(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 368 958**

(51) Int. CI.:
H04N 5/44 (2011.01)
H04N 5/765 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07823317 .8**
(96) Fecha de presentación: **20.07.2007**
(97) Número de publicación de la solicitud: **2047676**
(97) Fecha de publicación de la solicitud: **15.04.2009**

(54) Título: **ENTIDAD ELECTRÓNICA PORTÁTIL EXTRAÍBLE ASEGURADA, QUE COMPRENDE MEDIOS PARA AUTORIZAR UNA RETRANSMISIÓN DIFERIDA.**

(30) Prioridad:
31.07.2006 FR 0653212

(45) Fecha de publicación de la mención BOPI:
24.11.2011

(45) Fecha de la publicación del folleto de la patente:
24.11.2011

(73) Titular/es:
OBERTHUR TECHNOLOGIES
50 quai Michelet
92300 Levallois-Perret, FR

(72) Inventor/es:
BERTIN, Marc

(74) Agente: **Lehmann Novo, Isabel**

DESCRIPCIÓN

Entidad electrónica portátil extraíble asegurada, que comprende medios para autorizar una retransmisión diferida

La presente invención se refiere a una entidad electrónica portátil protegida extraíble que comprende medios para autorizar una retransmisión diferida. Se aplica, en particular, a los soportes de información extraíbles que incluyen medios de protección como, por ejemplo, tarjetas de circuito integrado de microcontrolador protegido, por ejemplo, conformes a la norma ISO 7816, llaves USB (Bus Serie Universal), tarjetas SD (Digital Protegido) o una tarjeta de microcircuito conforme a la especificación de MMC (Lector de Memoria Multimedia).

La invención se refiere, además, a un dispositivo electrónico de lectura de una tal entidad electrónica o terminal central, que comprende medios de retransmisión diferida del contenido de la entidad y ocasionalmente, medios de recepción de un contenido difundido.

La presente invención encuentra una aplicación en la recepción de un flujo de datos multimedia difundido, en particular, la recepción de la televisión digital terrestre o de flujos audiovisuales difundidos en una red informática, por ejemplo Internet o telefónica y en particular, la recepción de cadenas de pago, de segmentos musicales o de películas, que necesitan un abono o un pago previo a la visualización.

Un ejemplo de entidad electrónica portátil es una llave electrónica, denominada *dongle,* que comprende, en general, una interfaz que le permite conectarse a un terminal central, que puede ser una estación de trabajo, un ordenador, un teléfono móvil, un asistente personal, una televisión digital, un lector MP3, por ejemplo. Con más frecuencia, la interfaz de la llave electrónica está conforme a la norma USB (Bus Serie Universal) que describe un sistema de bus serie universal desarrollado para garantizar una gestión simple y rápida de los intercambios de datos entre un terminal central y un dispositivo periférico, por ejemplo una entidad electrónica portátil, un teclado u otro dispositivo electrónico. La interfaz de la entidad electrónica puede, asimismo, estar conforme a otras normas tales como la norma ISO 7816, la norma PCMCIA (acrónimo de “Personal Computer Memory Card International Association” que significa Asociación Internacional para las Tarjetas de Memoria de Ordenadores Personales) o la norma MMC. La entidad electrónica portátil puede comprender, además, una interfaz sin contacto, en particular, una interfaz conforme a la norma WIFI o Bluetooth (marcas registradas) o ISO 14443.

El flujo de datos multimedia difundido comprende, en particular, datos multimedia y/o datos de programas. En el caso de datos multimedia, se requiere una aplicación de audio y/o visual que permite la visualización o la audición de los datos. En el caso de datos de programas, se recurre a medios para ejecutar los datos. Los datos están, en particular, bajo forma digital, por ejemplo en el formato MPEG o de tipo de DVB (Difusión de Vídeo Digital).

Es conocido a partir del documento EP 1 633 133, titulado “Aparato portátil para permitir la reproducción de televisión”, una llave USB que comprende medios de recepción de un flujo de datos difundido, denominado también flujo “broadcasted” en tecnología anglosajona y medios de conexión a un terminal central para transmitir al terminal central datos emitidos desde el flujo de datos objeto de recepción. La llave USB, descrita en este documento, puede comprender, además, medios de re-codificación y de compresión de datos.

Sin embargo, este dispositivo descrito no permite asegurar la restitución de los datos recibidos.

Este dispositivo no confiere, en efecto, un grado de seguridad totalmente satisfactorio en la medida en que ni el terminal central, ni la entidad electrónica no están asegurados. De lo anterior se deduce que una persona mal intencionada puede obtener los datos del flujo y utilizarlos sin haber adquirido los derechos asociados a estos datos.

Es necesario, en particular, en lo que respecta a las cadenas de pago, en efecto, que solamente los usuarios que hayan adquirido una autorización, también denominada licencia, estén en condiciones de recibir los datos.

Se conoce la existencia de receptores de televisión que comprenden medios de memorización, capaces de restituir, en un instante dado, un programa grabado con anterioridad, registrando un programa difundido en el mismo instante. A continuación, se denomina esta funcionalidad como “la retransmisión diferida”. Dichos receptores se describen, en particular, en las solicitudes de patente US 5.241.428 y EP -789488.

Asimismo, se conoce el documento JP2004193944 que describe una retransmisión diferida aplicada a un teléfono móvil capaz de recibir y de visualizar un programa de televisión, siendo el programa en curso de difusión automáticamente grabado durante una conversación telefónica con el fin de que el usuario pueda, más adelante, visualizar el programa grabado.

Sin embargo, el registro de una parte de un contenido difundido, para realizar la función de retransmisión diferida, plantea problemas de seguridad. Se quiere, en efecto, impedir la copia ilícita del contenido difundido.

La presente invención trata de subsanar estos inconvenientes. A este respecto, la presente invención se refiere a una entidad electrónica portátil, con seguridad informática, extraÍble que comprende:

- medios de recepción de un contenido digital difundido,

- medios de emisión de dicho contenido digital difundido recibido,

- medios protegidos de retransmisión diferida del contenido digital recibido adaptados para prohibir una reproducción del contenido digital recibido antes de su emisión y para provocar la emisión, por los medios de emisión, de modo diferido en el tiempo, del contenido digital recibido,

- estando dichos medios adaptados para funcionar en paralelo o casi en paralelo.

Gracias a estas disposiciones el contenido digital difundido es objeto de recepción y se puede retransmitir, en particular, hacia medios de procesamiento o de visualización en diferido y de manera protegida.

A este respecto, los medios de recepción realizan la recepción del contenido digital difundido, mientras que el contenido ya recibido está en curso de retransmisión en un momento posterior al momento de recepción.

De este modo, estos medios son llevados a funcionar en paralelo, en particular, si la entidad electrónica posee varios procesadores o en cuasi-paralelo, si la entidad electrónica posee un solo procesador, con el fin de estar adaptados, a la vez, a realizar la recepción del contenido digital difundido y para su retransmisión.

En la entidad electrónica portátil, que comprende medios de seguridad informática, la restitución del contenido digital difundido recibido se realiza de manera protegida, prohibiendo así las copias ilícitas.

Según una característica particular, la entidad electrónica comprende medios de memorización de dicho contenido digital recibido.

Según esta característica, el contenido digital recibido se memoriza, permitiendo así una relectura posterior para una retransmisión del contenido en diferido.

Los medios de memorización pueden ser de la memoria volátil (RAM) o de la memoria no volátil, por ejemplo, de la memoria instantánea Flash.

Según características particulares, los medios protegidos de retransmisión diferida comprenden medios de autenticación de un usuario.

Gracias a estas disposiciones, el acceso al contenido a retransmitir sólo se puede realizar por un usuario legítimo.

Según características particulares, los medios protegidos de retransmisión diferida comprenden medios para limitar la velocidad de emisión de dicho contenido por los medios de emisión o el número de retransmisiones o la frecuencia de retransmisión.

Gracias a estas disposiciones, la reproducción por emisión rápida del contenido con miras a su grabación, en al menos un soporte de información, se hace lenta y por lo tanto, poco eficaz. En una forma de realización preferida, la velocidad de emisión está limitada a la velocidad de recepción de dicho contenido.

Según características particulares, los medios protegidos de retransmisión diferida comprenden medios de cifrado adaptados para cifrar el contenido digital recibido y medios para descifrar del contenido digital cifrado.

