(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 319 183**

(51) Int. Cl.:
H04N 7/167 (2006.01)
H04N 5/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03798315 .2**
(96) Fecha de presentación : **19.09.2003**
(97) Número de publicación de la solicitud: **1552694**
(97) Fecha de publicación de la solicitud: **13.07.2005**

(54) Título: **Sistema de descifrado de datos de acceso condicional.**

(30) Prioridad: **27.09.2002 CH 1623/02**
04.12.2002 CH 2048/02

(45) Fecha de publicación de la mención BOPI:
05.05.2009

(45) Fecha de la publicación del folleto de la patente:
05.05.2009

(73) Titular/es: **Nagravision S.A.**
22, route de Geneve
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es: **Nahum, Sylvain-Victor y**
Stransky, Philippe

(74) Agente: **Tomás Gil, Tesifonte Enrique**

DESCRIPCIÓN

Sistema de descifrado de datos de acceso condicional.

La presente invención se refiere a un sistema de descifrado de datos de acceso condicional.

Tales sistemas son utilizados particularmente en el campo de la televisión digital de pago. En tal caso, el flujo digital de datos transmitido hacia el televisor es cifrado con el fin de poder controlar la utilización y de definir condiciones para tal utilización. Este cifrado es realizado gracias a las palabras de control (Control Words) que son intercambiadas en intervalos regulares (normalmente entre 5 y 30 segundos, aunque unos intervalos claramente más largos puedan ser utilizados) con el fin de disuadir todo ataque destinado a encontrar de nuevo tal palabra de control.

Para que el receptor pueda descifrar el flujo cifrado por estas palabras de control, estas últimas le son enviadas independientemente del flujo en unos mensajes de control (ECM) cifrados por una clave propia del sistema de transmisión entre un centro de gestión y un módulo de seguridad de la unidad de usuario. Efectivamente, las operaciones de seguridad son efectuadas en un módulo de seguridad (SC) que es realizado generalmente en forma de tarjeta chip, conocida como inviolable. Este módulo puede ser de tipo móvil o estar integrado directamente en el receptor.

En el momento del descifrado de un mensaje de control (ECM), se ha verificado, en el módulo de seguridad (SC), que el derecho para acceder al flujo considerado está presente. Este derecho puede ser controlado por mensajes de autorización (EMM) que cargan tal derecho en el módulo de seguridad. Otras posibilidades son previsibles también tales como el envío de claves de descifrado.

Para la continuación de lo expuesto, se llamará "evento" un contenido video, audio (por ejemplo MP3) o datos (programa de juego por ejemplo) cifrado según el método conocido por las palabras de control, cada evento pudiendo ser cifrado por una o varias palabras de control, cada una teniendo una duración de validez determinada.

La contabilización de la utilización de tales eventos se basa en la actualidad en el principio del abono, de la compra de eventos o del pago por unidad de tiempo.

El abono permite definir un derecho asociado a uno o varios canales de difusión transmitiendo estos acontecimientos y permite al usuario obtener estos canales en claro si el derecho está presente en su módulo de seguridad.

Paralelamente, es posible definir derechos propios a un evento, tal como una película o un partido de fútbol. El usuario puede adquirir este derecho (compra por ejemplo) y este evento será gestionado específicamente por este derecho. Este método es conocido bajo la denominación de "pay-per-view" (PPV).

En lo que se refiere al pago por unidad de tiempo, el módulo de seguridad comprende un crédito cargado en función del consumo real del usuario. De este modo por ejemplo, una unidad será cargada cada minuto en este crédito sea cual sea el canal o evento. Es posible según las implementaciones técnicas, variar la unidad de contabilización, sea en la duración, o en el valor del tiempo concedido, e incluso combinando estos dos parámetros para adaptar la facturación al tipo de evento transmitido.

Un mensaje de control (ECM) no sólo contiene la palabra de control, sino también las condiciones para que esta palabra sea reenviada al receptor/descodificador. Durante el descifrado de las palabras de control, se comprobará si un derecho asociado a las condiciones de acceso enunciadas en el mensaje está presente en el módulo de seguridad.

La palabra de control es reenviada a la unidad de usuario sólo cuando la comparación es positiva. Esta palabra de control está contenida en un mensaje de control ECM que está cifrado por una clave de transmisión.

