(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 514 467**

(51) Int. CI.:

H04N 21/418 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.02.2005 E 05728113 (1)**

(97) Fecha y número de publicación de la concesión europea: **23.07.2014 EP 1716706**

(54) Título: **Procedimiento de emparejamiento de un terminal receptor con una pluralidad de tarjetas de control de acceso**

(30) Prioridad:

20.02.2004 FR 0450323

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.10.2014

(73) Titular/es:

VIACCESS (100.0%)
LES COLLINES DE L'ARCHE, TOUR OPÉRA C
92057 PARIS LA DÉFENSE, FR

(72) Inventor/es:

BEUN, FRÉDÉRIC;
BOUDIER, LAURENCE;
ROQUE, PIERRE y
TRONEL, BRUNO

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Procedimiento de emparejamiento de un terminal receptor con una pluralidad de tarjetas de control de acceso

Campo técnico

La invención se sitúa en el dominio de la aseguramiento de datos digitales difundidos y de equipos receptores destinados a recibir esos datos en una red de distribución de datos y/o servicios, y se refiere más específicamente a un procedimiento de emparejamiento de un equipo receptor de datos digitales con una pluralidad de módulos externos de seguridad que tienen, cada uno de ellos, un identificador único.

Estado de la técnica anterior

De vez en cuando, los operadores ofrecen datos y servicios en línea accesibles por medio de terminales dotados de procesadores de seguridad. En general, los datos y servicios distribuidos son codificados con la emisión de claves secretas y descodificados en la recepción mediante las mismas claves secretas previamente puestas a disposición del abonado.

Además de las técnicas convencionales de control de acceso en base a codificación durante la emisión y descodificación durante la recepción de los datos distribuidos, los operadores proponen técnicas basadas en el emparejamiento del terminal de recepción con un procesador de seguridad para evitar que los datos y servicios distribuidos sean accesibles a usuarios dotados de un terminal robado o de un procesador de seguridad pirateado tal como, por ejemplo, una tarjeta inteligente falsificada.

El documento WO 99/57901 describe un mecanismo de emparejamiento entre un receptor y un módulo de seguridad basado, por una parte, en el cifrado y el descifrado de las informaciones intercambiadas entre el receptor y el módulo de seguridad mediante una clave única almacenada en el receptor o en el módulo de seguridad, y por otra parte, en la presencia de un número de receptor en el módulo de seguridad.

Un inconveniente de esta técnica resulta del hecho de que la asociación entre un receptor y un módulo de seguridad que está emparejado con el mismo se establece a priori, y no permite al operador gestionar eficazmente su parque de equipos receptores a efectos de impedir el desvío de este equipo para las utilizaciones fraudulentas.

Un objeto del procedimiento de emparejamiento según la invención es el de permitir que cada operador limite las utilizaciones de su parque de material de recepción configurando y controlando dinámicamente el emparejamiento del equipo receptor y los módulos externos destinados a cooperar con ese equipo.

Exposición de la invención

La invención preconiza un procedimiento de emparejamiento de un equipo receptor de datos digitales con una pluralidad de módulos externos de seguridad que tienen, cada uno de ellos, un identificador único.

El procedimiento según la invención incluye las siguientes etapas:

- conectar un módulo externo de seguridad al equipo receptor,

- memorizar sobre la marcha en el equipo receptor el identificador único del módulo de seguridad conectado.

Este procedimiento incluye una fase de control que consiste en verificar, en cada conexión posterior de un módulo externo de seguridad al equipo receptor, si el identificador del citado módulo está memorizado en ese equipo receptor.

A este efecto, el procedimiento según la invención incluye además una etapa consistente en transmitir al equipo receptor una señalización que incluye al menos un mensaje de gestión de la memorización del identificador del módulo externo de seguridad y/o un mensaje de gestión de la fase de control.

La citada señalización incluye al menos una de las consignas siguientes:

- autorizar la memorización,

- prohibir la memorización,

- eliminar los identificadores ya memorizados en el equipo receptor,

- activar o desactivar la fase de control.

En una primera variante de realización del procedimiento, la citada señalización incluye una consigna de reconfiguración mediante la que se transmite al equipo receptor una lista actualizada de los identificadores de los módulos externos de seguridad emparejados con el citado equipo receptor.

La citada lista es transmitida al equipo receptor ya sea directamente, o ya sea a través de un módulo externo de seguridad conectado a dicho equipo receptor.