Según características particulares, la entidad electrónica, tal como se expuso sucintamente con anterioridad comprende, además, medios de memorización de informaciones de cifrado y/o de descifrado.

Según características particulares, dicha entidad electrónica portátil extraíble, con seguridad informática, comprende medios de memorización de al menos una parte de una aplicación de retransmisión diferida en una zona de memoria de la entidad electrónica portátil protegida.

Gracias a estas disposiciones, se prohíbe una modificación de la ejecución de esta aplicación, lo que mejora la protección del contenido retransmitido. Se protege, asimismo, contra las copias ilícitas de la aplicación.

Según una característica particular, el acceso a dicha memoria de la entidad electrónica portátil está protegido por medios de seguridad informática.

Según características particulares, dicha aplicación comprende medios para formar una interfaz hombre-máquina adecuada para controlar dicha aplicación.

Según una característica particular, la interfaz hombre-máquina se gestiona por medios que pertenecen a una estación central.

Según características particulares, dicha entidad electrónica portátil protegida extraíble comprende medios para ejecutar dicha aplicación, siendo dichos medios de protección capaces de asegurar la ejecución de dicha aplicación.

Se protege, así, la propia aplicación y los medios de ejecutarla, lo que aumenta la seguridad contra las modificaciones de la ejecución de esta aplicación y las copias ilícitas de la aplicación.

Según características particulares, la aplicación de retransmisión diferida pone en práctica una zona de memorización reservada a dicho contenido, de magnitud predeterminada.

Según características particulares, la aplicación de retransmisión diferida comprende medios para configurar la magnitud de dicha zona de memorización de dicho contenido.

Según características particulares, la aplicación de retransmisión diferida está adaptada, cuando dicha memoria de almacenamiento de dicho contenido de magnitud predeterminada está llena, para controlar la retransmisión del contenido a partir del inicio operativo de la memoria intermedia.

Gracias a estas disposiciones, cuando la magnitud de la zona de memorización está limitada, el contenido se difunde en el orden de su registro. El usuario tiene entonces la certeza de poder ver el contenido cuando este último ya no puede registrarse.

Según características particulares, la aplicación de retransmisión diferida pone en práctica un puntero de lectura y un puntero de escritura en una memoria cíclica adaptada para conservar el contenido digital recibido.

Según características particulares, dicha aplicación está adaptada para ejecutarse en cooperación con una estación central conectada a dicha entidad electrónica portátil protegida extraíble después de la carga de al menos una parte de la aplicación en la memoria de esta estación central.

Según características particulares, la aplicación de retransmisión diferida es de iniciación automática, después de la conexión de la entidad electrónica al terminal central.

Según características particulares, los medios de protección están adaptados para proporcionar seguridad al menos en parte a la ejecución de dicha aplicación de retransmisión diferida así cargada y ejecutada en el terminal central, según un modo de protección predeterminado.

Según características particulares, los medios de protección están adaptados para formar, en cada carga, al menos una parte de dicha aplicación de retransmisión diferida.

Según características particulares, la formación de dicha parte utiliza un valor imprevisible.

Según características particulares, los medios de protección de la aplicación de retransmisión diferida son, además, adecuados para proteger cualquier modificación aportada a dicha aplicación de retransmisión diferida.

Según características particulares, dicha aplicación de retransmisión diferida pone en práctica al menos una clave criptográfica temporal.

Según características particulares, la aplicación de retransmisión diferida comprende al menos un programa principal ejecutado por un terminal central y al menos un programa auxiliar memorizado y ejecutado en dicha entidad electrónica conectada al terminal central, generando dicho programa principal órdenes de ejecución de la totalidad o parte de dicho programa auxiliar.

Según características particulares, el programa auxiliar se segmenta en una pluralidad de tramos, estando asociado a cada tramo un código de autenticación.

Según características particulares, la entidad electrónica, tal como fue sucintamente expuesta con anterioridad, comprende medios de verificación de los códigos de autenticación de los tramos y medios de bloqueo de dicha entidad en caso de verificación negativa.

Según características particulares, la aplicación de retransmisión diferida está adaptada para decodificar el contenido digital recibido.

Según características particulares, la entidad electrónica, tal como fue sucintamente expuesta con anterioridad, comprende medios de conversión del contenido digital recibido, incluyendo dichos medios de conversión una interfaz de recepción adaptada para conectarse a una antena de recepción.

Según características particulares, la entidad electrónica tal como fue sucintamente descrita con anterioridad, comprende medios de conversión del contenido digital recibido, incluyendo dichos medios de conversión una interfaz de recepción adaptada para conectarse a una red cableada.

Según una característica particular, la entidad electrónica comprende, sobre su superficie exterior, medios de control adecuados para controlar la lectura, el avance rápido, el retroceso rápido y el registro de un contenido digital difundido recibido.

Al ser las ventajas, objetos y características particulares de este dispositivo y de este sistema similares a las de la entidad electrónica portátil protegida extraíble, tales como los sucintamente expuestos con anterioridad, por ello, no se mencionan aquí de nuevo.

Otras ventajas, objetos y características de la presente invención serán más evidentes a partir de la descripción dada a continuación, hecha con un objetivo explicativo y no limitativo, haciendo referencia a los dibujos adjuntos, en donde:

- la Figura 1 representa, de forma esquemática, un primer modo de realización de la entidad y del lector objetos de la presente invención;

- la Figura 2 representa, de forma esquemática, un segundo modo de realización de la entidad y del lector objetos de la presente invención;

- la Figura 3 representa, de forma esquemática, un tercer modo de realización de la entidad y del lector objetos de la presente invención;

- la Figura 4 representa, de forma esquemática, un cuarto modo de realización de la entidad y del lector objetos de la presente invención;

- la Figura 5 representa, de forma esquemática, un quinto modo de realización de la entidad y del lector objetos de la presente invención y

- la Figura 6 representa, bajo la forma de un logigrama, etapas puestas en práctica en un modo de realización particular del método objeto de la presente invención.

A través de toda la descripción, se utilizan indiferentemente los términos de “contenido digital difundido”, “flujo de datos difundido” o “flujo multimedia difundido”. Estos contenidos o flujos difundidos constituyen los datos difundidos procesados por la entidad electrónica portátil protegida extraíble, objeto de la presente invención.

En toda la descripción, preferentemente, las zonas de memorias puestas en práctica son de magnitud configurable.

Se observa, en la Figura 1, una entidad electrónica portátil protegida extraíble 100 y un dispositivo electrónico de lectura 150 de la entidad 100. La entidad 100 comprende un controlador de seguridad informática 110, un puerto de entrada de señales de reloj 115, un puerto de entrada/salida 120 y una memoria 125. La entidad 100 es, por ejemplo, una tarjeta de tipo MMC especialmente dedicada a la puesta en práctica de la presente invención.

El dispositivo electrónico de lectura 150, también denominado lector o estación central, comprende un soporte 155 de la entidad 100, un puerto de salida de reloj 160, un puerto de entrada/salida 165, una memoria de programa 170, un controlador 175, un medio de recepción de contenido digital 180 y un medio de emisión de contenido digital 185 también denominado medio de retransmisión.

Un medio de recepción comprende, en particular, una antena y un convertidor analógico. Un medio de emisión está, en particular, conectado a una pantalla y a un altavoz, de modo que se restituya al usuario el contenido digital recibido.

En el modo de realización de la presente invención ilustrado en la Figura 1, los medios protegidos de retransmisión diferida adecuados para proteger la retransmisión comprenden el controlador de seguridad informática 110 y la memoria 125. El controlador de seguridad informática 110 puede ser, en ocasiones, relativamente rudimentario. Por ejemplo, puede tratarse, en el caso de una tarjeta de memoria instantánea flash protegida, de un microcontrolador de memoria flash que tiene la particularidad de verificar una contraseña para autorizar el acceso a la memoria instantánea o a una parte de esta memoria.

Sin embargo, el controlador de seguridad informática 110 es preferentemente más complejo. En este caso, los medios protegidos de retransmisión diferida pueden comprender medios criptográficos y/o medios de seguridad del controlador 110, siendo la seguridad efectuada, por ejemplo, mediante contramedidas contra los ataques por fallo o por medida de corriente.

El controlador de seguridad informática 110 está preferentemente certificado según los criterios EAL (acrónimo de Nivel de Seguridad de Evaluación) o FIPS (acrónimo de Federal Information Processing Standard).

