(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 378 404**

(51) Int. CI.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07787939 .3**
(96) Fecha de presentación: **26.07.2007**
(97) Número de publicación de la solicitud: **2052516**
(97) Fecha de publicación de la solicitud: **29.04.2009**

(54) Título: **Método de acceso condicional local para equipos móviles**

(30) Prioridad:
02.08.2006 EP 06118345

(45) Fecha de publicación de la mención BOPI:
12.04.2012

(45) Fecha de la publicación del folleto de la patente:
12.04.2012

(73) Titular/es:
NAGRAVISION S.A.
22-24, ROUTE DE GENEVE
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:
MOREILLON, Guy

(74) Agente/Representante:
Tomas Gil, Tesifonte Enrique

DESCRIPCIÓN

Método de acceso condicional local para equipos móviles

Campo técnico

[0001] La invención se refiere al campo del acceso condicional a un flujo de datos digitales difundido por vía hertziana y recibido por una pluralidad de equipos móviles, tales como, por ejemplo, un teléfono móvil, un asistente personal PDA (Personal Digital Assistant), un receptor portátil de televisión digital, un ordenador portátil.

[0002] Los datos difundidos están encriptados y sólo se pueden recibir en claro por equipos autorizados cuyo usuario ha adquirido los derechos necesarios. Estos derechos, almacenados en un módulo de seguridad asociado al equipo móvil, consisten en un conjunto de claves que permiten decodificar las palabras de control contenidas en mensajes de control ECM (Entitlement Control Messaje) difundidos en el flujo de datos audio / video.

[0003] Un módulo de seguridad es un dispositivo conocido como inviolable que contiene diversas claves de encriptación / desencriptación, informaciones que sirven para identificar a un usuario en una red y datos que definen derechos adquiridos por el usuario para la recepción de un contenido difundido. El módulo de seguridad puede presentar formas diferentes tales como una tarjeta chip móvil insertada en un lector, un circuito integrado soldado sobre una tarjeta madre, una tarjeta del tipo tarjeta SIM (Subscriber Identity Module) que se encuentra en la mayoría de los equipos móviles.

[0004] Este módulo se puede realizar en forma de software y formar parte del software del equipo móvil. De preferencia, este software se ejecutará en una zona particular de la memoria con el fin de minimizar las intrusiones de otros software.

Antecedentes técnicos

[0005] Actualmente los equipos móviles configurados para la recepción de programas de televisión digital se basan en tecnologías normalizadas tales como OMA (Open Mobile Alliance), DVB-H (Digital Video Broadcast, Handheld), o DMB (Digital Multimedia Broadcasting) que es de algún modo una extensión de banda ancha de DAB (Digital Audio Broadcasting).

[0006] La tecnología OMA implementa una solución completa única para un mercado determinado como el de los teléfonos móviles donde cada equipo y los proveedores de contenido soportan la tecnología OMA.

[0007] La tecnología DVB fue concebida para normalizar los descodificadores de televisión digitales (set top boxes) con el fin de reducir sus costes a gran escala. Esta normaliza los elementos que intervienen al nivel del acceso condicional con respecto al contenido difundido en el formato MPEG-2 o MPEG-4 para la televisión móvil en Internet. Estos elementos consisten en el algoritmo de encriptación del contenido difundido, los mensajes de control ECM conteniendo las claves de desencriptación o palabras de control, los mensajes de administración EMM conteniendo los derechos de los usuarios y la interfaz entre el descodificador y el módulo de seguridad que controla el acceso condicional.

[0008] En el caso particular de la televisión móvil DVB-H, la protección del contenido se desarrolla por el grupo DVB-CBMS (Digital Video Broadcasting - Convergence of Broadcast and Mobile Services).

[0009] La normalización no se extiende ni al contenido de valor añadido de los mensajes ECM y EMM, ni al método de protección de éstos. Cada servidor de acceso condicional utiliza su propia estructura de datos y sus propios medios de protección para un mismo contenido difundido. La tecnología DVB ofrece así numerosas posibilidades de desarrollo de la seguridad del contenido.

