos de servicios por parte de un terminal en referencia a una estructura por capas de claves de seguridad.

Tal como se ha ilustrado en la figura 4, una primera capa se utiliza para permitir la realización del registro de servicios entre el terminal 10 y el RI 30 (S11). Debería observarse que dicho registro de dispositivos se puede realizar en una modalidad fuera de línea o en una modalidad en línea. Ejemplos de la modalidad en línea incluyen el uso de un canal de difusión o interacción.

A través de la primera capa se puede transmitir al RI 30 una clave pública del terminal 10, y se negocia un algoritmo de seguridad que se utilizaría entre el terminal 10 y el RI 30. En este caso, en el terminal 10 se puede generar un contexto de RI. El contexto de RI puede contener información negociada cuando el terminal 10 se registra en el RI 30, particularmente, una ID de RI, un certificado del RI, una versión, un algoritmo de seguridad, y otra información.

Una segunda capa, que se utiliza como capa de gestión de dominios, se utiliza para abonarse a y abandonar (terminar) un dominio de servicios particular. En este caso, antes de utilizar la segunda capa, el terminal 10 puede recibir una guía de servicios que contiene información (información de servicios, información de dominios, o similares) para describir servicios de difusión/multidifusión que puede utilizar el terminal 10.

Después de confirmar los servicios que se pueden utilizar en el terminal 10 a través de la guía de servicios, el usuario solicita una suscripción de dominio desde el RI 30 utilizando el terminal 10 (S13), el RI 30 transmite una clave de dominio cifrada utilizando la clave pública hacia el terminal 10 (S15). Cuando solicita la suscripción de dominio, el terminal 10 transmite una ID de servicio o ID de agrupamiento de servicios, una ID de terminal, una firma digital de terminal, y similares, como tipos de parámetro.

Como consecuencia de la suscripción de dominio, se genera un contexto de dominio en el terminal 10. El contexto de dominio contiene información relacionada con la clave de dominio, una ID de dominio, una validez de dominio, y similares.

Cuando el terminal solicita un abandono (terminación) de dominio del RI 30, el RI 30 elimina el terminal correspondiente 10 de una lista de terminales que pertenecen al dominio, y el terminal 10 elimina (termina) su relación con el dominio.

Una tercera capa se utiliza como capa de gestión de RO. El RI 30 utiliza la tercera capa para transmitir el RO de dominio de servicios al terminal 10 (S17). En este caso, el RO de dominio contiene una o más claves de cifrado de datos de servicios (por ejemplo, SEK: Clave de Cifrado de Servicios) que se cifra(n) utilizando la clave de dominio.

El RI 30 puede transmitir directamente el RO de dominio de servicios al terminal 10, o puede transmitirlo al terminal 10 a través del servidor de difusión/multidifusión 20. Es decir, el RI 30 transfiere el RO de dominio de servicios hacia el servidor de difusión/multidifusión 20, y el servidor de difusión/multidifusión 20 que ha recibido el RO transmite el RO correspondiente al terminal 10. En este caso, el RO transmitido desde el RI 30 se puede transferir al terminal 10 a través del servidor de difusión/multidifusión 20. La transmisión del RO directamente al terminal 10 ó a través del servidor de difusión/multidifusión 20 se puede utilizar selectivamente según se requiera. Si al RI 30 se le pueden proporcionar las funciones necesarias realizadas por el servidor de difusión/multidifusión 20, entonces el RI 30 puede transmitir directamente el RO hacia el terminal 10.

Una cuarta capa se utiliza como capa de cifrado de servicios. El servidor de difusión/multidifusión 20 transmite datos de servicios cifrados utilizando la clave de cifrado de datos de servicios hacia el terminal 10 a través de la cuarta capa (S19). El terminal 10 recibe el RO con respecto a un dominio de servicios particular y los datos de servicios cifrados utilizando la clave particular de cifrado de datos de servicios, y decodifica los datos de servicios utilizando el RO. Posteriormente se explicará un método para decodificar los datos de servicios por parte del terminal.

Por consiguiente, puesto que la clave de cifrado de datos de servicios para decodificar los datos de servicios se ha cifrado utilizando la clave de dominio, un terminal que tenga la misma clave de dominio puede obtener la clave de cifrado de datos de servicios para así ejecutar los datos de servicios.

La figura 5 es un diagrama de flujo de señales que ilustra una segunda forma de realización para un método ejemplificativo con el fin de gestionar derechos digitales según la presente invención. El proceso para recibir un RO de dominio y datos de servicios por parte del terminal se representa en referencia a la estructura por capas de claves de seguridad.

En particular, en la segunda forma de realización de la presente invención, además de la clave o claves de cifrado de datos de servicios (por ejemplo, SEK: Clave de Cifrado de Servicios) de la primera forma de realización, para proporcionar una protección y seguridad adicionales para los datos de servicios se utiliza una clave de cifrado de mensajes de claves (por ejemplo, TEK: Clave de Cifrado de Tráfico) para inducir la clave de cifrado de datos de servicios.

Por consiguiente, además de compartir una clave pública (PK), existe una relación particular con respecto a ciertas claves de seguridad (es decir, clave de dominio, SEK, TEK) utilizadas por el dispositivo (terminal) y el emisor de derechos (RI). A saber, la clave de dominio se utiliza para el cifrado y el descifrado de un objeto derechos (RO) que contiene una o más SEK, la SEK se utiliza para el cifrado y el descifrado de la TEK, mientras que la TEK se utiliza para el cifrado y el descifrado de contenido.

Tal como se ilustra en la figura 5, en primer lugar, cuando el terminal 10 solicita el registro en el RI 30 en la primera capa (S21), se negocia un algoritmo de seguridad que se utilizará entre el terminal 10 y el RI 30. Debería observarse que dicho registro del dispositivo se puede realizar en una modalidad fuera de línea o una modalidad en línea. Ejemplos de la modalidad en línea incluyen el uso de un canal de difusión o interacción.

Como consecuencia de la solicitud de registro, se genera un contexto de RI en el terminal 10. El contexto de RI contiene información relacionada con una ID de RI, un certificado del RI, una versión, un algoritmo de seguridad, y otra información.

Antes de ejecutar una operación en la segunda capa, el terminal 10 puede recibir una guía de servicios con respecto a servicios de difusión/multidifusión que se pueden utilizar de este modo.

En una segunda capa, el terminal 10 solicita una suscripción con el dominio de servicios para proporcionar un servicio o agrupamiento de servicios particular desde el RI 30 (S23). El RI 30 transmite al terminal 10, la clave de dominio que se cifra utilizando la clave pública del terminal 10 (S25). Cuando solicita la suscripción de dominio, el terminal 10 transmite la ID de servicio o ID de agrupamiento de servicios, una ID de terminal, una firma digital de terminal, y similares, al RI 30.