Según un modo de realización particular, el controlador de seguridad informática 110 está asociado a, o incluye medios de limitación de, la velocidad de emisión del contenido digital. La velocidad de emisión puede determinarse, en particular, con respecto al volumen de los datos digitales a transmitir, al tiempo de restitución de estos datos o a alguna otra magnitud. Tales medios de limitación utilizan medios de medida del tiempo interno a la entidad electrónica 100, en particular un reloj o son del tipo condensador, tal como se describe en el documento FR 2837959, por ejemplo.

Por intermedio de estos medios internos de medida, los medios de limitación están adaptados para decidir prohibir la emisión de una parte del contenido de la memoria 125, en particular cuando, después de la recepción de una parte de una orden de control, la emisión del contenido de la memoria tuviera que efectuarse a una velocidad superior a la velocidad máxima de emisión autorizada.

El controlador de seguridad informática 110 está adaptado para efectuar una autenticación de la estación central 150 antes de autorizar la retransmisión diferida del contenido digital recibido. Por ejemplo, el controlador de seguridad informática 110 está adaptado para verificar el código de autenticación proporcionado por la estación central, según técnicas conocidas en sí mismas.

El controlador de seguridad informática 110 está adaptado para memorizar en la memoria 125 un contenido digital cifrado. En variantes de esta realización, el contenido digital difundido está cifrado y se memoriza sin descifrado. En otras variantes, el contenido digital, ocasionalmente ya cifrado, se descifra por el controlador de seguridad informática 110 antes de memorizarse en la memoria 125 y, en el momento de la retransmisión diferida del contenido digital, el controlador de seguridad informática 110 cifra el contenido digital memorizado, por ejemplo, por medio de una clave temporal común con la estación central.

El controlador 175 y la memoria de programa 170 están adaptados para poner en práctica un programa de retransmisión diferida conjuntamente con la ejecución de un programa por el controlador de seguridad informática 110.

Conviene señalar que, según la invención, la recepción del contenido digital difundido y la retransmisión se efectúan en paralelo o en cuasi-paralelo. De este modo, en el momento de la retransmisión del contenido digital ya recibido, es posible proseguir la recepción del contenido en curso de difusión.

Se observa, en la Figura 2, la presencia de elementos constitutivos de una entidad electrónica extraíble 200, que forman aquí un *dongle* (seguro informático) decodificador o una llave electrónica USB. En el modo de realización ilustrado en la Figura 2, el contenido digital difundido o flujo multimedia difundido que se recibe, se memoriza en una memoria 275 de un terminal central 260 y se retransmite poniendo en práctica medios distribuidos entre la entidad 200 y el terminal central 260. La entidad electrónica 200 comprende una interfaz 255 que permite conectarse al puerto 265 del terminal central 260.

Según un modo de realización, la interfaz 255 y el puerto 265 están conformes a la norma USB. En una variante de este modo de realización, las interfaces 255 y 265 son del tipo PCMCIA o MMC o conforme a la norma ISO 7816.

El terminal central 260 es susceptible de recibir, leer y/o procesar datos. A este respecto, comprende, en particular, una unidad central de procesamiento CPU 270 y una memoria viva 275, preferentemente no volátil, por ejemplo, un disco duro, que incluye la zona de memoria intermedia 280 y una zona de memoria de aplicación de software.

El registro del contenido digital difundido en la memoria intermedia 280 puede ser permanente, iniciado por un evento tal como un cambio de temática o de control que ponga en práctica la interfaz hombre-máquina gestionada por la aplicación de información 285 telecargada desde la entidad 200 en una memoria volátil a partir de la aplicación 245. El contenido digital, que se va a registrar, es cifrado por la entidad 200 y descifrado por el terminal central 260 poniendo en práctica una aplicación informática 285 telecargada desde la entidad 200 en una memoria volátil.

Esta aplicación 285 permite, además, la retransmisión diferida del contenido digital almacenado en la memoria 280.

La entidad electrónica, en este caso una llave USB 200, presenta una forma general constituida por circuitos montados normalmente en un circuito impreso. Otras variantes de arquitectura son evidentes para un experto en esta materia.

La llave USB 200, aunque de magnitud reducida (al tratarse, en efecto, de una entidad electrónica de bolsillo o portátil al alcance de la mano según la terminología inglesa “hand-held” permite, en efecto, reagrupar los circuitos descritos más adelante. Una tal llave USB 200 posee, por otro lado, un conector (que participa en la interfaz anteriormente citada) formado en la prolongación de su propio cuerpo, es decir, principalmente de una cubierta que recubre el conjunto de los circuitos electrónicos y que delimita el volumen exterior de la llave USB 200.

Un órgano que forma un concentrador 235, denominado también “hub”, en la terminología anglosajona, permite conectar, de forma conocida, varios periféricos conformes a la norma USB al puerto USB 255.

La entidad 200 comprende un lector de tarjeta de circuito integrado 225 adaptado para comunicarse según el protocolo USB y conectado al concentrador 235. Una forma de realización preferida, el lector de tarjeta de circuito integrado 225 es un periférico USB estándar, en donde los controladores están integrados al sistema operativo del terminal central 260, lo que confiere la ventaja de evitar la instalación previa de dichos controladores en el momento de la utilización de la llave USB 200. Por ejemplo, el lector de tarjetas de circuito integrado comprende un controlador de tipo USB CCID (Interfaz de Tarjeta de Circuito Integrado).

Una tarjeta de circuito integrado 220, que forma los medios protegidos de retransmisión diferida, está alojada en el lector de tarjetas de circuitos integrados 225; la tarjeta de circuito integrado 220 (a veces, denominada tarjeta de microcircuito) está adaptada, en particular, para autorizar (es decir, en algún modo, a decidir y a controlar) la retransmisión de los datos y para asegurar esta retransmisión de los datos. La tarjeta de circuito integrado 220 es, por ejemplo, una tarjeta de formato ID-000 conforme a la norma ISO -7816. El lector 225 comprende un alojamiento que permite recibir la tarjeta 220. Una cubierta extraíble (no representada) permite, por ejemplo, insertar la tarjeta 220 en el alojamiento adecuado.

Como variante, la tarjeta de circuito integrado 220 es un circuito de tipo microcontrolador protegido adaptado para comunicarse según la norma USB, por ejemplo, un circuito directamente fijado y conectado al circuito de la entidad 200, sin la presencia de lector. Dicho microcontrolador protegido es, por sí mismo, capaz de decidir y de garantizar la retransmisión de los datos.

La entidad 200 comprende, además, una memoria 240. En la práctica, la memoria 240 comprende al menos una parte no volátil. Por ejemplo, la memoria 240 es una memoria de tipo flash de 128 Mb.

La memoria 240 está controlada por un controlador 230, que está conectado al concentrador 235.

Además, la entidad electrónica 200 comprende medios de recepción 205 de un flujo de datos difundido, medios 205 que permiten la conversión de una señal recibida en un flujo de datos multimedia protegido. Estos medios de recepción 205 comprenden una interfaz de recepción, en particular, un conector 210 adaptado para conectarse a una antena de RF o a una parábola de recepción de un flujo emitido por satélite o a una red por cable. La interfaz de recepción puede ser, además, un receptor de datos inalámbrico, por ejemplo, conforme a la norma WIFI o Bluetooth.

Como variante, la entidad electrónica 200 incluye una antena de recepción (en lugar de un conector a una tal antena).

Los medios de recepción 205 comprenden, además, medios de conversión, por ejemplo, un circuito de sintonización (a veces denominado “tuner”) y un circuito de demodulación, por ejemplo de demodulación QPSK 215.

Los medios de recepción 205, conectados al concentrador 235, están así adaptados para recibir un flujo de datos conforme, por ejemplo, al formato MPEG o al formato DVB. En esta etapa de procesamiento, los datos son siempre protegidos, por ejemplo, cifrados por medio de una clave criptográfica.

La memoria 240 memoriza una aplicación de retransmisión diferida 245 que comprende, en particular, medios de descifrado de los datos del flujo recibido, medios de decodificación del flujo difundido, en particular adecuados para extraer del flujo DVB los datos en el formato MPEG, medios de descompresión por ejemplo un decodificador MPEG y medios de gestión de una interfaz de hombre-máquina 250. Esta interfaz hombre-máquina 250 adopta, por ejemplo, la forma de una ventana rectangular en donde se visualiza, de una parte, el contenido digital y, de otra parte, teclas de control, por ejemplo, de lectura, pausa, avance rápido, retroceso rápido y grabación en una memoria intermedia 280 del flujo difundido recibido de la entidad electrónica 200, descrita más adelante.