Con preferencia, la citada fase de control incluye un procedimiento consistente en interrumpir el tratamiento de datos si el identificador del módulo externo de seguridad conectado no ha sido previamente memorizado en el equipo receptor.

El procedimiento según la invención se aplica mientras los datos son distribuidos en abierto, e igualmente cuando esos datos son distribuidos de forma codificada mediante una palabra de control cifrada. En este último caso, cada módulo externo de seguridad incluye derechos de acceso a los citados datos y un algoritmo de descodificación de dicha palabra de control para descodificar los datos.

La señalización de control se transmite en un mensaje EMM (Entitlement Management Message, en inglés) específico de un módulo externo de seguridad asociado a ese equipo receptor o en un mensaje EMM específico de ese equipo receptor, y para un equipo receptor dado, la lista actualizada de identificadores de módulos externos de seguridad emparejados con ese equipo receptor es transmitida asimismo en un mensaje EMM específico de un módulo de seguridad asociado a ese equipo receptor.

Alternativamente, la citada señalización es transmitida en un flujo privado a un grupo de equipos receptores, y la lista actualizada de identificadores de los módulos externos es transmitida asimismo en un flujo privado a cada uno de los equipos receptores. En este último caso, el citado flujo privado es tratado mediante una lógica dedicada ejecutable en cada equipo receptor en función del identificador del módulo externo de seguridad que se le ha asociado.

Según otra variante, la señalización es transmitida a un grupo de equipos receptores en un mensaje EMM específico de un grupo de módulos externos de seguridad asociados a los citados equipos receptores o en un mensaje EMM específico de dicho grupo de equipos receptores, y para un grupo de equipos receptores dado la lista actualizada de identificadores de los módulos externos es transmitida en un mensaje EMM específico de un grupo de módulos externos de seguridad asociados a los citados equipos receptores.

Por otra parte, para un grupo de equipos receptores dado, la señalización de control y la lista actualizada pueden ser transmitidas igualmente a un grupo de equipos en un flujo privado.

En ese caso, el citado flujo privado es tratado por una lógica dedicada ejecutable en cada equipo receptor en función del identificador del módulo externo de seguridad que se le haya asociado.

Durante la transmisión de la señalización y de las listas actualizadas efectuada por medio de los EMM, el procedimiento incluye un mecanismo destinado a impedir la utilización de un EMM transmitido a un mismo módulo de seguridad en dos equipos receptores distintos.

Los EMM específicos de un módulo de seguridad o de un equipo receptor presentan el formato siguiente:

```
EMM-U_section() {
table_id = 0x88                 8 bits
section_syntax_indicator = 0    1 bit
DVB_reserved                    1 bit
ISO_reserved                    2 bits
EMM-U_section_length            12 bits
unique_address_field            40 bits
para (i=0; i<N; i++) {
        EMM_data_byte           8 bits
        }
}
```

Los EMM específicos en todos los módulos externos de seguridad o en todos los equipos receptores, presentan la forma siguiente:

```
EMM-G_section() {
table_id = 0x8A o 0x8B          8 bits
section_syntax_indicator = 0    1 bit
DVB_reserved                    1 bit
ISO_reserved                    2 bits
EMM-G_section_length            12 bits
```

```
para (i=0; i<N; i++) {
        EMM_data_byte              8 bits
        }
}
```

Los EMM específicos de un subgrupo de módulos externos de seguridad o de un subgrupo de equipos receptores presentan el siguiente formato:

```
EMM-S_section() {
table_id = 0x8E                    8 bits
section_syntax_indicator = 0       1 bit
DVB_reserved                       1 bit
ISO_reserved                       2 bits
EMM-S_section_length               12 bits
share_address_field                24 bits
reserved                           6 bits
data_format                        1 bit
ADF_scrambling_flag                1 bit
para (i=0; i<N; i++) {
        EMM_data_byte              8 bits
        }
}
```

Según una característica suplementaria, los identificadores de módulos de seguridad están agrupados en una lista cifrada.

El procedimiento puede ser utilizado en una primera arquitectura en la que el equipo receptor incluye un descodificador y el módulo de seguridad incluye una tarjeta de control de acceso en la que están memorizadas las informaciones relativas a los derechos de acceso de un abonado a los datos digitales distribuidos por un operador.