Por lo tanto, en el terminal 10 que ha recibido la clave de dominio desde el RI 30 se genera un contexto de dominio. El contexto de dominio contiene información relacionada con la clave de dominio, una ID de dominio, una validez de dominio, y similares. Cuando el terminal 10 solicita una suscripción a uno o más dominios de servicios, el número de claves de dominio e ID de dominio que puede tener el terminal 10 sería igual al número de dominios.

Una tercera capa se utiliza como capa de gestión de RO. El RI 30 transmite el RO de dominio de servicios al terminal 10 a través de la tercera capa (S27). En este caso, puesto que el RO de dominio contiene una o más claves de cifrado de datos de servicios (por ejemplo, SEK: Clave de Cifrado de Servicios) que se cifra(n) utilizando la clave

de dominio, solamente los terminales que pertenecen al dominio de servicios que tiene la clave de dominio pueden decodificar la clave de cifrado de datos de servicios.

Como en la primera forma de realización, el RI 30 puede transmitir directamente el RO al terminal 10, o puede transmitirlo al terminal 10 a través del servidor de difusión/multidifusión 20. Si al RI 30 se le proporcionan las capacidades necesarias del servidor de difusión/multidifusión 20, entonces el RO se puede transmitir directamente al terminal 10.

Una cuarta capa se utiliza como capa de transmisión de claves. El RI 30 transmite la clave de cifrado de datos de servicios (por ejemplo, TEK: Clave de Cifrado de Tráfico) que se cifró utilizando la clave de cifrado de mensajes de claves al terminal 10 a través de la cuarta capa. Por consiguiente, solamente los terminales que tienen la clave de cifrado de mensajes de claves pueden decodificar la clave de cifrado de datos de servicios.

La clave de cifrado de datos de servicios se puede transmitir al terminal 10 a través del servidor de difusión/multidifusión 20 así como a través del RI 30. En este caso, el RI 30 transmite la clave de cifrado de datos de servicios hacia al servidor de difusión/multidifusión 20, que a continuación transmite la clave correspondientes de cifrado de datos de servicios hacia el terminal 10. Si al RI 30 se le proporcionan las capacidades necesarias del servidor de difusión/multidifusión 20, entonces la TEK se puede transmitir directamente al terminal 10.

Una quinta capa se utiliza como capa de cifrado de servicios. El servidor de difusión/multidifusión 20 transmite datos de servicios cifrados utilizando la clave de cifrado de datos de servicios al terminal 10 a través de la quinta capa (S31).

La estructura por capas de claves de seguridad según la presente invención puede tener otras configuraciones que sean diferentes de las mostradas en la primera y segunda formas de realización para el dominio de servicios.

La presente invención se puede entender adicionalmente haciendo referencia a la figura 6, que representa una jerarquía de claves para protección de servicios según la presente invención. A saber, la figura 6 presenta la jerarquía de claves para protección de servicios con el dominio según la presente invención.

La capa 1 implementa el registro del dispositivo (terminal). El material de claves y metadatos adquiridos durante la fase de registro posibilitarán que el dispositivo descifre y autentique objetos de derechos y posteriormente que acceda a contenido.

La figura 6 muestra una situación en la que el dispositivo registra su clave pública con el emisor de derechos (RI) a través de un registro de dispositivo y el emisor de derechos cifra la Clave de Cifrado de Servicios (SEK) utilizando una clave pública del dispositivo. En este caso, no solamente el dispositivo sino también otro dominio se puede registrar también con el emisor de derechos. Para hacerlo así, el dominio puede registrar una “clave pública de dispositivos en el dominio” o “clave de dominio” con el emisor de derechos.

La capa 2 implementa una función de Gestión de Grupos de Servicio. Para dispositivos que tienen acceso a un canal de interacción se puede utilizar el Protocolo de Unión/Abandono de Dominios del OMA DRM. Esta capa entrega una Clave de Cifrado de Servicios (SEK) como clave de dominio. La Clave de Cifrado de Servicios (SEK) se puede actualizar a través de la creación de un dominio nuevo o a través de una actualización de dominio.

La capa 3 implementa una función de gestión de derechos. Un Objeto Derechos (RO), que se puede proteger por medio de una clave de servicio (por ejemplo, SEK), contiene la clave de tráfico (por ejemplo, TEK) que es necesaria para descifrar (una parte de) el servicio, junto con los identificadores que permiten vincular la clave de tráfico con el contenido cifrado y el dominio. El cripto-periodo (es decir, tiempo de vida) de la clave de tráfico puede ser relativamente breve para evitar ataques de distribución de tiempo real.

La idea que subyace tras la capa 3 es proporcionar una seguridad mejorada, escalabilidad y un soporte enriquecido de casos de uso. La especificación para la capa 3 debería garantizar que se satisfacen estos requisitos.

Debería observarse que la estructura arquitectónica no excluye soluciones que incluyan elementos de seguridad variables, tales como, derivación de claves.

Puesto que la ejecución de la Capa 2 puede verse perturbada por condiciones inesperadas, la Capa 3 se debería implementar para ser ejecutada después de un tiempo de retardo razonable desde el inicio de los procedimientos de la Capa 2.

La Capa 4 implementa el cifrado del contenido de difusión con la clave de tráfico. El cifrado se puede realizar sobre la capa de red (es decir IP), la capa de transporte (por ejemplo, UDP), o la capa de sesión (por ejemplo, RTP).

La presente invención se puede entender asimismo haciendo referencia a las figuras 7 a 10 y a la siguiente descripción.

Las funciones de Protección de Servicios y Contenidos posibilitan una manera, independiente del BDS, para proteger tanto contenido como servicios distribuidos dentro de los servicios de Difusión Móvil. La figura 7 ilustra la diferencia entre Protección de Servicios y Protección de Contenido.

La protección de servicios tiene el propósito de permitir acceder a un servicio, es decir para un conjunto definido de datos (audio-visuales) durante una cantidad especificada de tiempo. La protección de servicios no asume ninguna responsabilidad por el contenido después de haber sido liberado hacia el terminal de usuario; no proporciona ningunos medios técnicos para proteger contenido fuera de la canalización de transporte de bits que esta implementando el control de acceso.

La protección de contenido tiene el propósito de proteger los elementos de contenido individuales. El contenido puede tener o no derechos de uso asociados al mismo tras su distribución.

La Protección de Servicios, con independencia de la Protección de Contenido, está destinada a la gestión de suscripciones. En ausencia de protección de contenido, los derechos de uso para contenido en general pueden ser libres, o estar sujetos a la legislación aplicable, un modelo de negocio u otros requisitos; sin embargo, dichas consideraciones se sitúan más allá del alcance de estas definiciones. La Protección de Contenido trata sobre derechos de uso tras la distribución, los cuales especifican cómo se puede utilizar el contenido de acuerdo con permisos y restricciones.