Para que el derecho esté presente en el módulo de seguridad, éste está cargado en general en este módulo por un mensaje de autorización (EMM) que por razones de seguridad, es cifrado en general por una clave diferente llamada clave de derecho (RK).

Según una forma conocida de difusión de televisión de pago, los tres elementos sucesivos son necesarios para descifrar un evento en un momento determinado:

- los datos relativos al evento cifrado por una o una pluralidad de palabras de control (CW),
- el o los mensajes de control ECM conteniendo las palabras de control (CW) y las condiciones de acceso (AC)
- el derecho correspondiente almacenado en el módulo de seguridad que permite verificar dichas condiciones de acceso.

Los sistemas de descifrado del tipo descrito más arriba están todos formados actualmente por equipamientos relativamente grandes. Estos están conectados a un dispositivo de explotación o de visualización como un televisor por

ejemplo por medio de un cable. No están previstos para poder ser desplazados fácilmente. En consecuencia, no es posible desplazar su propio descodificador y conectarlo simplemente en otro televisor, y adquirir derechos puntuales. Además, en los sistemas actuales, relativamente pocas instalaciones poseen una línea de retorno permitiendo comunicarse desde el descodificador hacia un centro de gestión. Las instalaciones que tienen una línea de retorno no tienen en general interfaz para poder comunicar fácilmente con ese centro de gestión. De hecho, las líneas de retorno están previstas para una comunicación entre el descodificador y el centro de gestión, pero no entre el usuario y ese centro. Es por lo tanto difícil adquirir derechos puntuales de manera rápida y sencilla. Además, en todos los sistemas conocidos, el flujo conteniendo los datos, los mensajes de control y los mensajes de autorización provienen de una fuente única que gestiona sus propios abonos, sin poder ofrecer una gama de abonos de diferentes fuentes.

La comunicación con un centro de gestión ha sido mejorada en sistemas permitiendo cargar unos derechos puntuales. Tal sistema está descrito en la patente norteamericana US 5,901,339. Este documento describe un sistema comprendiendo varios centros de difusión de datos o de eventos cifrados, destinados a transmitir estos eventos a un sistema de explotación como un televisor u otro medio de visualización. Estos eventos están asociados por una parte a un número de identificación único y por otra parte a un código de descifrado. El sistema incluye también un centro de carga al que son transmitidos, antes de la difusión, unos eventos, el número de identificación de cada evento, asociado al código de descifrado. Cuando un usuario desea adquirir derechos para descifrar un evento cifrado, llama el centro de carga por medio de un aparato de comunicación tal como un teléfono, e indica el número de identificación del evento que quiere adquirir. El centro de carga transmite al aparato de comunicación, el código de descifrado del evento considerado. A su vez, el aparato de carga transmite ese código al descodificador del usuario. Cuando el evento es difundido, el descodificador posee el código de descifrado y el evento puede ser descifrado y visualizado.

Este sistema implica cierto número de restricciones. En particular, puesto que el código de descifrado es recibido a petición del usuario, no es cómodo utilizar varios códigos para un mismo evento. Este código debe ser el mismo durante toda la duración de este evento. Esto presenta un inconveniente desde el punto de vista de la seguridad. Como comparación, en los sistemas actuales, las palabras de control utilizadas para el cifrado y descifrado de eventos son intercambiadas en intervalos que pueden variar de 2 a 30 segundos aproximadamente.

En el sistema según US 5,901,339, varios centros de difusión están conectados a un único centro de carga. Esto implica particularmente que todos los difusores tengan que instalar sus medios criptográficos en el mismo centro de carga, lo cual no es óptimo desde el punto de vista de la seguridad.

Este sistema presenta también otros defectos relativos a la seguridad. Por una parte, la transmisión del código de descifrado entre el centro de carga y el descodificador del usuario se efectúa por medio de una línea telefónica a través de un teléfono sin medio de seguridad. Esto implica que sea relativamente fácil obtener este código de forma ilegal y utilizarlo con respecto a otro descodificador. Por otra parte, como el centro de carga no dispone de ninguna información relativa al descodificador que requiera el código de descifrado, se puede utilizar este código en cualquier descodificador. Eso significa que una vez adquirido en toda legalidad, el código de descifrado puede ser transmitido fácilmente a otros descodificadores para descifrar ilegalmente un evento o datos.