En la práctica, el controlador 230 es capaz de emular el funcionamiento de un lector de CD-ROM que incluye un software de gestión de la aplicación de retransmisión diferida 245 de tipo de iniciación automática denominado también “autorun”. En otros términos, el software de gestión de la aplicación de retransmisión diferida es cargado y ejecutado automáticamente por el terminal central cuando la entidad 200 se conecta al terminal central 260.

Según un modo de realización, la aplicación de retransmisión diferida 245 se memoriza en la memoria 240 de forma protegida, por ejemplo, controlando el acceso a esta aplicación por medio de un código de identificación. La protección del acceso de la aplicación 245 se realiza por el controlador 230 en colaboración con la tarjeta de circuito integrado.

Como variante, el software de gestión de la aplicación de retransmisión diferida 245 se carga en una zona de memoria no volátil ROM del controlador 230.

Según un modo de realización, se carga una nueva versión de la aplicación de retransmisión diferida 245 o cualquier otro programa.

Esta actualización es, por ejemplo, gestionada por un programa guardado en la memoria 240. A este respecto, el programa se conecta, de forma protegida, a una entidad autorizada, por ejemplo, a un servidor de red, utilizando, por ejemplo, los medios de seguridad de la tarjeta de circuito integrado 220, en particular, mediante autenticación, cifrado o firma electrónica.

En efecto, el terminal central en donde está conectada la entidad, puede conectarse a una red de comunicación unidireccional o bidireccional, por ejemplo a la red Internet o a una red de telecomunicación móvil.

Esta comunicación protegida se realiza, en particular, por medio de una clave de sesión.

Además, una clave de sesión K_1 puede utilizarse en los modos de realización siguientes, con el fin de realizar la protección de la comunicación entre la entidad electrónica (llave USB 200) y el terminal central 260, es decir, en este caso, la aplicación de retransmisión diferida.

Según un modo de realización, el flujo de datos asegurado (es decir protegido, por ejemplo, cifrado) se recibe por la entidad 200 y se descifra por esta última (es decir, por medios de descifrado instalados en su interior) por ejemplo, en el interior de los medios de recepción 205, en particular en colaboración con la tarjeta de circuito integrado 220. El flujo descifrado es entonces comunicado a la aplicación de retransmisión diferida 245 instalada en el terminal central 260 después de haber sido cifrado por la clave de sesión K_1 en la entidad 200, por ejemplo por medios de cifrado en el interior de los medios de recepción 205, en particular en colaboración con la tarjeta de circuito integrado 220. El terminal central 260 procede, entonces, a un nuevo descifrado del flujo gracias a la clave de sesión K_1.

Según otro modo de realización, el flujo de datos protegido (o cifrado) se recibe por los medios de recepción 205 de la entidad 200. La información contenida en el flujo de datos es, a continuación, transmitida a la tarjeta de circuito integrado 220. Esta última determina, a partir de las informaciones contenidas en el flujo de datos (o recibidas por otro lado), una clave de cifrado temporal K_2. La tarjeta de circuito integrado (220) comunica, a continuación, la clave de cifrado temporal K_2 al medio de recepción 205 que cifra, entonces, la clave de cifrado temporal K_2 por la clave de sesión K_1 y transmite el flujo de datos recibido y la clave de cifrado temporal K_2 cifrada en la aplicación de retransmisión diferida 245 instalada en el terminal central 260. El terminal central 260, que detenta la clave de sesión K_1, tiene así acceso a la clave de cifrado temporal K_2 y puede proceder entonces al descifrado del flujo.

La clave de sesión está, en particular, determinada a partir de una clave interna y de un dato extraído del flujo de datos o de un dato comunicado según otro medio; está, por ejemplo, memorizada en la tarjeta de circuito integrado 220 y transmitida al terminal central 260 dentro de la aplicación de retransmisión diferida 245.

Se observa que, en una variante no representada, es precisamente el terminal central 260 el que comprende medios de recepción de los contenidos digital difundidos, similares a los medios 205, 210 y 215 y no la entidad 200.

En un modo de realización particular, la aplicación de retransmisión diferida 245 comprende dos partes: un programa principal ejecutado por el terminal central 260 y al menos un programa auxiliar almacenado en la memoria 240 y ejecutado por la entidad 200 cuando está conectada al terminal central 260.

Dentro de este contexto, el programa principal genera órdenes de ejecución de la totalidad o parte de dicho programa auxiliar, en particular, después de la verificación positiva de la autenticación del portador de la entidad.

En un modo de realización particular, la partición en dos partes, de la aplicación de retransmisión diferida 245 puede realizarse de forma aleatoria, con una primera parte, principal, ejecutada por el terminal central 260 y otra parte, auxiliar, ejecutada por la entidad 200. Por ejemplo la o las zonas de corte son aleatorias. Esta partición aleatoria puede realizarse en cada carga de la aplicación de retransmisión diferida 245 en el terminal central 260 interviniendo, por ejemplo, automáticamente a continuación de cada conexión de la entidad electrónica portátil 200 al terminal central 260.

Por ejemplo, la aplicación de retransmisión diferida 245 es susceptible de cortarse previamente en varios tramos en una zona de memorización de la memoria 240 o en una zona de memoria ROM del controlador 230. A cada tramo se asocia, además, instrucciones de comunicación que permiten la comunicación entre el terminal 260 y la entidad 200. Esta asociación se realiza, por ejemplo, en el paso de la partición en varias partes de la aplicación de retransmisión diferida 245. Se selecciona, a continuación, de forma aleatoria grupos de tramos contiguos y se ejecuta únicamente entre las instrucciones de comunicación asociadas a cada tramo, las instrucciones de comunicación que separan dos grupos de tramos así seleccionados. En la práctica, cada tramo de la aplicación de retransmisión diferida 245 puede tener una magnitud diferente. Cada tramo está constituido por códigos escritos en lenguaje máquina, ensamblador C o Java, etc.

En el modo de realización ilustrado en la Figura 3, la memorización del contenido digital a retransmitir de manera diferida se efectúa en una entidad electrónica portátil protegida extraíble 300 y este contenido memorizado se retransmite poniendo en práctica medios distribuidos entre la entidad 300 y un terminal central 360. Se observa, en la Figura 3, que la entidad 300 es similar a la entidad 200 y comprende todos los elementos de la entidad 200, a los cuales se añaden un controlador de memoria 390 y una memoria 395, preferentemente no volátil. El terminal central 360 es similar al terminal 260 y comprende todos los elementos del terminal 260 con la excepción de la zona de memoria 280.

El contenido digital difundido recibido por la entidad 200 es cifrado y memorizado en la memoria viva 395, por el controlador de memoria 390, cuando deba ser retransmitido de modo diferido. Se observa que, cuando la memoria 395 es no volátil, el contenido digital se puede retransmitir en otro terminal central similar al terminal central 260.

La memoria 395 está preferentemente gestionada de forma cíclica.

El controlador de memoria 390 efectúa la gestión de dos punteros, ocasionalmente bajo el control de la interfaz hombre-máquina 250. El puntero de escritura define la posición, en la memoria 395, en donde debe estar escrito el contenido digital difundido que se va a recibir. El puntero de lectura define la posición, en la memoria 395, en donde debe ser leído el contenido digital a retransmitir en diferido.

Como se expuso con respecto a la Figura 6, preferentemente, si la memoria 395 está llena, es decir, si el puntero de escritura reagrupa el puntero de lectura, el controlador de memoria 390 inicia inmediatamente la lectura del contenido digital, es decir, que el controlador 390 lee el contenido digital y lo transmite al terminal central 360 en donde se descifra por la aplicación 385 y se retransmite en una pantalla de visualización (no representada).

De este modo, se evita destruir un contenido digital previamente recibido y no retransmitido por un nuevo contenido digital difundido recibido. Además, se evita interrumpir la memorización del contenido digital difundido en curso de recepción. En este modo de realización, el controlador 390 está controlado por la aplicación 285.

El controlador 390 está adaptado para autorizar la retransmisión diferida después de la presentación de un código de autenticación transmitido a la entidad por el terminal central, siendo este modo, por ejemplo, memorizado en la memoria 280. La verificación de la autenticación se realiza, por ejemplo, por la tarjeta de circuito integrado 220.

El controlador 390 recibe los datos leídos en la memoria 395 y controla los punteros de lectura y de escritura.