En esta arquitectura, el emparejamiento se efectúa entre el descodificador y la tarjeta de control de acceso.

El procedimiento puede ser utilizado en una segunda arquitectura en la que el equipo receptor incluye un descodificador y el módulo de seguridad incluye una interfaz de seguridad amovible, dotada de una memoria no volátil y destinada a cooperar, por una parte, con el descodificador, y por otra parte, con una pluralidad de tarjetas de control de acceso condicional para gestionar el acceso a los datos digitales distribuidos por un operador.

En esta arquitectura, el emparejamiento se efectúa entre el citado descodificador y la citada interfaz de seguridad amovible.

El procedimiento puede ser utilizado en una tercera arquitectura en la que el equipo receptor incluye un descodificador dotado de una interfaz de seguridad amovible que tiene una memoria no volátil y que está destinada a cooperar, por una parte, con el citado descodificador, y por otra parte, con una pluralidad de tarjetas de control de acceso condicional.

En esta arquitectura, el emparejamiento se realiza entre la citada interfaz de seguridad amovible y las citadas tarjetas de control de acceso.

En una aplicación particular del procedimiento según la invención, los datos son programas audiovisuales.

El procedimiento según la invención se lleva a cabo en un sistema que incluye una pluralidad de equipos receptores conectados a una red de difusión de datos y/o servicios, siendo cada equipo receptor susceptible de ser emparejado con una pluralidad de módulos externos de seguridad, incluyendo asimismo este sistema una plataforma de gestión comercial que comunica con los citados equipos receptores y con los citados módulos externos de seguridad. Este sistema incluye, además:

- un primer módulo dispuesto en la citada plataforma de gestión comercial, y destinado a generar peticiones de emparejamiento, y

- un segundo módulo dispuesto en los citados equipos receptores y destinado a tratar las citadas peticiones para preparar una configuración de emparejamiento y para controlar este emparejamiento.

La invención se refiere asimismo a un equipo receptor susceptible de ser emparejado con una pluralidad de módulos externos de seguridad para gestionar el acceso a datos digitales distribuidos por un operador.

Según la invención, este equipo incluye medios para memorizar sobre la marcha el identificador de cada módulo

externo de seguridad conectado al mismo.

En un primer modo de realización, el equipo receptor incluye un descodificador y el módulo externo de seguridad es una tarjeta de control de acceso que incluye informaciones relativas a los derechos de acceso de un abonado a los citados datos digitales, efectuándose el emparejamiento entre el citado descodificador y la citada tarjeta.

En un segundo modo de realización, el equipo incluye un descodificador y el módulo externo de seguridad es una interfaz de seguridad amovible dotada de una memoria no volátil y destinada a cooperar, por una parte, con el citado descodificador, y por otra parte, con una pluralidad de tarjetas de control de acceso condicional, para gestionar el acceso a los citados datos digitales, realizándose el emparejamiento entre el citado descodificador y la citada interfaz de seguridad amovible.

En un tercer modo de realización, el equipo incluye un descodificador dotado de una interfaz de seguridad amovible que tiene una memoria no volátil y que está destinada a cooperar, por una parte, con el citado descodificador, y por otra parte, con una pluralidad de tarjetas de control de acceso condicional, y donde el emparejamiento se realiza entre la citada interfaz de seguridad amovible y las citadas tarjetas de control de acceso.

La invención se refiere asimismo a un descodificador susceptible de cooperar con una pluralidad de módulos externos de seguridad para gestionar el acceso a programas audiovisuales distribuidos por un operador, teniendo cada módulo externo de seguridad un identificador único e incluyendo al menos un algoritmo de tratamiento de datos.

El descodificador según la invención incluye medios para memorizar sobre la marcha el identificador de cada módulo externo de seguridad conectado al mismo.

En un primer modo de realización, los citados módulos externos de seguridad son tarjetas de control de acceso en las que están memorizadas informaciones relativas a los derechos de acceso de un abonado a los datos digitales distribuidos por un operador.

En un segundo modo de realización, dichos módulos externos de seguridad son interfaces de seguridad amovibles que incluyen una memoria no volátil y que están destinadas a cooperar, por una parte, con el descodificador, y por otra parte, con una pluralidad de tarjetas de control de acceso condicional para gestionar el acceso a los datos digitales distribuidos por un operador.