El documento "EBU Technical Review" Winter 1995 Nº. 266 denominado "Functional model of a conditional access system" describe variantes de sistemas diferentes de acceso condicional destinados particularmente a la televisión de pago, estos sistemas utilizando un descifrado de dos niveles, es decir un primer nivel protegido por unos mensajes de control ECM y un segundo nivel utilizando mensajes de autorización EMM. En una de estas variantes, el sistema de acceso condicional está destinado a ser utilizado simultáneamente por varios difusores de datos de acceso condicional. El sistema tal como está descrito incluye principalmente un sistema de control de los derechos, encargado de generar y enviar los mensajes de autorización EMM, y un sistema de control de autorizaciones encargado de generar palabras de control para el cifrado de los datos de los difusores.

En todos los ejemplos representados y descritos en este documento, cada difusor está asociado de manera unívoca a un sistema de gestión de los derechos. No es posible asociar un único difusor a varios sistemas de gestión de derechos. En el sistema según este documento, el hecho de utilizar uno o varios proveedores de servicios es totalmente transparente para el usuario. De hecho, éste no puede elegir un operador u otro, sólo puede elegir un servicio, tanto si hay uno como si hay varios operadores.

Este sistema no permite resolver los problemas ligados con el desplazamiento simple del descodificador y la adquisición de derechos puntuales, ni el problema de comunicación entre el usuario y el centro de gestión.

La presente invención se propone paliar los inconvenientes de los sistemas del estado de la técnica anterior y realizar un sistema que pueda ser desplazado fácilmente y utilizado en prácticamente cualquier dispositivo de explotación adaptado. Además, tal sistema simplifica la gestión de los derechos de acceso al nivel del centro de difusión y ofrece una mayor flexibilidad al usuario al mismo tiempo que garantiza una seguridad óptima tal que las informaciones obtenidas por un usuario y destinadas a un descodificador determinado no pueden ser utilizadas en otro descodificador.

Estos objetivos son alcanzados por un sistema de descifrado de datos de acceso condicional, tal como está definido en la reivindicación 1.

La presente invención y sus ventajas serán mejor comprendidas en referencia a la descripción de diferentes modos de realización y a los dibujos anexos, en los que:

- la figura 1 representa una visión general de un primer modo de realización del sistema según la presente invención; y

- la figura 2 es una visión general de un segundo modo de realización de la invención.

En referencia a estas figuras, el sistema de la invención incluye esencialmente un centro de difusión 10 dispuesto para difundir datos cifrados, al menos un centro de gestión 11 dispuesto para difundir mensajes de autorización (EMM) y tratar la gestión de derechos de acceso a los datos cifrados, un dispositivo de explotación 12 destinado a convertir estos datos cifrados en utilizables, y un descodificador 13 dispuesto para descifrar al menos una parte de los datos cifrados.

El centro 10 de difusión de datos cifrados puede ser un dispositivo tradicional por cable o por satélite particularmente. Este centro emite datos en forma cifrados. La naturaleza de estos datos depende por supuesto de la utilización que se debe hacer de éstos. En el texto a continuación, los datos están utilizados supuestamente en un sistema de televisión de acceso condicional. Los datos son formados en consecuencia por un contenido video CT, es decir imágenes y sonido. Otros datos específicos para el uso también pueden estar incluidos, de manera bien conocida por el experto en la materia. Estos datos, o al menos una parte de éstos, son cifrados por medio de palabras de control y son anotados cw(CT) en las figuras.

Según una primera forma de realización, las palabras de control cw son transmitidas, en forma cifrada, por el centro de difusión al mismo tiempo que los datos cifrados. Según otra forma de realización, estas palabras de control pueden ser difundidas por el centro de gestión 11 debido al hecho de que la encriptación del mensaje de control, comprendiendo la palabra de control, es gestionada específicamente según un protocolo propio a cada centro de gestión.

La denominación "mensaje personal" representa un mensaje de autorización (EMM) en caso de que los mensajes de control (ECM) no sean específicos, estos mensajes personales permitiendo el acceso a los datos por la memorización de un derecho. La palabra de control es extraída de este mensaje y enviada al módulo de recepción generalmente en forma cifrada, de tal forma que las palabras de control no puedan ser copiadas en este nivel y enviadas a otro usuario.