La figura 8 presenta la jerarquía de claves para protección de servicios y protección de contenido.

La Capa 1 implementa la Autenticación. El material de claves y meta-datos adquiridos durante la fase de registro de la identidad del abonado (SI) o del dispositivo posibilitará al abonado o dispositivo ser autenticado y posteriormente acceder a contenido, y se almacenan de forma segura en el terminal o tarjeta inteligente. En este caso, la Tarjeta Inteligente puede ser una USIM/(R-)UIM. Al material de claves obtenido en la Capa 1, y utilizado para proteger la Clave de Larga Duración entregada en la Capa 2, se le hace referencia como Clave de Gestión de Abonados o Clave de Cifrado de Derechos.

La Capa 2 implementa la entrega de Mensajes de Claves de Larga Duración (LTKM). Esta capa entrega una clave de cifrado de servicios (SEK) o clave de cifrado de programas (PEK). La clave de cifrado de servicios o de programas es una clave intermedia, es decir, no cifra directamente el contenido sino que, por el contrario, protege una secuencia de claves de cifrado de tráfico (TEK). Para la gestión y protección de suscripciones de servicios la SEK o PEK se actualizará con un cripto-periodo normalmente mayor que la clave de tráfico TEK.

La Capa 3 implementa la entrega de Mensajes de Claves de Corta Duración sobre el canal de difusión o interactivo. Se envían al terminal, una TEK, cifrada por medio de una SEK o PEK, o datos necesarios que pueden ser utilizados para derivar la clave de tráfico, junto con los identificadores que permiten vincular la clave de tráfico con el contenido cifrado.

La idea que subyace tras la capa 3 es proporcionar una seguridad mejorada, escalabilidad y un soporte más enriquecido de casos de uso. La especificación para la capa 3 garantizará que se satisfacen estas ideas.

La capa 4, o Protección, implementa el cifrado de contenido de difusión con la clave de tráfico de Corta Duración. El cifrado se puede realizar sobre la capa de red (es decir, IP), la capa de transporte (por ejemplo, UDP), la capa de sesión (por ejemplo, RTP) o la capa de contenido (cifrado AU) para la protección de servicios.

La figura 9 muestra bloques de la función de protección de servicios e interfaces entre ellos. Como las características representadas en la figura 9 serán entendidas por los expertos en la materia, se omite una explicación detallada meramente por motivos de brevedad.

La figura 10 muestra una tabla que explica las interfaces y establece correspondencias de las mismas con puntos de referencia de BCAST:

<u>Función de Aplicación de Archivos/Aplicación de Flujos Continuos</u>

La Función de Aplicación de Archivos/Aplicación de Flujos Continuos (FA/SA) en el BSA es responsable de recibir archivos y flujos continuos desde la Creación de Contenidos, y de enviar el archivo y el flujo continuo con atributos e información adicional a la Distribución/Adaptación de Servicios del BCAST.

<u>Función de Gestión de SP</u>

La Función de Gestión de Protección de Servicios (SP-M) en el BSM es responsable del registro, la entrega de LTKM sobre el canal de interacción. El mensaje de claves de larga duración que contiene la SEK se entrega al SP-C desde la SP-M. Los terminales de solamente difusión requieren un canal fuera de banda para iniciar la solicitud de

registro y la entrega de mensajes de claves de larga duración, y los terminales de solamente difusión reciben respuestas para el registro y la entrega de mensajes de claves de larga duración sobre el canal de difusión.

La SP-M también administra la entrega de STKM y la gestión segura de grupos. El STKM, entregado desde la SP-M a la SP-KD, se distribuye al SP-C sobre el canal de difusión. El esquema de gestión segura de grupos se puede utilizar para la difusión eficaz del mensaje de claves de larga duración y el procedimiento de revocación. La SP-M está a cargo de la gestión de dominios. El terminal puede unirse a un dominio o abandonar un dominio utilizando la SP-M.

Función de Distribución de Claves de SP

La Función de Distribución de Claves de Protección de Servicios (SP-KD) en el BSD/A es responsable de la difusión de LTKM y STKM. El terminal puede adquirir la TEK a partir del STKM para el descifrado de los servicios cifrados. El STKM, el LTKM y materiales de claves de registro se envían desde la SP-M hacia la SP-KD para su distribución hacia los Terminales. La SP-KD también transfiere el STKM, el LTKM y materiales de claves sobre el canal de difusión para terminales de solamente difusión.

Función de Cifrado de SP

La Función de Cifrado de Protección de Servicios (SP-E) en el BSD/A es responsable del cifrado de servicios para su entrega sobre el canal de difusión. La TEK, entregada desde la SP-M, se utiliza para cifrar servicios. El formato del servicio cifrado depende del sistema específico de protección de servicios.

Función de Descifrado de SP

La Función de Descifrado de Protección de Servicios (SP-D) en el Terminal es responsable de descifrar los servicios cifrados utilizando la TEK extraída del STKM. El STKM se entrega desde la SP-M a la SP-KD y el SP-C recibe el STKM desde la SP-KD sobre el canal de difusión.

Función de Cliente de SP

La Función de Cliente de Protección de Servicios (SP-C) está o bien solamente en el Terminal o bien tanto en el Terminal como en la Tarjeta Inteligente. El SP-C es responsable del registro y la adquisición del LTKM y el STKM. Después del registro, el SP-C adquiere la REK, SMK o GMK que se deriva del registro. El LTKM contiene la SEK que se utiliza para cifrar el STKM. El SP-C también adquiere la TEK descifrando el STKM que utiliza la SEK, y la TEK se envía al SP-D para el descifrado de los servicios cifrados.

REIVINDICACIONES

1. Método de gestión de derechos digitales para un servicio de difusión-multidifusión, siendo realizado el método por un terminal, y comprendiendo:

realizar un procedimiento de registro con una red, compartiéndose una clave pública del terminal durante el procedimiento de registro realizado a través de un canal de difusión o canal de interacción;

caracterizado porque el método comprende además:

enviar, a la red, un mensaje de solicitud para unirse a un dominio de servicios que se corresponde con un agrupamiento de servicios que comprende una pluralidad de servicios que comparten una clave de dominio común para cada agrupamiento de servicios;

recibir, desde la red, la clave de dominio común para el agrupamiento de servicios, habiéndose cifrado la clave de dominio común mediante el uso de la clave pública;

recibir, desde la red, un Objeto Derechos (RO) de dominio de servicios que incluye una pluralidad de Claves de Cifrado de Servicios, SEK, cifrándose cada SEK por medio de la clave de dominio común recibida, y difundiéndose de forma general el RO de dominio de servicios a través del canal de difusión o siendo transmitido directamente a través del canal de interacción hacia una pluralidad de terminales que se unieron al dominio de servicios;

recibir, desde la red, una Clave de Cifrado de Tráfico, TEK, que se cifra utilizando una de entre la pluralidad de SEK, difundiéndose la TEK a través del canal de difusión o transmitiéndose directamente a través del canal de interacción; y

recibir, desde la red, datos de servicios del servicio de difusión-multidifusión, cifrándose los datos de servicios mediante el uso de la TEK.