La invención se refiere asimismo a una interfaz de seguridad amovible que incluye una memoria no volátil y que está destinada a cooperar, por una parte, con un equipo receptor, y por otra parte, con una pluralidad de tarjetas de control de acceso condicional, para gestionar el acceso a los datos digitales distribuidos por un operador, teniendo cada tarjeta un identificador único e incluyendo informaciones relativas a los derechos de acceso de un abonado a los citados datos digitales.

La interfaz según la invención incluye medios para registrar sobre la marcha el identificador de cada tarjeta de control de acceso en la citada memoria no volátil.

En una primera variante, esta interfaz es una tarjeta PCMCIA (acrónimo de Personal Computer Memory Card International Association) que incluye una lógica de descodificación de datos digitales.

En una segunda variante, esta interfaz es un módulo lógico que puede ser ejecutado ya sea en el equipo receptor o ya sea en el módulo externo de seguridad.

La invención se refiere además a un programa de ordenador ejecutable en un equipo receptor susceptible de cooperar con una pluralidad de módulos externos de seguridad que tienen, cada uno de ellos, un identificador único y en los que están almacenadas informaciones relativas a los derechos de acceso de un abonado a los datos digitales distribuidos por un operador.

Este programa de ordenador incluye instrucciones para memorizar sobre la marcha el identificador de cada módulo externo de seguridad conectado a dicho equipo receptor e instrucciones destinadas a generar localmente parámetros de control de emparejamiento del equipo receptor con un módulo externo de seguridad en función de una señalización transmitida a dicho equipo receptor por el operador.

Este programa de ordenador incluye además instrucciones destinadas a verificar, en cada utilización posterior de un módulo externo de seguridad, con el equipo receptor, si el identificador de dicho módulo externo de seguridad está memorizado en el equipo receptor.

Breve descripción de los dibujos

Otras características y ventajas de la invención se pondrán de relieve mediante la descripción que sigue, tomada a

título de ejemplo no limitativo con referencia a los dibujos anexos, en los que:

la figura 1 representa una primera arquitectura para la puesta en práctica del emparejamiento según la invención;

la figura 2 representa una segunda arquitectura para la puesta en práctica del emparejamiento según la invención;

la figura 3 representa una tercera arquitectura para la puesta en práctica del emparejamiento según la invención;

la figura 4 representa mensajes EMM de configuración y de utilización de las funcionalidades de emparejamiento según la invención;

la figura 5 representa un diagrama de estado de la función de emparejamiento según la invención; y

la figura 6 representa un organigrama que ilustra un modo particular de realización del emparejamiento según la invención.

Exposición detallada de modos de realización particulares

La invención va a ser descrita ahora en el marco de una aplicación en la que un operador que difunde programas audiovisuales lleva a cabo el procedimiento según la invención para limitar la utilización de su parque de equipos receptores a sus propios abonados.

El procedimiento puede ser llevado a cabo en tres arquitecturas distintas ilustradas respectivamente mediante las figuras 1, 2 y 3. Los elementos idénticos en estas tres arquitecturas serán designados mediante referencias idénticas.

La gestión de emparejamiento se realiza a partir de una plataforma comercial 1 controlada por el operador y que comunica con el equipo receptor instalado en el domicilio del abonado.

En la primera arquitectura, ilustrada mediante la figura 1, el equipo receptor incluye un descodificador 2 en el que se ha instalado una lógica de control de acceso 4, y el módulo externo de seguridad es una tarjeta de control de acceso 6 que incluye informaciones relativas a los derechos de acceso de un abonado a los programas audiovisuales difundidos. En ese caso, el emparejamiento se efectúa entre el descodificador 2 y la citada tarjeta 6.

En la segunda arquitectura ilustrada mediante la figura 2, el equipo receptor incluye un descodificador 2, no dedicado al control de acceso, y el módulo externo de seguridad es una interfaz de seguridad amovible 8 dotada de una memoria no volátil y en la que está instalada la lógica de control de acceso 4. Esta interfaz 8 coopera, por una parte, con el citado descodificador 2, y por otra parte, con una tarjeta 6 entre una pluralidad de tarjetas de control de acceso condicional, para gestionar el acceso a los citados programas audiovisuales.

En esta arquitectura, el emparejamiento se realiza entre la citada interfaz de seguridad amovible 8 y la citada tarjeta de control de acceso 6.