El o, más generalmente, los centros de gestión 11 se encargan de gestionar los derechos de acceso a los datos. Estos pueden gestionar cada uno diferentes tipos de derechos, particularmente abonos, accesos puntuales, paquetes de programas diferentes. Para realizarlo, estos difunden también los mensajes de autorización (EMM) correspondientes, con destino a descodificadores relativos.

El dispositivo de utilización 12 está adaptado, por supuesto, a los datos para transmitir. En el caso elegido de televisión de acceso condicional, el dispositivo de explotación es un televisor.

El descodificador 13 incluye un módulo de recepción y de descifrado 14 de los datos y un módulo de gestión 15 de los derechos de acceso a estos datos. El módulo de gestión de los derechos es realizado de tal manera que sea fácilmente portátil. Puede juiciosamente ser realizado a través de un teléfono móvil. El módulo de gestión incluye también un módulo de seguridad 16. Este módulo de recepción y de descifrado puede comprender medios de comunicación estandardizados con el módulo de gestión. De este modo, el módulo de recepción es capaz de dialogar con cualquier módulo de gestión.

Un módulo de seguridad evolucionado puede comprender zonas de memoria propias a cada centro de gestión. En el caso de un teléfono móvil, el operador de telefonía puede conceder unas zonas de memoria que serán inicializadas después por unos parámetros propios a cada centro de gestión. Estos parámetros son por ejemplo una clave de desencriptación de los mensajes de autorización (EMM), la identificación del abonado según el sistema propio a dicho centro de gestión, incluso un crédito.

En el caso que unos operadores diferentes no deseen integrar su seguridad en un módulo común, o simplemente para aumentar la flexibilidad de uso, se puede prever un sistema de conexión que permita cambiar fácilmente de módulo de seguridad, o bien utilizar varios a la vez. Estos módulos pueden ser realizados en forma de tarjeta chip cooperando con un lector apropiado del módulo de gestión o en una forma más compacta permitiendo la instalación de varios módulos de seguridad simultáneamente. En tal caso, cada chip controla las autorizaciones procedentes de uno de los centros de gestión.

También es posible prever una tarjeta u otro soporte comprendiendo varios chips, cada uno de ellos controlando las autorizaciones procedentes de uno de los centros de gestión. Tal módulo de seguridad es ilustrado por la figura 2, con la referencia 16.

El módulo de seguridad, o cada uno de los módulos si existen varios, contiene un número de identificación único (UA) y datos propios de los centros de gestión 11 con los que estos módulos están autorizados a comunicar. Eso significa que antes de poder obtener y descifrar un mensaje de autorización (EMM) procedente de un centro de gestión, los datos relativos a este centro de gestión deben haber sido cargados previamente en el módulo de seguridad. Los

datos propios del centro de gestión son por ejemplo una clave de cifrado o un código permitiendo formar una clave de cifrado, estos datos permitiendo proteger el enlace entre el centro de gestión y el módulo de seguridad. Según un modo de realización ventajoso, los mensajes de autorización EMM son enviados al módulo de seguridad en forma cifrada a través de una clave que depende a la vez del centro de gestión referido y del número de identificación única UA de ese módulo de seguridad. De esta manera, un mensaje de autorización recibido por un módulo de seguridad no podrá ser utilizado por otro módulo. Además, un módulo falsificado, que no contiene los datos propios del centro de gestión no podrá utilizar el mensaje de autorización ya que no será capaz de descifrarlo.

El módulo de gestión 15 incluye ventajosamente un lector de tarjeta chip destinado a ser utilizado con una tarjeta de crédito o una tarjeta de prepago 17. De esta manera, se garantiza la gestión de los pagos cuando un evento es solicitado. Esto permite además el uso del módulo de gestión como monedero electrónico. Tal tarjeta está ilustrada con la referencia 17 en la figura 2.

Según un modo de realización poniendo en funcionamiento varios centros de gestión para los datos difundidos hacia el módulo de recepción, se ha previsto añadir a dichos datos cifrados informaciones descriptivas para permitir al usuario conectarse en el centro de gestión apropiado. Estas informaciones descriptivas son transmitidas desde el módulo de recepción hacia el módulo de gestión y pueden ser visualizadas en dicho módulo. El usuario puede efectuar su elección e iniciar una comunicación con un centro, siempre y cuando su módulo de seguridad soporte las funciones de seguridad exigidas por este centro de gestión. Estas informaciones descriptivas, además de describir el producto video o audio, comprenden una dirección de tipo telefónico o Internet. Esta dirección será utilizada para el diálogo en vista del envío del mensaje personal permitiendo recibir los derechos o las claves necesarias para el acceso a los datos cifrados.