[0010] Se conoce bien el hecho de permitir a un difusor que controle la recepción de un evento según el emplazamiento geográfico. De hecho, los difusores desean prohibir el acceso a un contenido tal como una retransmisión deportiva en los alrededores del lugar donde se desarrolla este evento. De este modo, por el conocimiento del emplazamiento de cada receptor, una orden llamada de «blackout» se envía al receptor, por ejemplo con el o los códigos postales que no pueden visualizar el evento en directo. El módulo de seguridad del receptor que contiene la información de localización (por ejemplo el código postal del abonado al servicio), al recibir este mensaje, va a aplicar por consiguiente una nueva regla durante la verificación de los derechos y aunque el receptor tenga los derechos para este evento, el mensaje de «blackout» tiene prioridad para prohibir el acceso al evento al no reenviar las palabras de control que han servido para encriptar el evento.

[0011] Sin embargo, en el ámbito móvil, esta noción de "código postal" ya no existe y no es posible prohibir una recepción sobre tal dispositivo portátil.

Breve descripción de la invención

[0012] El objetivo de la presente invención es que se pueda tener los mismos medios de restricción en el mundo móvil que lo que se aplica con receptores fijos.

[0013] Este objetivo se alcanza mediante un método de acceso condicional a un flujo de datos digitales encriptados con al menos una palabra de control y difundido a través de un emisor de una red de difusión con al menos un equipo móvil, este emisor transmitiendo también un flujo de mensajes de control conteniendo las palabras de control y las condiciones de acceso, este equipo móvil siendo conectado también a una red de comunicación móvil a través de un punto de acceso móvil, dicho método se caracteriza por el hecho de que incluye las siguientes etapas:

- recepción por el equipo móvil del flujo de mensajes de control,
- determinación de un identificador de localización de dicho móvil sea por el identificador del punto de acceso móvil o bien por el identificador del emisor de la red de difusión,
- verificación de las condiciones de acceso contenidas en el mensaje de control, dichas condiciones comprendiendo una condición de recepción ligada a al menos un identificador de punto de acceso móvil y/o de un identificador de emisor de la red de difusión,
- comparación entre el identificador de localización con el o los identificadores contenidos en las condiciones de acceso,
- autorización o bloqueo del acceso a dicho flujo de datos cuando la comparación es positiva.

[0014] Este método se puede utilizar para bloquear el acceso a los equipos móviles en una zona determinada (blackout), o al contrario para autorizar el acceso únicamente en esta zona (hot spot).

[0015] Según el modo de realización, la manera para determinar el identificador de localización se puede basar en el identificador de la célula móvil (punto de acceso móvil) o el identificador del emisor de la red de difusión.

[0016] En el primer caso, es muy probable que la precisión de localización sea más precisa debido al escaso alcance de los puntos de acceso móvil.

[0017] El documento WO 2005/036820 describe dos tipos de verificación hechas por un receptor, la verificación de los derechos a priori y la verificación del comportamiento a posteriori. Describe la implementación de un módulo de supervisión del funcionamiento del equipo móvil que tiene por tarea verificar un gran número de parámetros con el fin de determinar si el equipo tiene un comportamiento no autorizado. Uno de los parámetros se refiere a la función blackout que se activa gracias a un módulo GPS.

[0018] El documento US 2006/112188 describe un método de realización de la función "blackout" para un teléfono móvil. La solución propuesta consiste en identificar la posición del teléfono móvil, por ejemplo por la torre de transmisión (transmission tower) mediante la cual el teléfono tiene acceso a la red y para autorizar o prohibir la transferencia del contenido expuesto al "blackout" actuando directamente sobre la fuente de emisión. En el segundo caso, la red de difusión incluye una pluralidad de emisores que además de difundir el flujo de datos, difunden unos datos de servicio en los que se puede identificar el emisor sobre el cual se ha colocado el equipo móvil.

Breve descripción de las figuras

[0019] La invención se entenderá mejor gracias a la descripción detallada siguiente que se refiere a las figuras anexas provistas a modo de ejemplos en ningún modo limitativos.

- La figura 1 ilustra un esquema funcional de un ejemplo de configuración con dos emisores dispuestos en lugares distintos y que pueden ser captados por un equipo móvil local.
- La figura 2 ilustra un ejemplo esquematizado de zonas de difusión de los emisores de la red de difusión y de las células de la red móvil al interior de estas zonas de difusión.