2. Método según la reivindicación 1, que comprende además:

descifrar los datos de servicios recibidos utilizando la TEK.

3. Método según la reivindicación 1 ó 2, en el que la clave de dominio común y el RO de dominio de servicios se reciben desde un Emisor de Derechos (RI) de la red.

4. Método según cualquiera de las reivindicaciones 1 a 3, en el que el mensaje de solicitud es un mensaje de solicitud de suscripción de dominio utilizado para solicitar la suscripción con un dominio de servicios para proporcionar un servicio o agrupamiento de servicios particular desde el RI.

5. Método según la reivindicación 4, en el que, cuando se solicita la suscripción con el dominio de servicios, se envía al RI por lo menos una de entre una ID de servicio o una ID de agrupamiento de servicios, una ID de terminal, y una firma digital de terminal.

6. Método de gestión de derechos digitales para un servicio de difusión general-multidifusión, realizándose el método mediante una red y comprendiendo:

realizar un procedimiento de registro con un terminal, compartiéndose una clave pública del terminal durante el procedimiento de registro realizado a través de un canal de difusión o canal de interacción;

caracterizado porque el método comprende además:

recibir, desde el terminal, un mensaje de solicitud para unirse a un dominio de servicios que se corresponde con un agrupamiento de servicios que comprende una pluralidad de servicios que comparten una clave de dominio común para cada agrupamiento de servicios;

enviar, al terminal, la clave de dominio común para el agrupamiento de servicios, la clave de dominio común que se cifró utilizando la clave pública;

enviar, al terminal, un Objeto Derechos (RO) de dominio de servicios que incluye una pluralidad de Claves de Cifrado de Servicios, SEK, cifrándose cada SEK mediante el uso de la clave de dominio común enviada, y difundiéndose el RO de dominio de servicios a través del canal de difusión o siendo transmitido directamente a través del canal de interacción hacia una pluralidad de terminales que se unieron al dominio de servicios;

enviar, al terminal, una Clave de Cifrado de Tráfico, TEK, que se cifra utilizando una de entre la pluralidad de

SEK, difundiéndose la TEK a través del canal de difusión o transmitiéndose directamente a través del canal de interacción; y

enviar, al terminal, datos de servicios del servicio de difusión-multidifusión, cifrándose los datos de servicios mediante la utilización de la TEK.

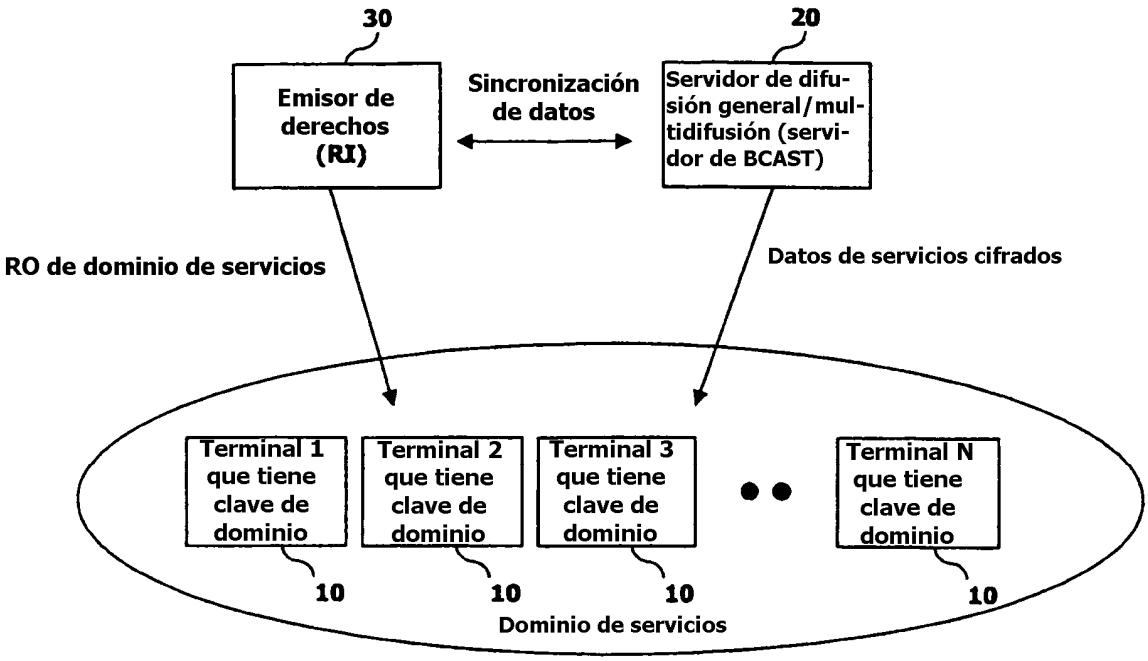
7. Método según la reivindicación 6, en el que la clave de dominio común y el RO de dominio de servicios se envían desde un Emisor de Derechos (RI) de la red.

8. Método según la reivindicación 6 ó 7, en el que el mensaje de solicitud es un mensaje de solicitud de suscripción de dominio utilizado para solicitar la suscripción con un dominio de servicios para proporcionar un servicio o agrupamiento de servicios particular desde el RI.

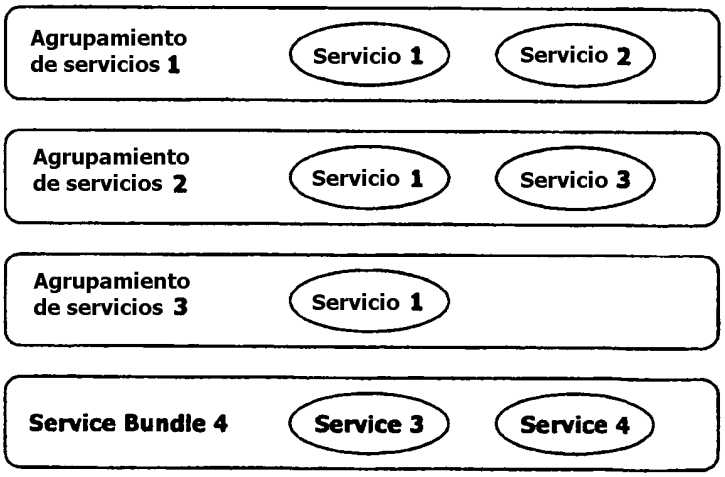
9. Método según la reivindicación 8, en el que, cuando se solicita la suscripción con el dominio de servicios, el RI recibe por lo menos una de entre una ID de servicio o un ID de agrupamiento de servicios, una ID de terminal, y una firma digital de terminal.