Según un modo de realización particular, la memoria 395 es una parte de la memoria 240 de la entidad electrónica 200, pudiendo esta parte ser protegida. En este modo de realización, las funciones del controlador 390 se realizan, por ejemplo, por el controlador 230.

En el modo de realización ilustrado en la Figura 4, la memorización del contenido digital a retransmitir de manera diferida se efectúa en una entidad electrónica portátil protegida extraíble 400 y la retransmisión del contenido memorizado se efectúa poniendo en práctica medios que sólo se encuentran en esta entidad 400. Se observa, en la Figura 4, que la entidad 400 es similar a la entidad 200 y contiene todos los elementos de la entidad 200, a los cuales se añaden un controlador de memoria 490 y la memoria 395, preferentemente no volátil. El terminal central 460 es similar al terminal 260 y comprende todos los elementos del terminal 260 a excepción de las zonas de memoria 280 y 285 que son sustituidas por una zona de memoria 480.

El contenido digital recibido por la entidad 400 es descifrado, siendo la clave proporcionada por la tarjeta de circuito integrado 220 y memorizada en la memoria 395, por el controlador de memoria 490, cuando debe retransmitirse de manera diferida. Se observa que, cuando la memoria 395 es no volátil, el contenido digital puede retransmitirse en otro terminal central similar al terminal central 460.

La memoria 395 es preferentemente gestionada de forma cíclica.

El controlador de memoria 490 efectúa la gestión de dos punteros, ocasionalmente bajo el control de la interfaz hombre-máquina 250. El puntero de escritura define la posición, en la memoria 395, en donde debe escribirse el contenido digital difundido que se va a recibir. El puntero de lectura define la posición, en la memoria 395, en donde debe leer el contenido digital a retransmitir de manera diferida.

Según se expuso con respecto a la Figura 6, preferentemente, si la memoria 395 está llena, es decir, si el puntero de escritura reagrupa el puntero de lectura, el controlador de memoria 490 inicia inmediatamente la lectura del contenido digital, es decir, que el controlador 490 lee el contenido digital, lo descifra y lo transmite al terminal central 360, en donde es retransmitido en una pantalla de visualización (no representada).

De esta manera, se evita destruir un contenido digital previamente recibido y no retransmitido por un contenido digital difundido en curso de recepción. Además, se evita interrumpir la memorización del contenido digital difundido en curso de recepción.

En este modo de realización, la tarjeta de circuito integrado 220 regula el controlador de memoria 490 y en particular, el puntero de le lectura.

Según un modo de realización particular, la memoria 395 es una parte de la memoria 240 de la entidad electrónica 200, pudiendo esta parte estar protegida. En este modo de realización, las funciones del controlador 490 se realizan, por ejemplo, por el controlador 230.

Según una variante de realización, la entidad 400 comprende, sobre su superficie exterior, botones que permiten controlar la retransmisión diferida, en particular, las funciones de lectura, pausa, retroceso rápido, avance rápido y grabación.

Además, la aplicación de retransmisión se memoriza en la memoria 480 del terminal central 460.

Se observa, en la Figura 5, un modo de realización particular de la entidad electrónica portátil protegida extraíble objeto de la presente invención, que adopta la forma de una tarjeta denominada SIM o USIM (Módulo de Identificación del Abonado Universal) 500 que incluye, además, una interfaz MMC. Esta tarjeta presenta un contacto de alimentación común 505, un contacto de puesta a cero 510, un contacto de reloj SIM 515, un contacto de comunicación de datos MMC 520, un contacto de masa común 525, un contacto de reloj MMC 530, un contacto de entrada/salida de datos SIM 535, un contacto de control MMC 540, un controlador 545, una memoria adaptada para memorizar el contenido digital recibido 550, un microcontrolador 565 que comprende una memoria EE-PROM que conserva y que pone en práctica una aplicación protegida de retransmisión diferida 570, por ejemplo similar a la aplicación 245. Esta aplicación está, además, adaptada para realizar las funciones de cifrado, de descifrado y de gestión de interfaz hombre-máquina, funciones descritas en otra parte. Esta memoria almacena un menú que el teléfono puede poner en práctica por decisión del usuario.

El microcontrolador 565 está adaptado para controlar el acceso a la memoria 550 por intermedio del controlador 545. En un modo de funcionamiento de la entidad electrónica 500, en el momento de la recepción, por un teléfono (no representado) que presenta la entidad 500, de un contenido digital difundido a retransmitir de forma diferida, el contacto de control de datos MMC 520 recibe el contenido con el fin de memorizarlo en la memoria 550. A este respecto, el teléfono emite una orden, bajo la forma de una APDU (Unidad de Datos de Protocolos de Aplicación) por intermedio del contacto de entrada/salida de datos SIM 535 con el fin de controlar la escritura en memoria 550.

La retransmisión de los datos memorizados en diferido se controla por el teléfono o por la aplicación asegurada de retransmisión diferida 570. A este respecto, los datos memorizados son leídos por el controlador 545 (a la recepción de órdenes por el contacto de órdenes MMC 540) bajo el control del microcontrolador 565 con el fin, de una parte, de solamente restituir estos datos a los usuarios legítimos y, de otra parte, de descifrar los datos si fuera necesario.

Además, es posible limitar la velocidad de retransmisión así como el número o la frecuencia de retransmisión.

Se describe ahora, haciendo referencia a la Figura 6, un modo particular de puesta en práctica del sistema constituido por la entidad electrónica portátil protegida extraíble y por el terminal central.

La Figura 6 es un algoritmo que ilustra una aplicación de la invención a una combinación de un medio de visualización y de un teléfono.

En el momento de una llamada telefónica (etapa 605) entrante o saliente, mientras el usuario está en curso de audición o de visualización del contenido digital difundido recibido, el contenido digital difundido se memoriza con el fin de poderse retransmitir posteriormente. A este respecto en la etapa 610, se inicia el modo de retransmisión en diferido.

De este modo, en la etapa 615 el contenido digital difundido es recibido y memorizado.

El contenido recibido puede cifrarse, asimismo, en el momento de su memorización (etapa 620).

Si se detecta (etapa 625) el final de la llamada telefónica o el hecho de que la memoria está llena, entonces la retransmisión del contenido memorizado es activada.

De este modo, la retransmisión se efectúa (etapa 635) mientras que se prosigue la recepción, siendo memorizado el contenido difundido recibido con miras a su posterior retransmisión.

Estas operaciones se efectúan en paralelo, en particular si el dispositivo posee varios procesadores o en cuasi-paralelo si el dispositivo solamente posee un procesador único.

En el momento de la retransmisión, el contenido memorizado puede ser descifrado si este último fue previamente cifrado, en particular, en el momento de la etapa 620.

Además, en el momento de la retransmisión, se controla que la retransmisión pueda tener lugar de forma que se prohíba una reproducción del contenido digital recibido.

REIVINDICACIONES

1. Entidad electrónica portátil extraíble asegurada, que comprende:

- medios de recepción de un contenido digital difundido;
- medios de emisión de dicho contenido digital difundido recibido y
- medios de retransmisión diferida del contenido digital recibido adaptados para producir la emisión, por los medios emisores, y de forma diferida en el tiempo, del contenido digital recibido caracterizada porque:
- dichos medios de retransmisión diferida del contenido digital recibido están protegidos de modo que se prohíba una reproducción del contenido digital, antes de la emisión de dicho contenido digital recibido,
- estando dichos medios adecuados para funcionar en paralelo o en cuasi-paralelo.

2. La entidad electrónica según la reivindicación 1, caracterizada porque la entidad electrónica contiene medios de memorización de dicho contenido digital recibido.

3. La entidad electrónica según una cualquiera de las reivindicaciones precedentes, caracterizada porque los medios protegidos de retransmisión diferida comprenden medios de autenticación de un usuario.

4. La entidad electrónica según una cualquiera de las reivindicaciones precedentes, caracterizada porque los medios protegidos de retransmisión diferida comprenden medios para limitar la velocidad de transmisión de dicho contenido por los medios de emisión o el número de retransmisiones o la frecuencia de retransmisión.

5. La entidad electrónica según una cualquiera de las reivindicaciones precedentes, caracterizada porque los medios protegidos de retransmisión diferida comprenden medios de cifrado adaptados para cifrar el contenido digital recibido y medios de descifrado del contenido digital cifrado y porque comprende, además, medios de memorización de informaciones de cifrado y/o de descifrado.