En la tercera arquitectura, ilustrada mediante la figura 3, el equipo receptor incluye un descodificador 2 en el que está instalada una lógica de control de acceso 4, donde este descodificador 2 está conectado a una interfaz de seguridad amovible 8 que tiene una memoria no volátil que coopera con una tarjeta 6 entre una pluralidad de tarjetas de control de acceso condicional.

En este caso, el emparejamiento se efectúa entre el descodificador 2 y la interfaz de seguridad amovible 8.

La configuración y la utilización por el operador del emparejamiento resultan de comandos emitidos por la plataforma de gestión comercial 1.

La descripción que sigue se refiere a la puesta en práctica de la invención en el caso de emparejamiento de un descodificador 2 con una tarjeta 6. Las etapas ejecutadas se aplican a las tres arquitecturas descritas con anterioridad.

A la salida de fábrica de un descodificador 2, así como tras una tele-carga de la lógica de control de acceso 4 en este descodificador, todos los tratamientos de emparejamiento están inactivos. En particular:

- ningún identificador de tarjeta se encuentra memorizado en el descodificador 2,

- el número máximo de identificadores de tarjetas memorizables no ha sido inicializado,

- la memorización por el descodificador 2 del identificador de una tarjeta 6 no está activa,

- el control por el descodificador 2 del identificador de una tarjeta 6 no está activo.

Cuando se inserta una tarjeta válida en el lector de tarjeta previsto a este efecto en el descodificador 2, el emparejamiento entre esta tarjeta y el descodificador 2 puede ser configurado entonces por medio de una petición del operador en la plataforma de gestión 1, la cual emite hacia el descodificador 2 un mensaje de gestión EMM dedicado al emparejamiento. Este mensaje EMM es dirigido al descodificador 2 directamente, o bien indirectamente a través de la tarjeta 6. Este mensaje de gestión EMM permite realizar las tareas siguientes:

- activar en el descodificador 2 la función de emparejamiento; en ese caso, el descodificador 2 verifica si el identificador de la tarjeta 6 forma parte de los identificadores que tiene memorizados. Si no es ése el caso, y si el número máximo de identificadores de tarjetas memorizables no se ha alcanzado, el descodificador memoriza el identificador de esa tarjeta,

- desactivar en el descodificador la función de emparejamiento. En ese caso, el descodificador no controla ni memoriza el identificador de la tarjeta 6,

- eliminar los identificadores de tarjetas ya memorizados en el descodificador, y

- definir el número máximo de identificadores de tarjetas memorizables por el descodificador.

Además, el operador puede emitir, a través de la plataforma 1, un mensaje EMM que contenga una lista impuesta de identificadores de tarjetas 6 emparejadas a un descodificador 2. Un mensaje de ese tipo se direcciona al descodificador 2 indirectamente a través de la tarjeta 6.

Direccionamiento de mensajes EMM

Los mensajes EMM que permiten la configuración y la utilización de las funcionalidades ligadas al emparejamiento según el procedimiento de la invención, son emitidas por una vía EMM de un múltiplex digital tal como el definido en el estándar MPEG2/Sistema y en los estándares DVB/ETSI.

Esta vía puede difundir los EMM referenciando una dirección de tarjeta(s) que permita destinarlos:

- al descodificador en el que se inserta una tarjeta particular,

- a los descodificadores en los que se insertan las tarjetas de un grupo particular,

- a los descodificadores en los que se insertan todas las tarjetas.

Estos EMM destinados a los descodificadores “a través de la tarjeta” se utilizan especialmente cuando los descodificadores no disponen de ninguna dirección.

Esta vía puede difundir igualmente los EMM referenciando una dirección del (de los) descodificador(es) que permita destinarlos directamente:

- a un descodificador particular,

- a un grupo particular de descodificadores,

- a todos los descodificadores.

Los EMM destinados directamente a todos los descodificadores son utilizables igualmente cuando los descodificadores no disponen de dirección.

Los mensajes destinados a un descodificador designado por una tarjeta particular o directamente a un descodificador particular, son los EMM-U que presentan la estructura siguiente:

```
EMM-U_section() {
table_id = 0x88                     8 bits
section_syntax_indicator = 0        1 bit
DVB_reserved                        1 bit
ISO_reserved                        2 bits
EMM-U_section_length                12 bits
unique_address_field                40 bits
para (i=0; i<N; i++) {
        EMM_data_byte               8 bits
        }
```

}

El parámetro unique_adress_field es la dirección única de una tarjeta en un EMM-U tarjeta o la dirección única de un descodificador en un EMM_U descodificador.