El módulo de recepción y de descifrado 14 de los datos puede ser integrado directamente en el aparato de televisión 12. En ese caso, para poder leer unos datos cifrados en tal televisor, sólo se debe tener el módulo de gestión 15 y los derechos correspondientes al evento deseado. Este evento puede así ser visualizado a partir de cualquier televisor equipado de manera adecuada. Este modo de realización está ilustrado esquemáticamente por la figura 2. Según otra forma de realización ventajosa, puede estar formado por una caja que puede ser conectada a la televisión por medio de un cable de conexión o directamente por una salida en el televisor. Esto permite utilizar de forma sencilla, la presente invención en televisores existentes.

El sistema según la invención funciona de la manera siguiente:

Como se ha mencionado previamente, el contenido video CT es difundido por el centro de difusión 10 de datos cifrados. Simultáneamente, este primer centro difunde también la o las palabras de control cw que han sido utilizadas para cifrar los datos. Cuando se desea utilizar los datos del sistema de acceso condicionado, por ejemplo, para ver un evento tal como una película o un partido de fútbol por ejemplo, para el cual el acceso está sometido a un derecho, es necesario en primer lugar adquirir este derecho. Éste puede ser proporcionado por una tarjeta de prepago dispuesta en el módulo de gestión 15, o puede estar cargado en este módulo gracias a los medios de comunicación entre el módulo y uno de los centros de gestión 11, que gestiona los derechos de acceso.

Para obtener los mensajes de autorización EMM que van a permitir el descifrado de las palabras de control cw necesario para el descifrado de los datos y por lo tanto para la visualización del evento, el módulo de recepción y de descifrado 14 establece una comunicación con uno de los centros de gestión. Como se ha mencionado previamente, el módulo de recepción puede estar formado por un teléfono móvil. En tal caso, el contacto es establecido tecleando un número de teléfono correspondiente al centro de difusión. La elección del evento para el cual se desea adquirir los derechos se hace a través de un "menú" preregistrado, cada elección del menú correspondiente a un número particular en el teclado del teléfono móvil. La descarga del mensaje de autorización correspondiente al evento elegido se realiza después de haber pulsado una tecla de validación en el teclado del teléfono. Este mensaje de autorización es cifrado de manera ventajosa por medio de una clave dependiendo a la vez del número de identificación único UA del módulo de seguridad y de los datos propios del centro de gestión.

El módulo de recepción y de descifrado 14 está conectado al televisor, por ejemplo en una salida de éste o integrado directamente en el televisor.

En un primer modo de realización, el módulo de recepción 14 recibe, procedentes del primer dispositivo de difusión 10, los datos cifrados cw (CT) por medio de palabras de control cw así como las propias palabras de control cw. También recibe los mensajes de autorización EMM procedentes de uno de los centros de gestión 11. El módulo de recepción 14 transmite las palabras de control cw al módulo de gestión de los derechos. Esta transmisión puede ser efectuada por medio de ondas infrarrojas o radio por ejemplo. Este módulo de gestión de los derechos verifica que ha adquirido correctamente los derechos correspondientes al evento elegido. Si éste es el caso, los mensajes de control ECM son tratados en el módulo de seguridad para extraer de éstos las palabras de control cw. Estos son transmitidos después, a una frecuencia adecuada correspondiente a la frecuencia utilizada para el cifrado de los datos, al módulo de recepción 14 que los utiliza entonces para descifrar los datos y hacer así que el evento sea visible.

En un segundo modo de realización, ilustrado esquemáticamente por la figura 2, el flujo conteniendo los datos cifrados, los mensajes de control y los mensajes de autorización es recibido por el dispositivo de gestión de los derechos 15. Estos flujos son tratados como previamente y los datos descifrados son transmitidos en claro al dispositivo receptor.