6. La entidad electrónica según una cualquiera de las reivindicaciones precedentes, caracterizada porque comprende medios de memorización de al menos una parte de una aplicación de retransmisión diferida (245) en una zona de memoria de la entidad electrónica portátil protegida.

7. La entidad electrónica según la reivindicación 6, caracterizada porque el acceso a dicha memoria de la entidad electrónica portátil está protegido por medios de seguridad informática.

8. La entidad electrónica según la reivindicación 6 o 7, caracterizada porque dicha aplicación comprende medios para formar una interfaz hombre-máquina adecuada para controlar dicha aplicación y porque la interfaz hombre-máquina está gestionada por medios que pertenecen a una estación central.

9. La entidad electrónica según una cualquiera de las reivindicaciones 6 a 8, caracterizada porque la aplicación de retransmisión diferida pone en práctica una zona de memorización reservada a dicho contenido, de magnitud predeterminada.

10. La entidad electrónica según la reivindicación 9, caracterizada porque la aplicación de retransmisión diferida comprende medios para configurar la magnitud de dicha zona de memorización de dicho contenido.

11. La entidad electrónica según una cualquiera de las reivindicaciones 9 o 10, caracterizada porque la aplicación de retransmisión diferida está adaptada, cuando dicha memoria de almacenamiento de dicho contenido de magnitud predeterminada está llena, para controlar la retransmisión del contenido a partir de la iniciación operativa de la memoria intermedia.

12. La entidad electrónica según una cualquiera de las reivindicaciones 6 a 11, caracterizada porque la aplicación de retransmisión diferida pone en práctica un puntero de lectura y un puntero de escritura en una memoria cíclica adaptada para conservar el contenido digital recibido.

13. La entidad electrónica según una cualquiera de las reivindicaciones 6 o 12, caracterizada porque dicha aplicación está adaptada para ejecutarse en cooperación con una estación central conectada a dicha entidad electrónica portátil extraíble protegida, después de la carga de al menos una parte de la aplicación en la memoria de esta estación central y porque la aplicación de retransmisión diferida (245) es de iniciación automática, después de la conexión de la entidad electrónica (200) al terminal central (260).

14. La entidad electrónica según una cualquiera de las reivindicaciones 6 a 13, caracterizada porque la aplicación de retransmisión diferida (245) es adecuada para decodificar el contenido digital recibido.

15. La entidad electrónica según una cualquiera de las reivindicaciones precedentes, caracterizada porque comprende medios de conversión del contenido digital recibido, comprendiendo dichos medios de conversión una interfaz de recepción adecuada para conectarse a una antena de recepción.

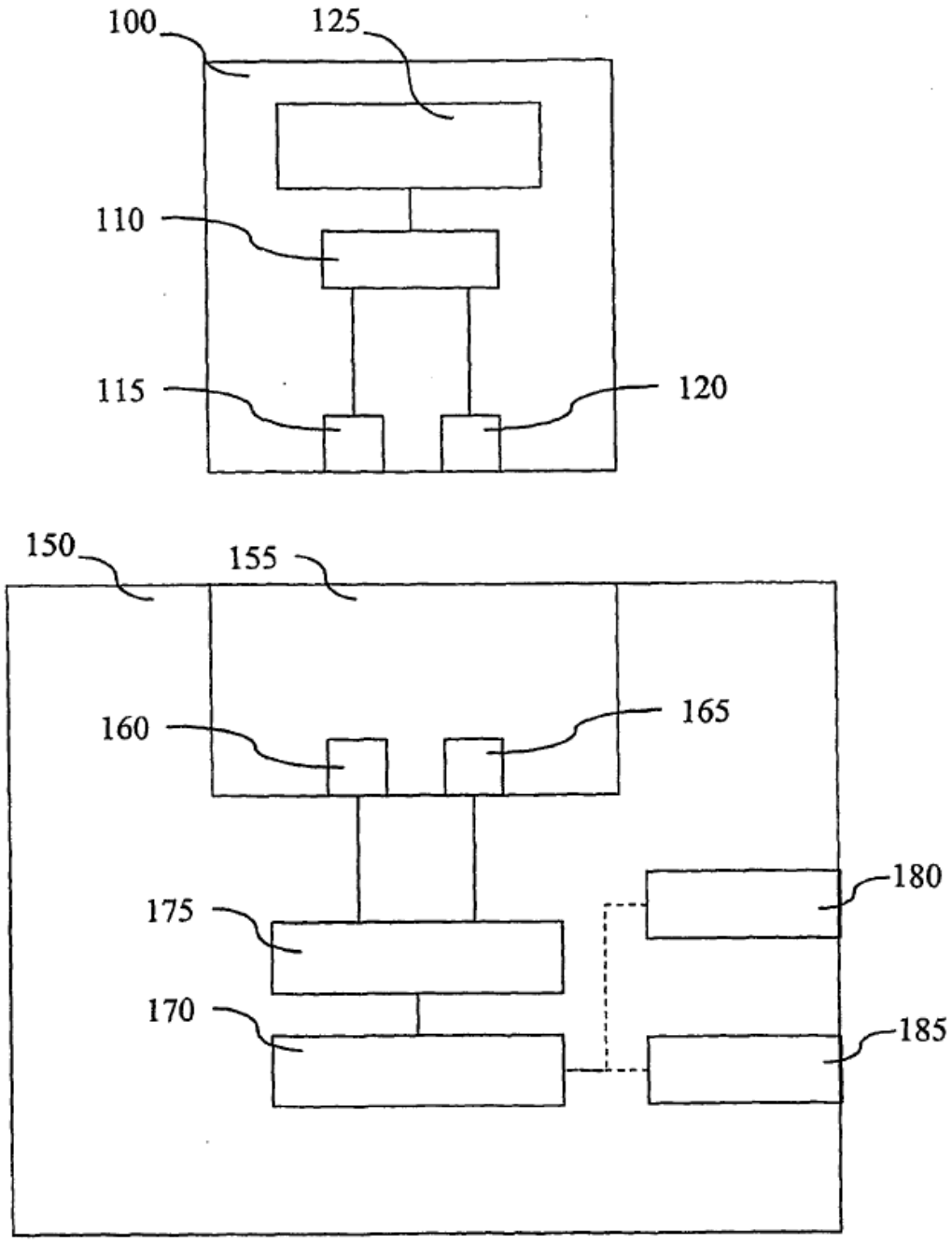

Figura 1

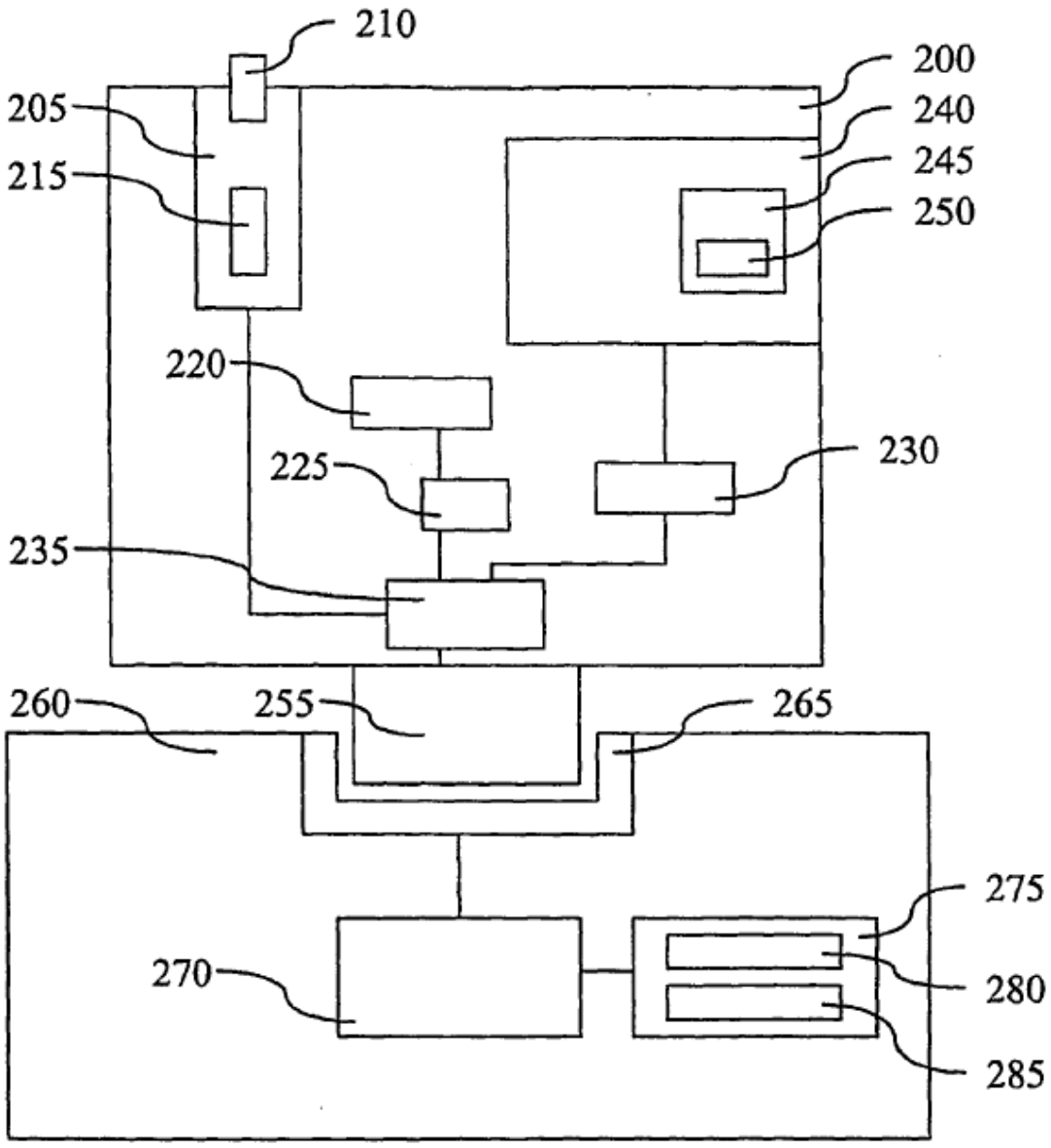
210
200
205
240
215
245
250
220
225
230
235
260
255
265
275
270
280
285