Los mensajes destinados a los descodificadores designados por un grupo particular de tarjetas o directamente a un grupo particular de descodificadores son los EMM-S que presentan la estructura siguiente:

EMM-S_section() {	
table_id = 0x8E	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-S_section_length	12 bits
shared_address_field	24 bits
reserved	6 bits
data_format	1 bit
ADF_scrambling_flag	1 bit
para (i=0; i<N; i++) {	
EMM_data_byte	8 bits
}	
}	

El parámetro shared_address_field es la dirección del grupo de tarjetas en un EMM-S tarjeta o la dirección del grupo de descodificadores en un EMM-S descodificador. Un descodificador de un grupo o una tarjeta de un grupo está afectado(a) por el mensaje si además está designado(a) explícitamente en un campo ADF contenido en EMM_data_byte y que puede estar cifrado según la información ADF_scrambling_flag.

Los mensajes destinados a los descodificadores designados por todas las tarjetas o directamente a todos los descodificadores, son EMM-G que presentan la estructura siguiente:

EMM-G_section() {	
table_id = 0x8A o 0x8B	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-G_section_length	12 bits
para (i=0; i<N; i++) {	
EMM_data_byte	8 bits
}	
}	

Contenido de los mensajes EMM

La figura 4 ilustra esquemáticamente el contenido de los datos EMM_data_byte de un mensaje EMM de emparejamiento. Este contenido depende de la función que va a ejecutar el descodificador 2 para la configuración o la utilización del emparejamiento.

Los datos EMM_data_byte incluyen los parámetros funcionales siguientes:

- ADF 20: complemento de dirección de un descodificador en un grupo de descodificadores; este parámetro es útil en caso de direccionamiento por grupo, en otro caso puede ser omitido; puede estar cifrado,

- SOID 22: identificación de mensajes de emparejamiento según la invención, entre otros tipos de mensajes,

- OPID/NID 24: identificación del parque de descodificadores y de la señal del operador,

- TIME 26: datos de marca de tiempo de la emisión del mensaje; este parámetro se utiliza para evitar la reproducción del mensaje por un mismo descodificador,

- CRYPTO 28: identificación de las funciones de protección criptográfica aplicadas a los parámetros FUNCTIONS 32.

Los parámetros FUNCTIONS pueden estar cifrados y protegidos por una redundancia criptográfica 30.

- FUNCTIONS 32: conjunto de parámetros que describen la configuración y la utilización del emparejamiento.

Los parámetros funcionales que anteceden están organizados libremente en los datos EMM_data_byte de un mensaje EMM. Una implementación preferida es la combinación de estos parámetros mediante la estructura T L V (Tipo Longitud Valor).

Tratamiento de los mensajes EMM

Los parámetros funcionales que anteceden están destinados a ser tratados por el descodificador 2.

Cuando son transmitidos en un EMM descodificador, estos parámetros constituyen el contenido útil del EMM.

Cuando son transmitidos en un EMM tarjeta, estos parámetros constituyen una parte, claramente identificable mediante la tarjeta, del contenido útil del EMM que contiene otros parámetros concernientes a la tarjeta. Esta última se encarga después de extraer los parámetros funcionales que le conciernen a partir del EMM, y de transmitirlos al descodificador 2. Una realización preferida para permitir esta clase de mecanismo consiste en integrar estos parámetros funcionales en un parámetro de encapsulación no tratable por parte de la tarjeta. De ese modo, con la detección por medio de la tarjeta 6 de esta encapsulación, la tarjeta 6 envía al descodificador 2 una respuesta de tipo “Parámetro No Interpretable (PNI)” acompañada del conjunto de parámetros del descodificador 2.

La tarjeta 6 recibe igualmente una orden fechada de inscripción de datos a través de un EMM tarjeta, que permite, por una parte, asegurar que la tarjeta 6 no ha tratado ya este mensaje en otro descodificador, con el fin de evitar la reproducción en otro descodificador, y por otra parte, limitar el tratamiento de este EMM por medio de un solo descodificador. Semánticamente, estos datos significan “Ya tratado”. Una realización preferida de este mecanismo de anti-reproducción consiste en la inscripción de estos datos de anti-reproducción en un bloque de datos FAC (Facilities Data Block, en inglés) de la tarjeta.