10. Método según cualquiera de las reivindicaciones 6 a 9, en el que la TEK se envía al terminal por medio de un servidor de BCAST de la red.

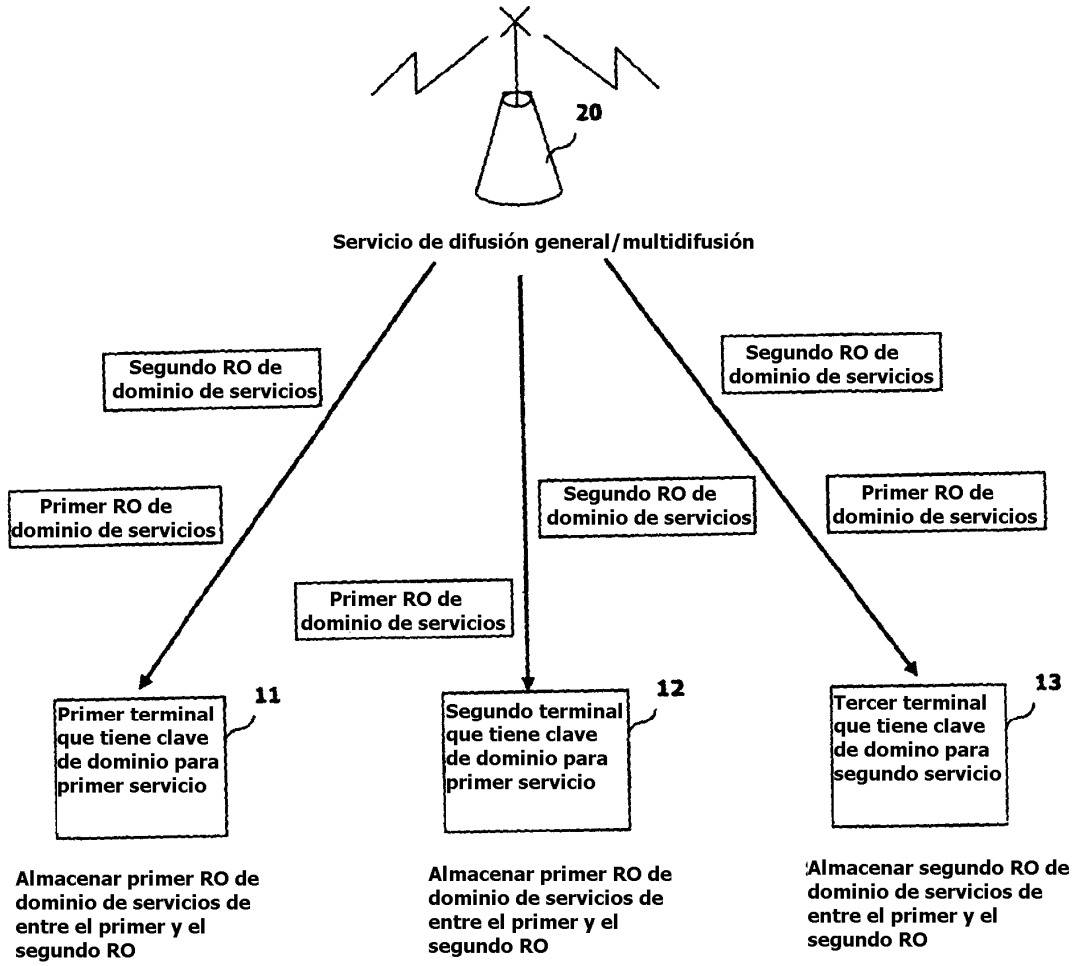
[Fig. 1]


30
20
Emisor de derechos (RI)
Sincronización de datos
Servidor de difusión general/multidifusión (servidor de BCAST)
RO de dominio de servicios
Datos de servicios cifrados
Terminal 1 que tiene clave de dominio
Terminal 2 que tiene clave de dominio
Terminal 3 que tiene clave de dominio
Terminal N que tiene clave de dominio
10
10
10
10
Dominio de servicios

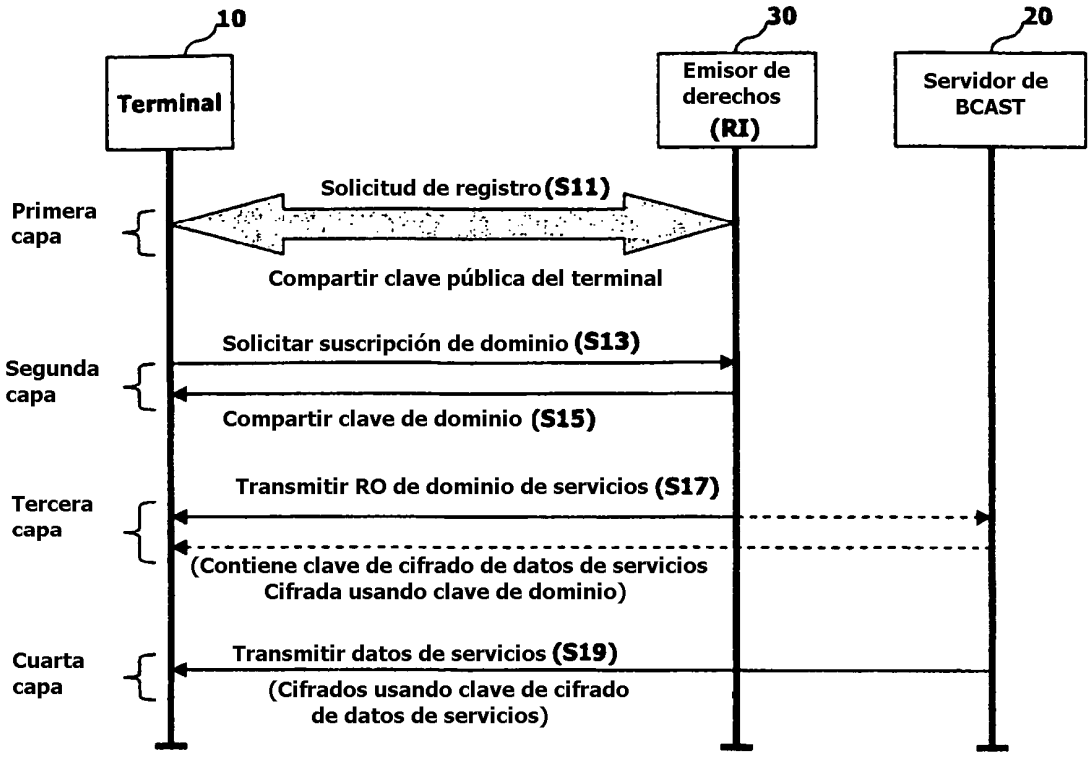
[Fig. 2]