Este sistema permite realizar un descodificador transportable fácilmente y que puede ser utilizado en cualquier televisor. En el caso de que el módulo de recepción de los datos 14 esté integrado en el televisor, sólo se debe disponer del módulo de gestión 15 para tener acceso a un evento. De esta manera, las restricciones para los usuarios son suprimidas. Además, el hecho de utilizar centros de gestión para los mensajes de autorización, distintos del centro de difusión de los datos aumenta la elección ofrecida al usuario y facilita el uso de sistemas de acceso condicional.

Debido al hecho de que las palabras de control están descifradas en el módulo de gestión y transmitidas hacia el módulo de recepción, la comunicación entre estos dos módulos será preferiblemente protegida. Por eso, existen diferentes procedimientos de emparejamiento generalmente adaptados a la pareja formada por la unidad de seguridad y el descodificador. En nuestro caso, estos procedimientos están aplicados entre el módulo de recepción y el módulo de gestión. Un ejemplo de este tipo de emparejamiento se describe en la solicitud WO 02/052515.

Para garantizar que las palabras de control no son diseminadas hacia otros módulos de recepción y de descifrado, y en un esquema de dos niveles es decir cuando el mensaje de control es de tipo personal, el centro de gestión puede solicitar una clave de cifrado propia del módulo de descifrado. Esta clave es codificada directamente en el módulo de descifrado y es única para cada módulo.

En el caso de que los mensajes de control ECM conteniendo las palabras de control cw sean enviados por el centro de gestión, o en el caso similar de que un evento sea cifrado por medio de una única clave enviada al módulo de seguridad por un centro de gestión, este centro de gestión aplica, sobre una palabra de control determinada, una encriptación propia a la clave única del módulo de descifrado, y después una encriptación propia al sistema de telecomunicación entre el centro de gestión y el módulo de seguridad al módulo de seguridad del módulo de gestión. De este modo, si este mensaje estaba interceptado por un módulo de seguridad falsificado, la palabra de control obtenida sería inutilizable para otro módulo de descifrado puesto que aún está codificada por la clave única de este módulo.

Según un modo de realización, el enlace entre el módulo de gestión y el centro de gestión es un enlace punto por punto protegido. Es entonces posible transmitir solicitudes en relación con las imágenes y eventos difundidos por el centro de difusión. Esta función es utilizada para disponer solicitudes a través del módulo de gestión o respuestas a interrogaciones.

En una forma de aplicación, las imágenes difundidas hacia el descodificador son imágenes reales procedentes de juegos de casino tales como la ruleta, el black jack y el titular de tal módulo de gestión puede de manera interactiva y en tiempo real, jugar desde el lugar donde se encuentra. Los medios de seguridad instalados para el acceso condicional a los datos teletransmitidos también pueden ser utilizados para este tipo de aplicación. En este tipo de aplicación, el casino está conectado con el centro de gestión para determinar la identidad del portador del módulo de gestión o al menos que este portador sea solvente. El centro de gestión concede un crédito a este portador y comunica esta información al casino.

Referencias citadas en la descripción

Esta lista de referencias citada por el solicitante ha sido recopilada exclusivamente para la información del lector. No forma parte del documento de patente europea. La misma ha sido confeccionada con la mayor diligencia; la OEP sin embargo no asume responsabilidad alguna por eventuales errores u omisiones.

Documentos de patente citados en la descripción

- US 5901339 A [0015] [0017]
- WO 02052515 A [0046]

Bibliografía distinta de patentes citada en la descripción

- Functional model of a conditional access system *EBU Technical Review*, 1995 [0019].

REIVINDICACIONES

1. Sistema de descifrado de datos con acceso condicional, este sistema poniendo en obra:

- un centro de difusión (10) dispuesto para difundir datos cifrados por al menos una palabra de control (cw),
- al menos dos centros de gestión (11) dispuestos para difundir los mensajes personales (ECM, EMM) relativos a la gestión de los medios de acceso a los datos cifrados,
- un dispositivo de explotación (12) destinado a convertir dichos datos cifrados en utilizables, y
- un descodificador (13) dispuesto para descifrar al menos una parte de los datos cifrados, instalado entre el centro de difusión (10) y el dispositivo de explotación (12),