Descripción detallada de la invención

[0020] Un flujo de datos digitales formando un contenido (C) encriptado con palabras de control (CW) se difunden con mensajes de control ECM. Estos datos digitales pueden comprender datos audio/vídeo de programas de televisión así como datos correspondientes a aplicaciones que se puede explotar por un equipo móvil.

[0021] Un servidor de un proveedor de contenidos de acceso condicional se conecta a una red de difusión (NET1). Esta red se difunde a través de varias antenas E1, E2 hacia unos equipos móviles EM1, EM2. Según la localización del equipo móvil, este último se conectará de preferencia a la antena E1 en vez de la antena E2.

[0022] De la misma manera, los equipos móviles EM1, EM2 se conectan a la red de telecomunicación móvil NET2 a través de antenas apropiadas F1, F2.

[0023] Tanto por medio de la red de antenas de difusión E1, E2 como por las antenas de telecomunicación móvil F1, F2, el equipo móvil puede determinar su posición geográfica. En el protocolo de comunicación de los dos sistemas de comunicación, el identificador de la antena se transmite al equipo móvil y sirve así de identificador de localización. Este identificador se utiliza por ejemplo para medir la calidad de recepción de una red.

[0024] Tal identificador no proporciona necesariamente una indicación geográfica y puede ser un simple valor alfanumérico.

[0025] Paralelamente, el emisor de difusión envía con el flujo de datos audio/vídeo, un flujo de datos de mensajes de control. El mensaje de control contiene la o las palabras de control que sirven para descodificar el contenido encriptado y contiene también las condiciones de acceso a este contenido.

[0026] Según la invención, las condiciones de acceso comprenden, además de los derechos necesarios para la recepción del contenido (abono por ejemplo), uno o unos identificadores de antenas relativo a la zona de prohibición o de autorización de recepción. Estos identificadores pueden referirse a la red de difusión NET1 o a la red de telecomunicación móvil NET2. Se puede incluir también en las condiciones de acceso una lista conjunta comprendiendo uno o unos identificadores de las dos redes.

[0027] Como se ve en la figura 2, es preferible usar los identificadores de la red de telecomunicación móvil C1 a Cn. La cobertura de cada célula es más pequeña, lo cual permite delimitar mejor la zona de prohibición. Sin embargo en ciertas circunstancias, por ejemplo para bloquear o autorizar el acceso a toda una ciudad, lo más sencillo es hacerlo a través de los identificadores de los emisores de difusión de esta ciudad.

[0028] Cuando un mensaje de control llega al equipo móvil, este mensaje se transmite a los medios de seguridad del equipo. Estos medios pueden ser, la tarjeta SIM del equipo móvil, un circuito especializado (soldado directamente sobre el circuito impreso), o bien estar realizado en forma de software. Estos medios de seguridad verifican si se cumplen las condiciones de acceso enumeradas en el mensaje de control. Estas condiciones pueden presentar varias formas, tales como un derecho específico a un contenido, un derecho general para un canal dado o un sistema de pago por tiempo tal y como se describe en la solicitud WO03/085959. Según la invención, además de las condiciones descritas previamente y ,siempre y cuando se haya limitado la recepción del contenido en función del emplazamiento geográfico, los medios de seguridad verifican si el identificador de localización obtenido de la antena de difusión o de telecomunicación está presente en la lista de identificadores incluida en el mensaje de control. Si el identificador de localización se incluye en la lista del o de los identificadores transmitidos en las condiciones de acceso, los medios de seguridad podrán, o bien reenviar la contraseña de control a los medios de desencriptación (versión hot spot) o al contrario bloquear la transmisión de la contraseña de control a los medios de desencriptación (blackout).

[0029] Se debe señalar que se encripta el mensaje de control con el fin de que un tercero no tenga acceso a los identificadores que sirven para restringir el acceso a los datos audio/vídeo. Según un modo particular de la invención, se puede firmar el identificador de localización con el fin de garantizar su integridad. El centro de difusión (o centro de telecomunicación según el modo de realización) utiliza su clave privada (de un par de claves asimétricas) para firmar el identificador. Esta firma se realiza de manera convencional por ejemplo utilizando un método de elección arbitraria (Hash) del identificador y de encriptación de resultado por la clave privada.