Agrupamiento de servicios 1
Servicio 1
Servicio 2
Agrupamiento de servicios 2
Servicio 1
Servicio 3
Agrupamiento de servicios 3
Servicio 1
Service Bundle 4
Service 3
Service 4

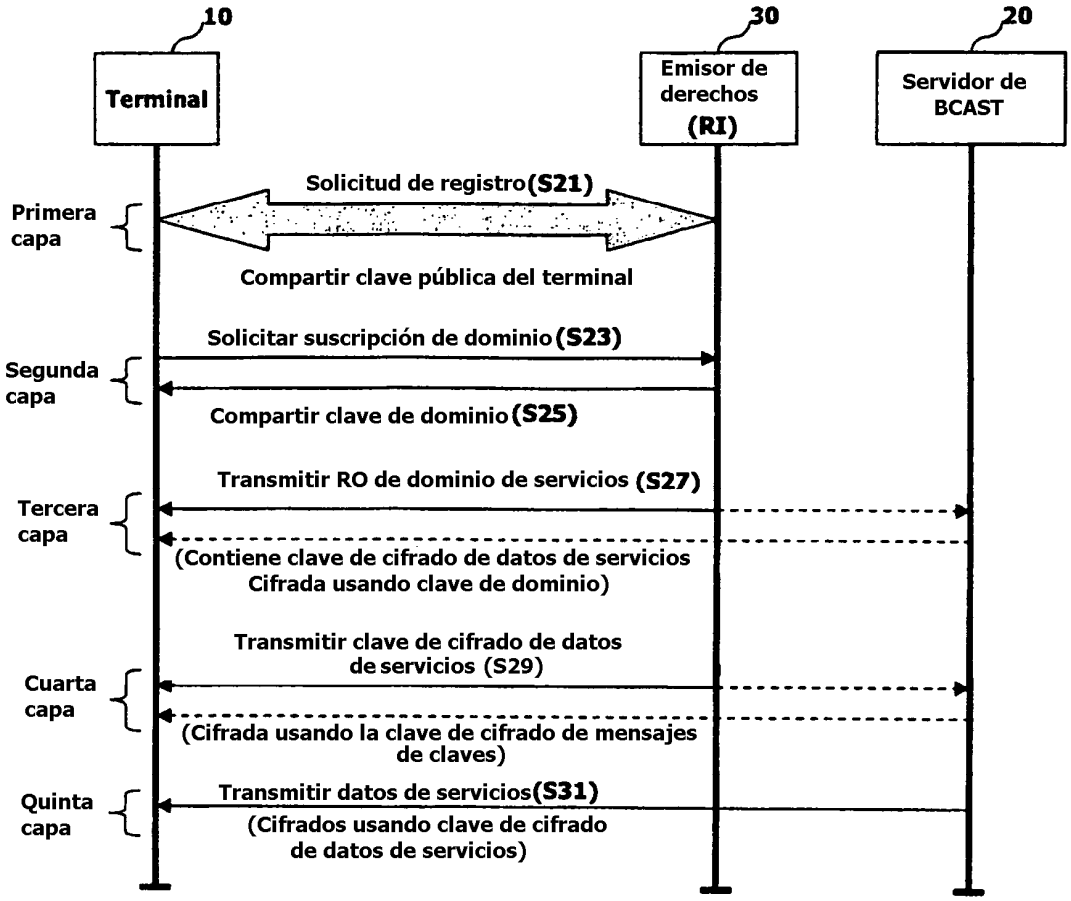
[Fig. 3]


20
Servicio de difusión general/multidifusión
Segundo RO de dominio de servicios
Primer RO de dominio de servicios
Primer RO de dominio de servicios
Segundo RO de dominio de servicios
Segundo RO de dominio de servicios
Primer RO de dominio de servicios
11
Primer terminal que tiene clave de dominio para primer servicio
12
Segundo terminal que tiene clave de dominio para primer servicio
13
Tercer terminal que tiene clave de domino para segundo servicio
Almacenar primer RO de dominio de servicios de entre el primer y el segundo RO
Almacenar primer RO de dominio de servicios de entre el primer y el segundo RO
Almacenar segundo RO de dominio de servicios de entre el primer y el segundo RO

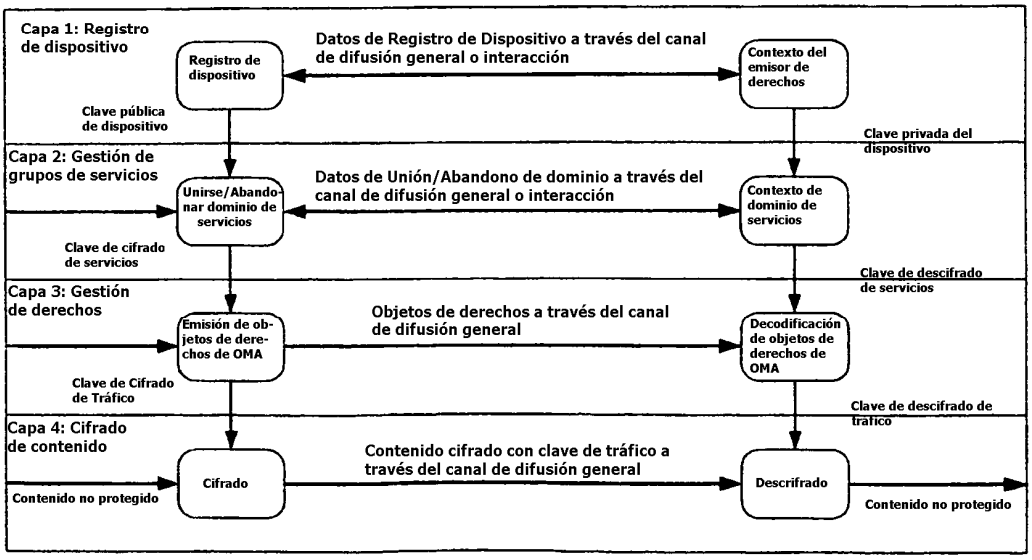
[Fig. 4]


10
30
20
Terminal
Emisor de derechos (RI)
Servidor de BCAST
Primera capa
Solicitud de registro (S11)
Compartir clave pública del terminal
Segunda capa
Solicitar suscripción de dominio (S13)
Compartir clave de dominio (S15)
Tercera capa
Transmitir RO de dominio de servicios (S17)
(Contiene clave de cifrado de datos de servicios Cifrada usando clave de dominio)
Cuarta capa
Transmitir datos de servicios (S19)
(Cifrados usando clave de cifrado de datos de servicios)