Figura 2

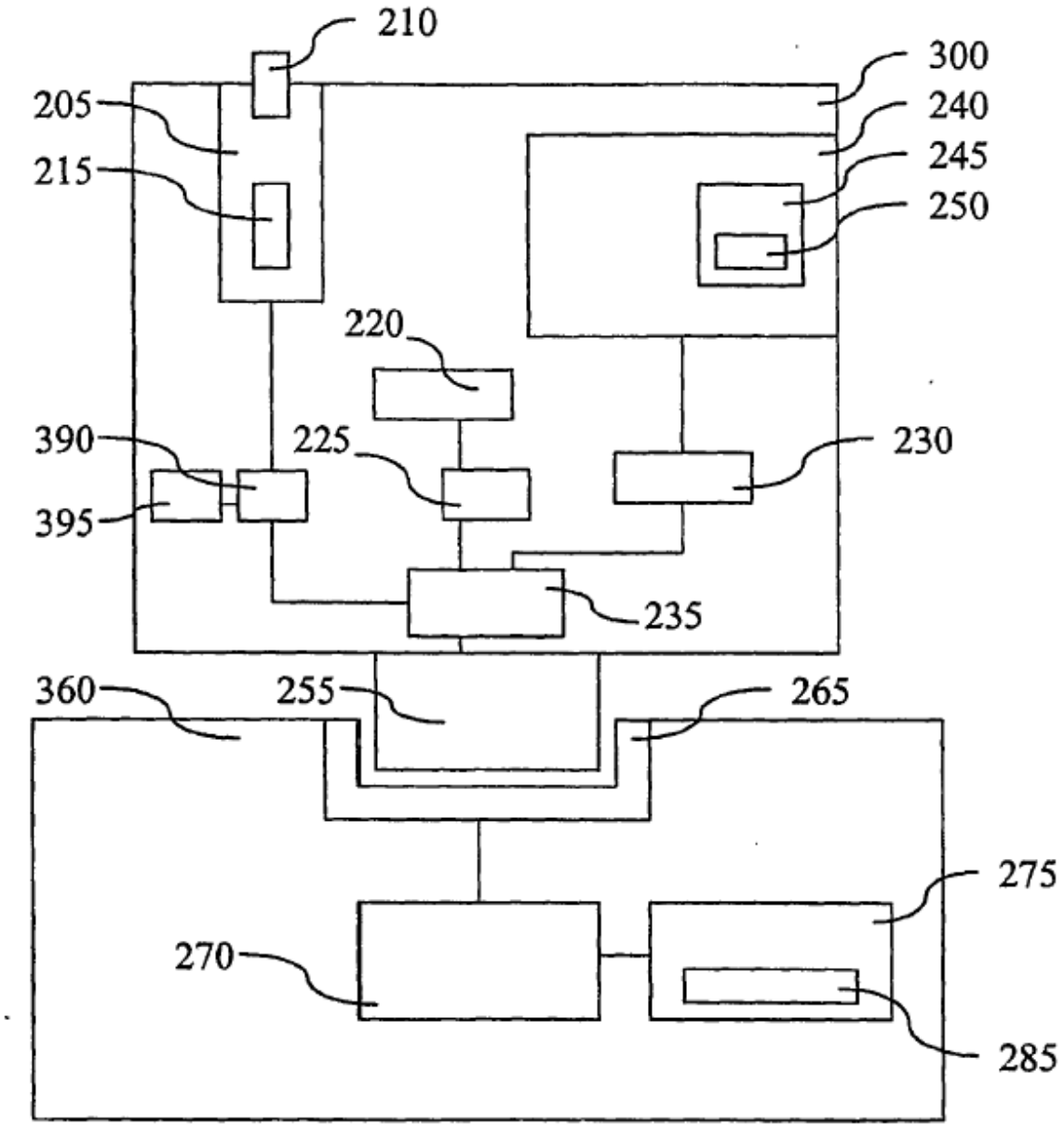
210
300
205
240
215
245
250
220
390
225
230
395
235
360
255
265
275
270
285

Figura 3

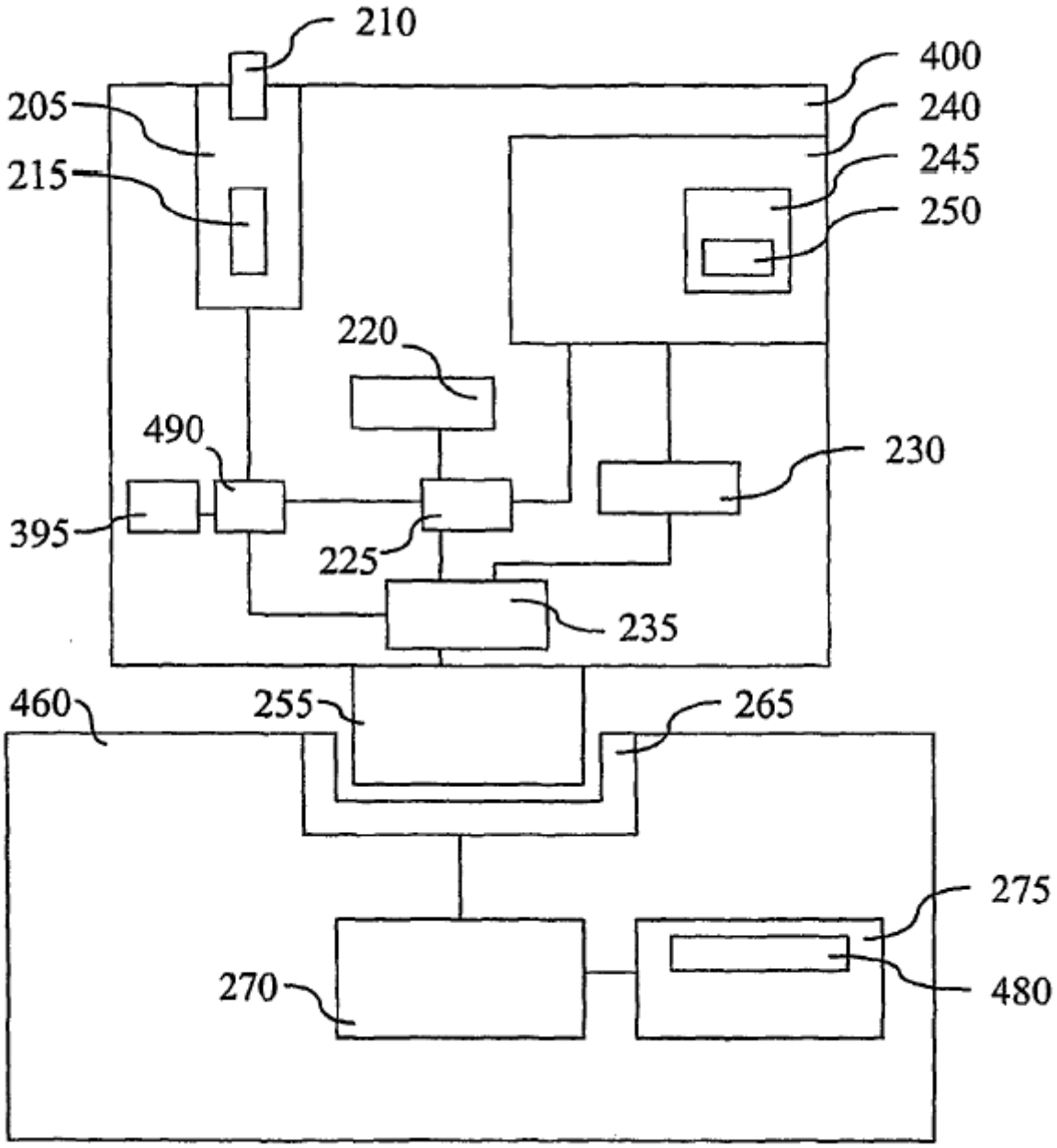
210
400
205
240
215
245
250
220
490
230
395
225
235
460
255
265
275
270
480