[0030] Durante la recepción, el módulo de seguridad posee la clave pública correspondiente, lo que le permite descodificar la firma para obtener el valor Hash supuesto y comparar este valor con el valor que el módulo de seguridad habrá calculado en el identificador de localización. La comparación del valor supuesto y del valor calculado permite, si son iguales, asegurarse de que no se ha modificado el identificador.

[0031] En un modo de realización particular, el módulo de seguridad se pre-inicializa mediante un valor de localización por defecto. Este valor se reemplaza por el identificador habitual cuando se ha comunicado al módulo de seguridad.

[0032] Cuando un mensaje de control llega a dicho módulo, y que contiene una orden de blackout, el valor por defecto se considera automáticamente parte de los identificadores de localización que deben estar en lista negra.

[0033] Según un modo de realización es posible definir una duración durante la cual un identificador es válido. Una vez terminada esta validez, y si no se ha transmitido ningún identificador más reciente al módulo de seguridad, se restablece el identificador por defecto, lo que tiene como consecuencia que éste se considere como activo en cada orden de blackout. Esta duración puede ser un parámetro del módulo de seguridad, o bien asociarse a los datos del identificador, por ejemplo a la firma. Para que no se pueda reutilizar un identificador, una fecha corriente se asocia al identificador, de preferencia

firmada con el propio identificador. De este modo, un identificador recogido previamente en otra célula no podrá reutilizarse en otro equipo móvil. A fin de reforzar la seguridad del conjunto, el módulo de seguridad negará todo identificador asociado a una fecha anterior a la del identificador transmitido previamente.

[0034] Además de las redes de telecomunicación conocidas como GSM, GPRS o UMTS, se puede utilizar otros medios de localización tales como por ejemplo Wifi, WiMax, Wibro, o cualquier red que disponga de un conjunto de antenas. La precisión de localización dependerá directamente de la densidad de antenas. Se debe señalar que el identificador contenido en el mensaje de control puede contener una serie de identificadores. Por ejemplo si los identificadores de las antenas en una ciudad comienzan todos por ABC (ABCV120, ABCJ11 etc.), es posible enviar únicamente el prefijo ABC para englobar todas las antenas ABCxxx. Otras posibilidades pueden incluir una serie tal como ABC100 a ABC200.

REIVINDICACIONES

1. Método de acceso condicional a un flujo de datos digitales encriptados con al menos una palabra de control y difundido a través de un emisor de una red de difusión con al menos un equipo móvil, este emisor transmitiendo además un flujo de mensajes de control conteniendo las palabras de control y las condiciones de acceso, este equipo móvil siendo conectado también a una red de comunicación móvil a través de un punto de acceso móvil, dicho método **se caracteriza por el hecho de que** incluye las etapas siguientes:

   - recepción por el equipo móvil del flujo de mensajes de control,
   - determinación por el equipo móvil de un identificador de localización de dicho móvil sea por el identificador del punto de acceso móvil o bien por el identificador del emisor de la red de difusión,
   - verificación por el equipo móvil de las condiciones de acceso contenidas en el mensaje de control, dichas condiciones comprendiendo una condición de recepción ligada a al menos un identificador de punto de acceso móvil y/o a un identificador de emisor de la red de difusión,
   - comparación entre el identificador determinado con el o los identificadores contenidos en las condiciones de acceso,
   - autorización o bloqueo del acceso a dicho flujo de datos si la comparación es positiva.

2. Método según la reivindicación 1, **caracterizado por el hecho de que** la autorización de acceso a dicho flujo de datos se autoriza sólo si el identificador de localización se incluye en la condición de recepción.

3. Método según la reivindicación 1, **caracterizado por el hecho de que** la autorización de acceso a dicho flujo de datos se autoriza sólo si el identificador de localización no se incluye en la condición de recepción.

4. Método según una de las reivindicaciones 1 a 3, **caracterizado por el hecho de que** el identificador de punto de acceso móvil se extrae de los datos de servicio recibidos de dicho punto de acceso móvil.

5. Método según una de las reivindicaciones 1 a 3, **caracterizado por el hecho de que** el identificador de emisor de la red de difusión se extrae de los datos de servicio recibidos de dicho emisor de la red de difusión.