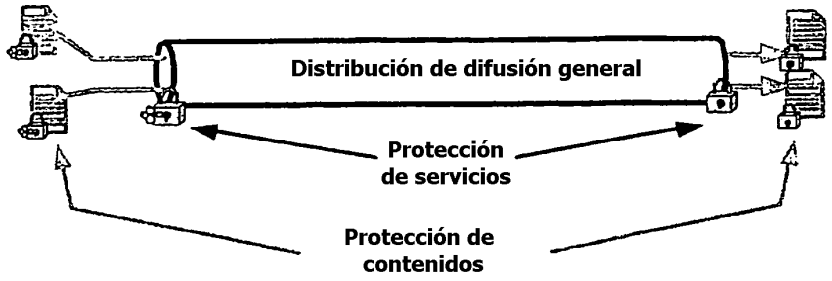
[Fig. 5]


10
30
20
Terminal
Emisor de derechos (RI)
Servidor de BCAST
Primera capa
Solicitud de registro(S21)
Compartir clave pública del terminal
Segunda capa
Solicitar suscripción de dominio(S23)
Compartir clave de dominio(S25)
Tercera capa
Transmitir RO de dominio de servicios (S27)
(Contiene clave de cifrado de datos de servicios Cifrada usando clave de dominio)
Cuarta capa
Transmitir clave de cifrado de datos de servicios (S29)
(Cifrada usando la clave de cifrado de mensajes de claves)
Quinta capa
Transmitir datos de servicios(S31)
(Cifrados usando clave de cifrado de datos de servicios)

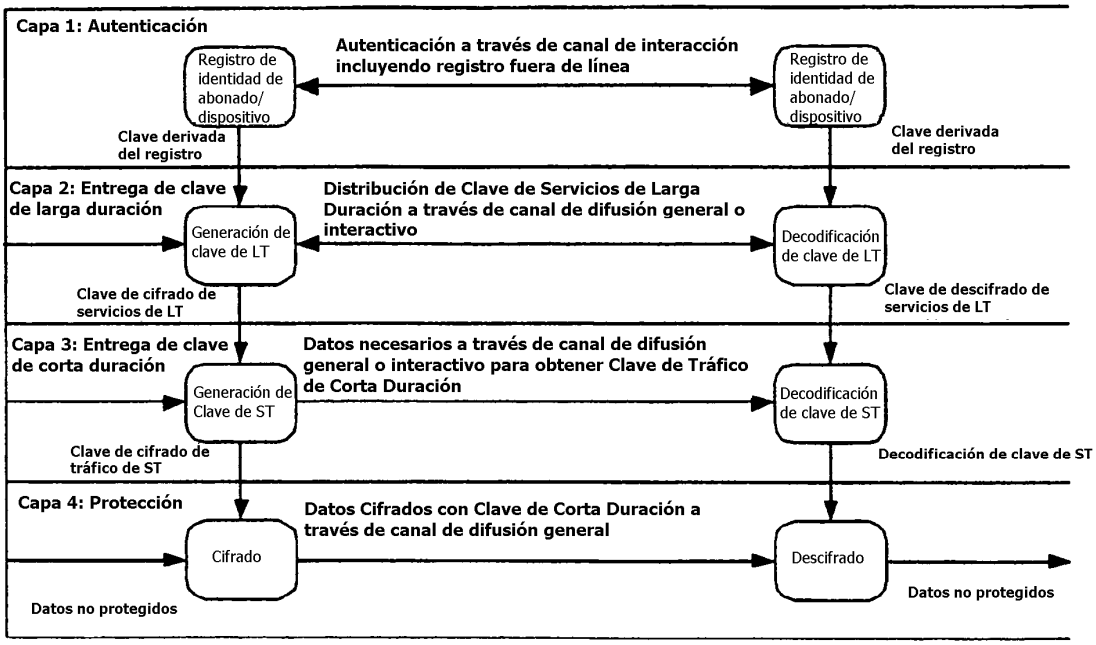
[Fig. 6]


Capa 1: Registro de dispositivo
Registro de dispositivo
Datos de Registro de Dispositivo a través del canal de difusión general o interacción
Contexto del emisor de derechos
Clave pública de dispositivo
Clave privada del dispositivo
Capa 2: Gestión de grupos de servicios
Unirse/Abandonar dominio de servicios
Datos de Unión/Abandono de dominio a través del canal de difusión general o interacción
Contexto de dominio de servicios
Clave de cifrado de servicios
Clave de descifrado de servicios
Capa 3: Gestión de derechos
Emisión de objetos de derechos de OMA
Objetos de derechos a través del canal de difusión general
Decodificación de objetos de derechos de OMA
Clave de Cifrado de Tráfico
Clave de descifrado de tráfico
Capa 4: Cifrado de contenido
Cifrado
Contenido cifrado con clave de tráfico a través del canal de difusión general
Descifrado
Contenido no protegido
Contenido no protegido