Figura 4

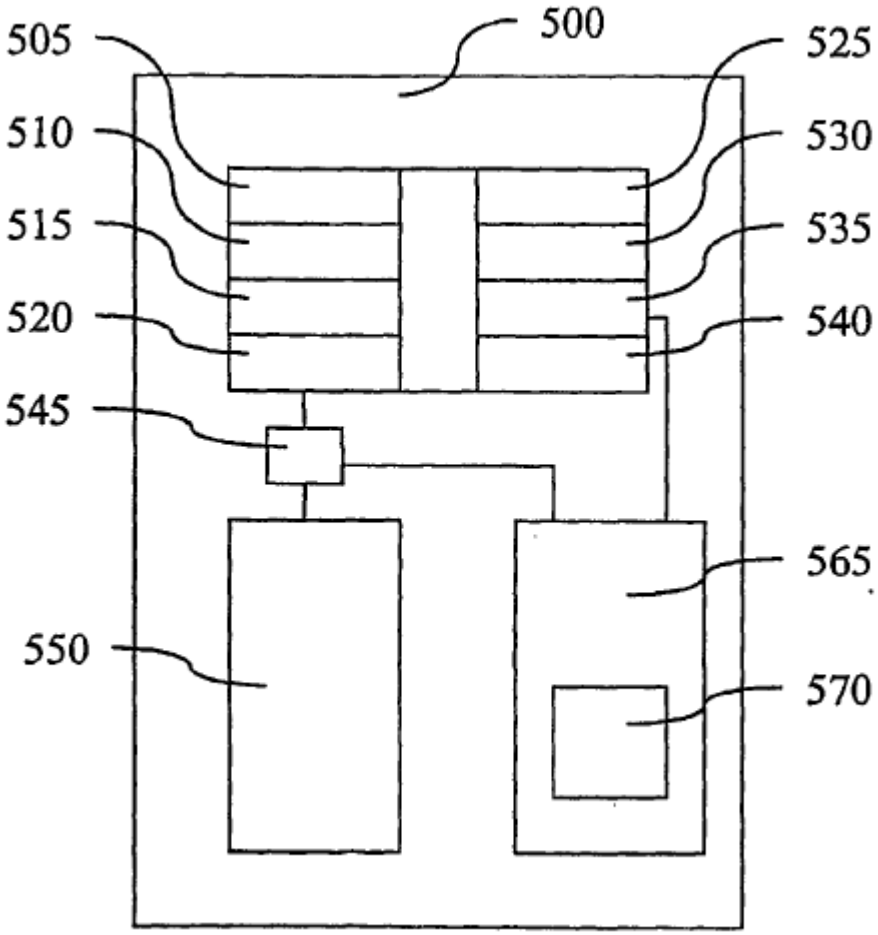

Figura 5

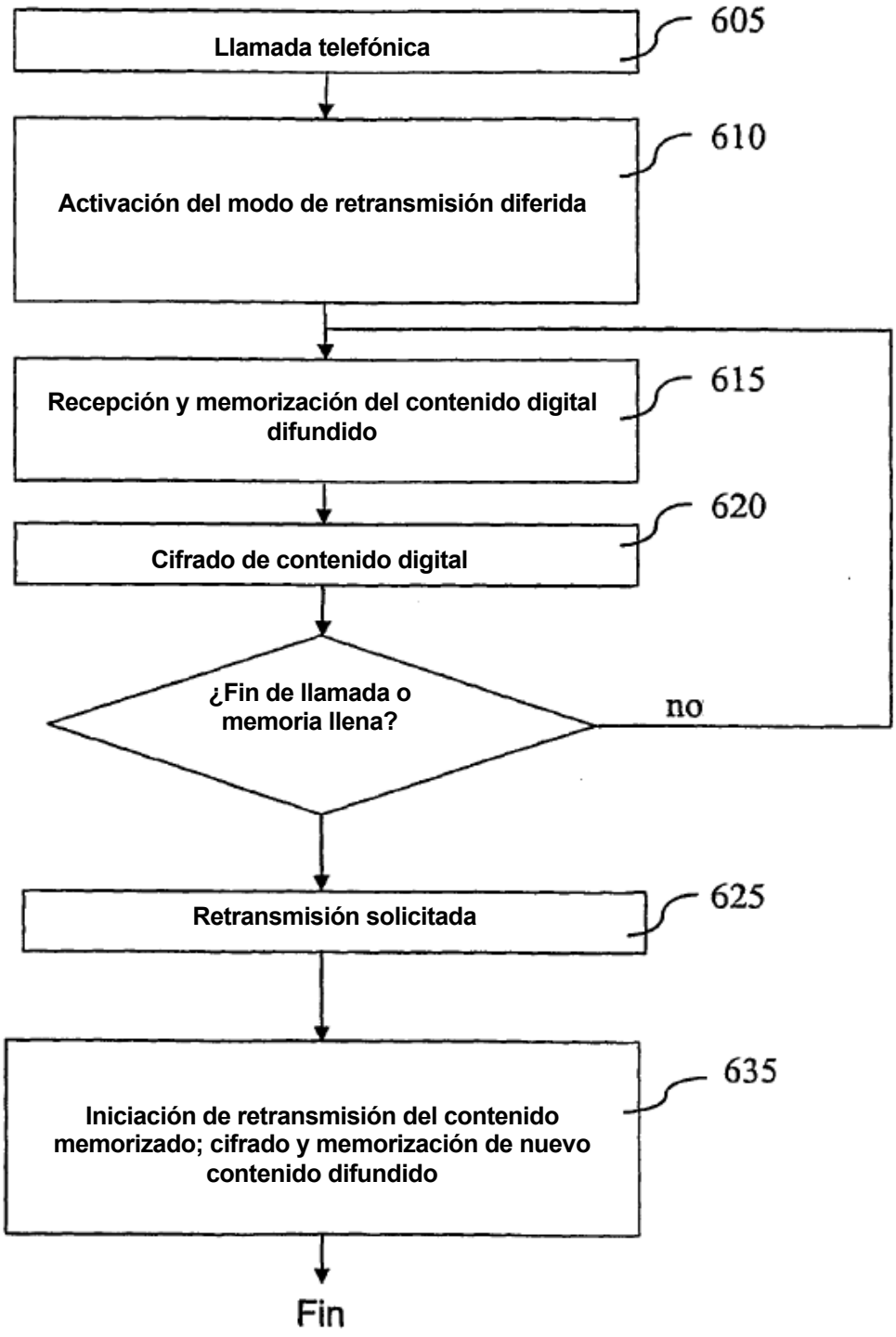
Llamada telefónica
605
Activación del modo de retransmisión diferida
610
Recepción y memorización del contenido digital difundido
615
Cifrado de contenido digital
620
¿Fin de llamada o memoria llena?
no
Retransmisión solicitada
625
Iniciación de retransmisión del contenido memorizado; cifrado y memorización de nuevo contenido difundido
635
Fin

Figura 6