6. Método según una de las reivindicaciones 1 a 5, **caracterizado por el hecho de que** las condiciones de acceso comprenden una lista de los identificadores de emisor de la red de difusión.

7. Método según una de las reivindicaciones 1 a 5, **caracterizado por el hecho de que** las condiciones de acceso comprenden una lista de los identificadores de punto de acceso móvil.

8. Método según una de las reivindicaciones 1 a 7, **caracterizado por el hecho de que** las condiciones de acceso comprenden al menos una descripción de un derecho relativo al contenido difundido y **por el hecho de que** el equipo móvil verifica la presencia de este derecho para autorizar o bloquear el acceso al contenido.

9. Método según una de las reivindicaciones 1 a 8, **caracterizado por el hecho de que** el equipo móvil incluye medios de seguridad encargados del tratamiento de las condiciones de acceso.

10. Método según una de las reivindicaciones 1 a 9, **caracterizado por el hecho de que** la red de comunicación móvil se selecciona en función de uno de los tipos GSM, GPRS, UMTS, WiMax, Wifi, Wibro.

11. Método según una de las reivindicaciones 1 a 9, **caracterizado por el hecho de que** el identificador contenido en las condiciones de acceso define una serie de identificadores de localización.

12. Método según una de las reivindicaciones 1 a 11, **caracterizado por el hecho de que** se firma el identificador de localización, y por el hecho de que el equipo móvil verifica la firma del identificador antes de su utilización para la comparación con el o los identificadores contenidos en las condiciones de acceso.

13. Método según una de las reivindicaciones 1 a 12, **caracterizado por el hecho de que** el equipo móvil incluye un identificador por defecto considerado como parte del o de los identificadores contenidos en las condiciones de acceso, que provocan el bloqueo del acceso a dicho flujo de datos si no se ha introducido ningún otro identificador.

14. Método según la reivindicación 13, **caracterizado por el hecho de que** una duración se asocia a la recepción de un identificador por el equipo móvil, el identificador por defecto siendo restablecido al expirar esta duración.