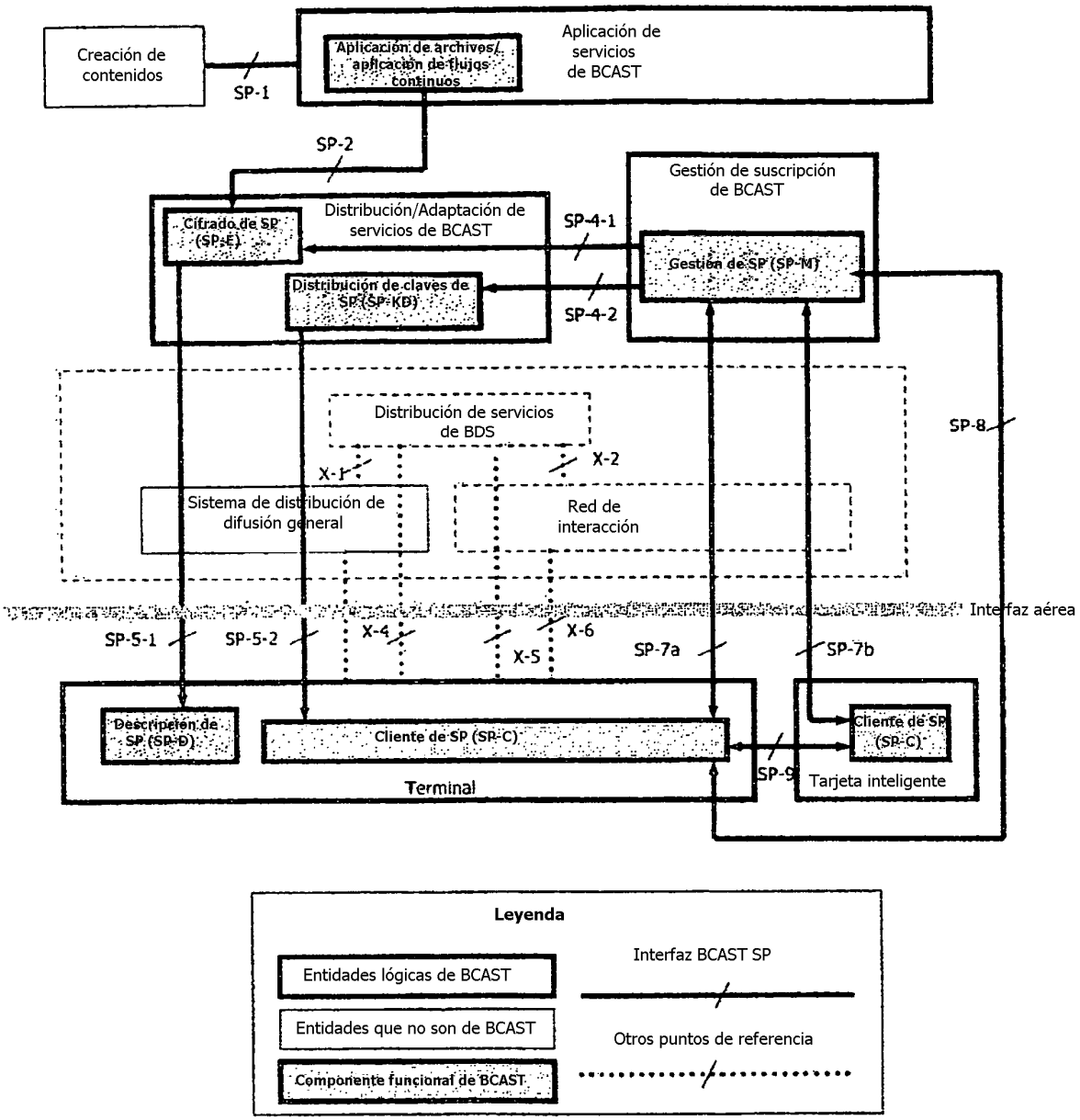
[Fig. 7]


Distribución de difusión general
Protección de servicios
Protección de contenidos

[Fig. 8]


Capa 1: Autenticación
Registro de identidad de abonado/ dispositivo
Autenticación a través de canal de interacción incluyendo registro fuera de línea
Registro de identidad de abonado/ dispositivo
Clave derivada del registro
Clave derivada del registro
Capa 2: Entrega de clave de larga duración
Generación de clave de LT
Distribución de Clave de Servicios de Larga Duración a través de canal de difusión general o interactivo
Decodificación de clave de LT
Clave de cifrado de servicios de LT
Clave de descifrado de servicios de LT
Capa 3: Entrega de clave de corta duración
Generación de Clave de ST
Datos necesarios a través de canal de difusión general o interactivo para obtener Clave de Tráfico de Corta Duración
Decodificación de clave de ST
Clave de cifrado de tráfico de ST
Decodificación de clave de ST
Capa 4: Protección
Cifrado
Datos Cifrados con Clave de Corta Duración a través de canal de difusión general
Descifrado
Datos no protegidos
Datos no protegidos

[Fig. 9]


Creación de contenidos
SP-1
Aplicación de archivos/ aplicación de flujos continuos
Aplicación de servicios de BCAST
SP-2
Gestión de suscripción de BCAST
Cifrado de SP (SP-E)
Distribución/Adaptación de servicios de BCAST
SP-4-1
Gestión de SP (SP-M)
Distribución de claves de SP (SP-KD)
SP-4-2
Distribución de servicios de BDS
SP-8
X-1
X-2
Sistema de distribución de difusión general
Red de interacción
Interfaz aérea
SP-5-1
SP-5-2
X-4
X-5
X-6
SP-7a
SP-7b
Descripción de SP (SP-D)
Cliente de SP (SP-C)
Cliente de SP (SP-C)
SP-9
Terminal
Tarjeta inteligente
Leyenda
Entidades lógicas de BCAST
Entidades que no son de BCAST
Componente funcional de BCAST
Interfaz BCAST SP
Otros puntos de referencia

[Fig. 10]

Interfaz	Punto de Referencia	Definición
SP-1	BCAST-1	Los archivos y el flujo continuo de la Creación de Contenidos se envían al BSD/A.
SP-2	BCAST-2	El servicio de difusión general (basado en distribución de archivos y/o flujos continuos) se puede - alimentar al BDS para una distribución no protegida hacia el terminal - alimentar al BDS para una distribución protegida al terminal, usando una protección de servicios nativa del BDS - alimentar al sistema de distribución de servicios de difusión general para una distribución al terminal protegida por la OMA
SP-4-1	BCAST-4	Esta interfaz entrega la TEK para el cifrado de servicios desde la SP-M al SP-E.
SP-4-2	BCAST-4	Esta interfaz entrega el STKM y LTKM para la suscripción desde la SP-M a la SP-KD.
SP-5-1	BCAST-5	Esta interfaz implementa la capa 4 ("Capa de Contenidos") del modelo de 4 capas. El servicio protegido por la OMA se distribuye al terminal a través del BDS. Nota: esta interfaz es idéntica a la FD-5 y la SD-5.
SP-5-2	BCAST-5	Esta interfaz implementa la capa 3 ("Capa de Entrega de Claves de Corta Duración") del modelo de 4 capas. Se distribuyen mensajes de claves de tráfico hacia el terminal a través del BDS. Otro cometido de esta interfaz es implementar la capa 2 ("Capa de Entrega de Claves de Corta Duración") del modelo de 4 capas para la entrega del mensaje de claves de larga duración a través del canal de difusión general. Esta interfaz conjuntamente con la interfaz SP-8 implementa también la capa 1 ("Capa de Autenticación") del modelo de 4 capas para el registro de terminales a través del canal de difusión general. La idea es registrar "terminales solamente de difusión general" (terminales que no tienen un canal de interacción) usando el canal de difusión general para establecer el material de claves que se requiere para transacciones posteriores. Esta interfaz cubre también el registro de dispositivos que forman juntos un dominio local de DRM.
SP-7	BCAST-7	Esta interfaz implementa las capas 2 y 1 del modelo de 4 capas para la entrega del mensaje de claves de larga duración y el registro a través del canal de interacción.
SP-8	BCAST-8	Esta interfaz proporciona un canal fuera de banda para el registro a través del canal de difusión general.
SP-9	N/A	Esta es la interfaz entre el terminal y la tarjeta inteligente. Esta interfaz no está presente para terminales que no tienen una tarjeta inteligente. NOTA: se requiere una argumentación adicional para determinar si la interfaz SP -9