caracterizado por el hecho de que

- el descodificador (13) está formado por un módulo de recepción y de descifrado (14) de los datos cifrados y por un módulo de gestión (15) de los derechos de acceso a estos datos, estos módulos siendo distintos físicamente, el módulo de recepción (14) estando conectado al dispositivo de explotación (12) y el módulo de gestión (15) estando dispuesto para comunicar con el módulo de recepción,
- de que el módulo de gestión (15) incluye un módulo de seguridad (16) comprendiendo un número de identificación único (UA) y datos que permiten proteger el enlace entre los centros de gestión (11) y el módulo de seguridad (16), este módulo de seguridad estando dispuesto para verificar el contenido de los mensajes personales (ECM, EMM) y para permitir o impedir el descifrado de la o de las palabras de control (cw) en función del contenido de los mensajes personales,
- de que el módulo de recepción (14) recibe los datos cifrados procedentes de dichos centros de difusión (10) a través de una primera vía de comunicación, y el módulo de gestión (15) recibe los mensajes personales (ECM, EMM) por el centro de gestión (11) a través de una segunda vía de comunicación
- y por el hecho de que el módulo de seguridad del módulo de gestión incluye datos propios a dichos centros de gestión (11) con los que puede comunicar.

2. Sistema de descifrado de datos según la reivindicación 1, **caracterizado** por el hecho de que la comunicación entre el módulo de recepción (14) y el módulo de gestión (15) es una comunicación por ondas.

3. Sistema de descifrado de datos según la reivindicación 1, **caracterizado** por el hecho de que el módulo de gestión (15) de los derechos es un teléfono móvil.

4. Sistema de descifrado de datos según la reivindicación 3, **caracterizado** por el hecho de que el módulo de seguridad (16) incluye las funciones de identificación necesarias a la telefonía, y al menos una zona memoria propia de un centro de gestión (11), esta zona comprendiendo los parámetros de seguridad para la recepción de los mensajes de autorización (EMM) de dicho centro de gestión.

5. Sistema según las reivindicaciones 1 a 4, **caracterizado** por el hecho de que el centro de difusión (10) está dispuesto para difundir los mensajes de control (ECM) comprendiendo la o las palabras de control (cw), y por el hecho de que los mensajes personales difundidos por los centros de gestión (11) corresponden a un mensaje de autorización (EMM).

6. Sistema según las reivindicaciones 1 a 4, **caracterizado** por el hecho de que los centros de gestión (11) están dispuestos para difundir mensajes personales comprendiendo la o las palabras de control (cw), el módulo de seguridad (16) del módulo de gestión (15) disponiendo de los medios para determinar si este mensaje le está destinado y de medios para transmitir esta palabra de control (cw) al módulo de recepción (14).

7. Sistema según la reivindicación 6, **caracterizado** por el hecho de que el módulo de recepción y de descifrado (14) comprende una clave única de desencriptación aplicada a la contraseña de control (cw), esta clave sirviendo para encriptar las palabras de control en el centro gestión (11) antes de su transmisión hacia el módulo de gestión (15).

8. Sistema de descifrado de datos según la reivindicación 1, **caracterizado** por el hecho de que el módulo de seguridad (16) del módulo de gestión (15) incluye parámetros de seguridad para la recepción de los mensajes de autorización (EMM) procedentes de centros de gestión (11) distintos.

9. Sistema de descifrado de datos según las reivindicaciones 1 a 8, el centro de difusión (10) estando dispuesto para transmitir las informaciones descriptivas de los datos cifrados, **caracterizado** por el hecho de que estos datos contienen las indicaciones necesarias en el establecimiento de una comunicación con el centro de gestión (11) encargado de la

autorización de estos datos, y son transmitidas al módulo de gestión (15), este último estando dispuesto para establecer una comunicación con el centro de gestión (11) en cuestión para obtener el mensaje de autorización (EMM).

10. Sistema de descifrado de datos según cualquiera de las reivindicaciones, **caracterizado** por el hecho de que el módulo de recepción y de descifrado (14) está integrado en el dispositivo de explotación (12).

11. Sistema de descifrado de datos según la reivindicación 1, **caracterizado** por el hecho de que el módulo de recepción y de descifrado (14) incluye medios de comunicación estandardizados con el módulo de gestión (15) de tal forma que un módulo de recepción y de descifrado (14) pueda dialogar con una pluralidad de módulos de gestión (15).