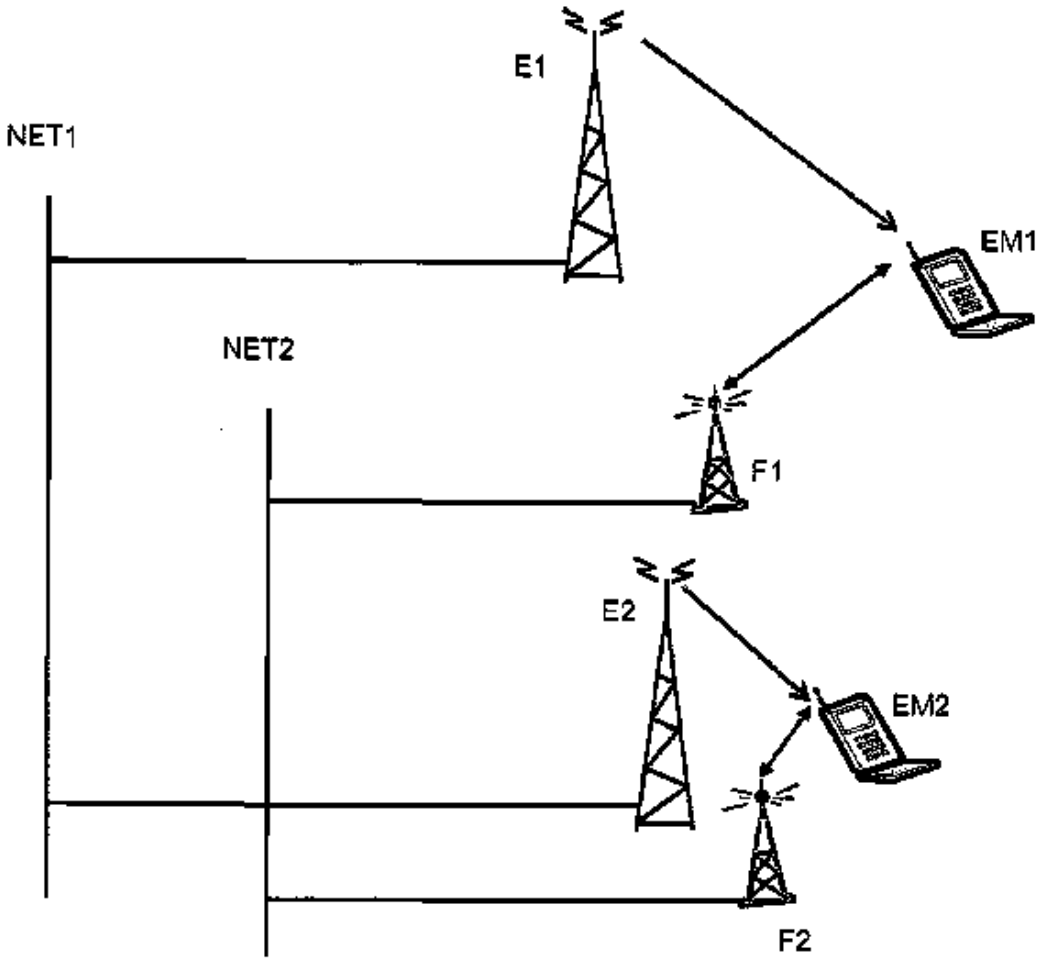

Fig. 1

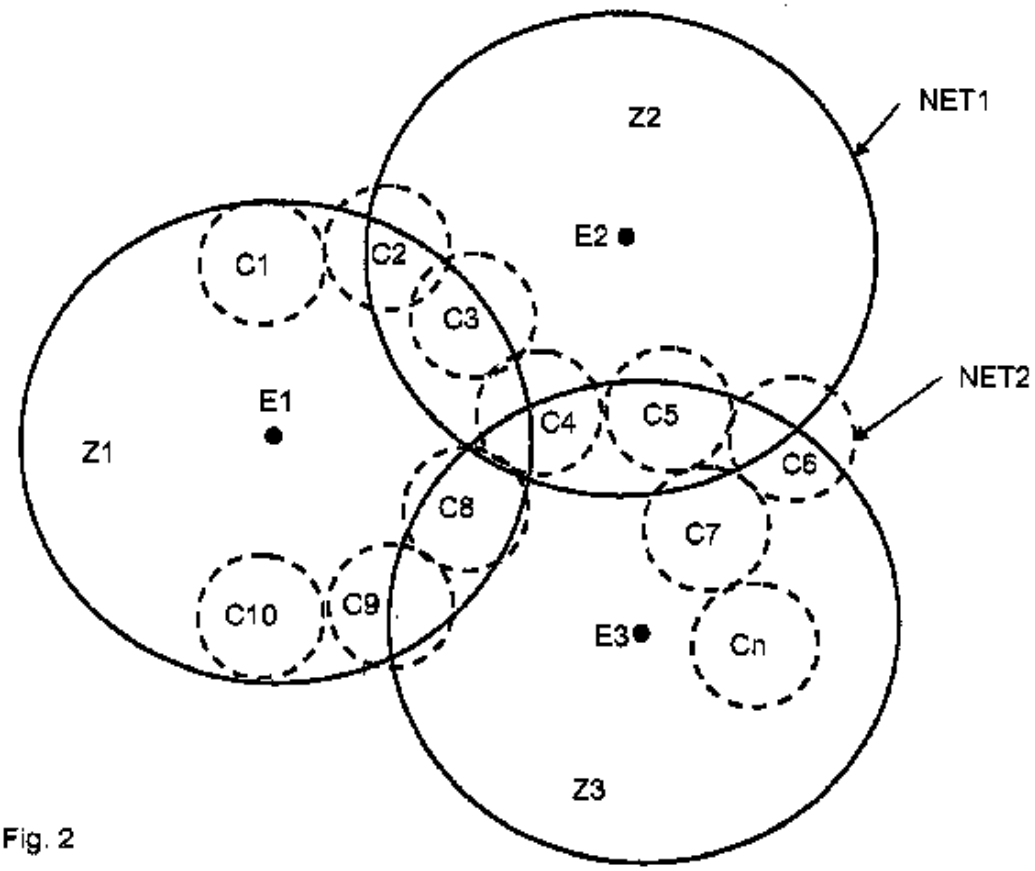

Fig. 2