12. Sistema de descifrado de datos según cualquiera de las reivindicaciones precedentes, **caracterizado** por el hecho de que el módulo de gestión (15) comprende medios para establecer una clave de emparejamiento con el módulo de recepción (14), esta clave estando destinada a encriptar y desencriptar al menos la o las palabras de control (cw) transmitidas desde el módulo de gestión (15) hacia el módulo de recepción (14).

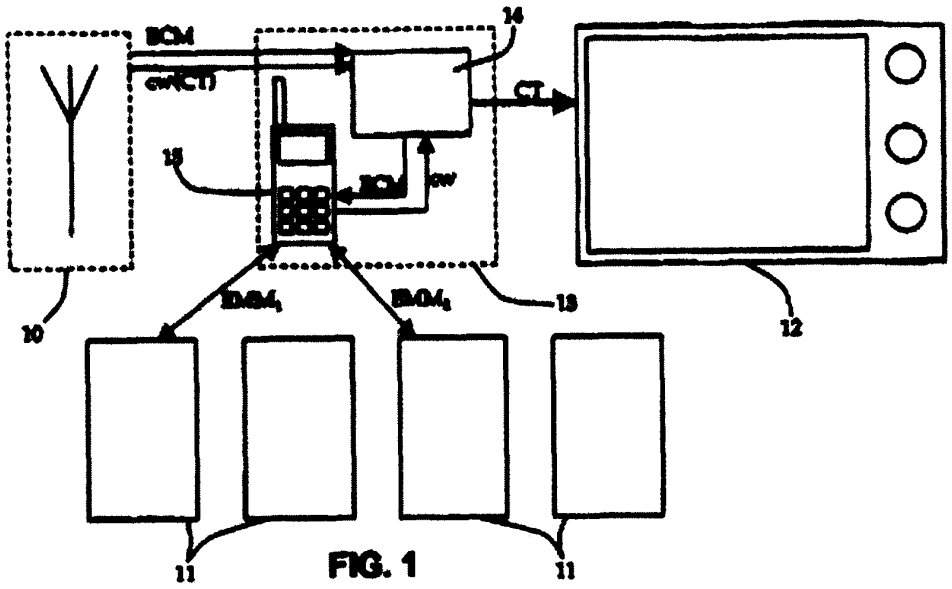

FIG. 1

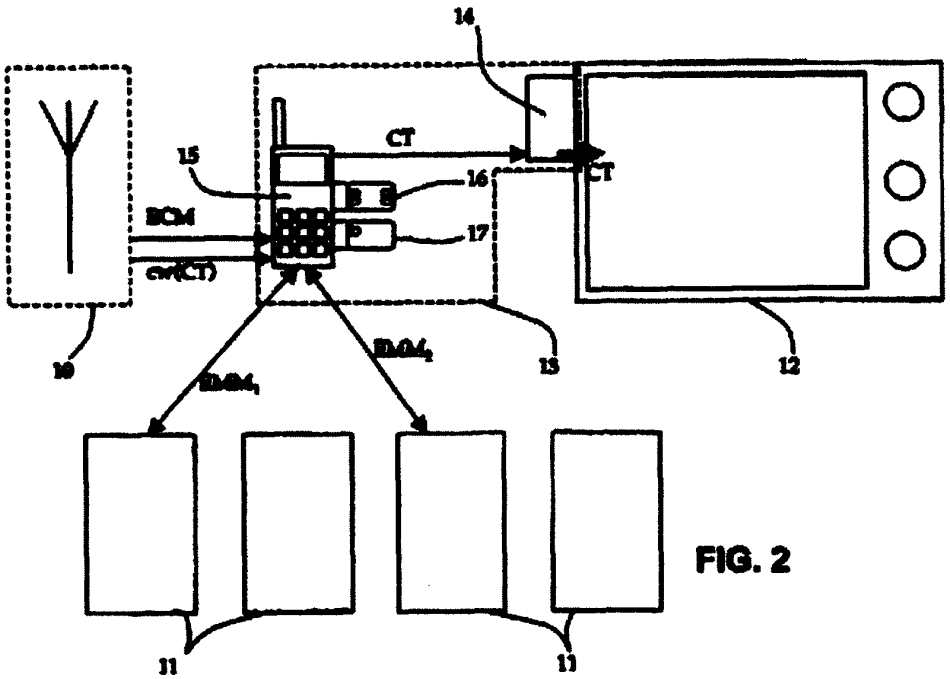

FIG. 2