Si a continuación del tratamiento de un EMM_tarjeta de emparejamiento la tarjeta responde “PNI” y “Ya Tratado”, el descodificador 2 no tiene en cuenta los parámetros que recibe.

Configuración y utilización del emparejamiento

El conjunto de parámetros FUNCTIONS 32 describe la configuración y la utilización del emparejamiento según la invención. Este conjunto de parámetros es una combinación cualquiera de los parámetros funcionales siguientes:

- MODO: este parámetro activa, desactiva o reinicializa la solución de emparejamiento. Tras la desactivación, el descodificador no controla el identificador de una tarjeta insertada en el descodificador, pero conserva la lista de identificadores ya memorizados, y tras la reinicialización, el descodificador no controla el identificador de una tarjeta insertada y no tiene ya el identificador de tarjetas memorizado.

- NBCA (Número de tarjetas autorizadas): este parámetro impone el número máximo de identificadores de tarjetas que un descodificador está autorizado a memorizar; cuando no se ha informado del mismo, el NBCA se define mediante la implementación del módulo lógico en el descodificador según la invención.

- LCA (Lista de tarjetas autorizadas): este parámetro impone a un descodificador la lista de identificadores de tarjetas con las que puede funcionar.

- Perturbación: este parámetro describe la perturbación a aplicar por el descodificador en el acceso a los datos en caso de una tarjeta no emparejada con el descodificador.

Los parámetros funcionales que antecede están organizados libremente en el conjunto de parámetros FUNCTIONS 32. Una implementación preferida es la combinación de estos parámetros mediante la estructura T L V (Tipo Longitud Valor).

Funcionamiento

Ahora se va a describir el funcionamiento del emparejamiento según la invención mediante referencia a las figuras 5 y 6.

La figura 5 es un diagrama funcional que ilustra esquemáticamente los estados de la función de emparejamiento de la lógica de control de acceso 4 incluida en un descodificador 2.

La función de emparejamiento está en estado inactivo 60 cuando la lógica de control de acceso 4 acaba de ser instalada o tele-cargada (etapa 61) o cuando ha recibido de la plataforma 1 una orden de desactivación del emparejamiento (etapa 62) o de reinicialización del emparejamiento (etapa 64). En este caso, la lógica de control de acceso 4 acepta funcionar con una tarjeta 6 insertada en el descodificador 2 sin verificar su emparejamiento con esta tarjeta.

Para efectuar la activación del emparejamiento en un descodificador 2, el operador define a través de la plataforma 1 un modo de emparejamiento (= activo), opcionalmente el número máximo NBCA de tarjetas 6 susceptibles de ser emparejadas con el descodificador 2 y el tipo de perturbación aplicable en el acceso a los datos en caso de fallo del emparejamiento. En función de estas informaciones, la plataforma 1 genera y emite (flecha 68) un mensaje EMM que direcciona el, o los, descodificador(es) afectado(s) y que contiene(n) los parámetros de configuración. La función de emparejamiento en el descodificador pasa al estado activo 70.

El operador puede desactivar el emparejamiento en el descodificador 2, a través de la plataforma 1 que genera y emite (flecha 72) un mensaje EMM que direcciona el, o los, descodificador(es) afectado(s) y que contiene una orden de desactivación sin borrado del contexto de emparejamiento 62 o de una orden de RAZ del contexto de emparejamiento 64. La función de emparejamiento en el descodificador pasa al estado inactivo 60.

Cualquiera que sea el estado inactivo o activo de la función de emparejamiento, ésta puede recibir (etapa 74) una lista de tarjetas autorizadas LCA mediante un EMM emitido por la plataforma 1.

La toma en consideración de una tarjeta 6 por la función de emparejamiento en un descodificador 2, se describe en el organigrama de la figura 6.

Con la inserción (etapa 80) de una tarjeta 6 en el descodificador 2, la lógica de control de acceso 4 incorporada en el descodificador comprueba (etapa 82) si la función de emparejamiento está en estado activo 70.

Si la función de emparejamiento está en el descodificador en el estado inactivo 60, el descodificador acepta funcionar con la tarjeta introducida (etapa 92).

Si la función de emparejamiento está en el descodificador en el estado activo 70, la lógica de control de acceso lee el identificador de la tarjeta y verifica (etapa 84) si este identificador de la tarjeta insertada está ya memorizado en el descodificador 2. Si el identificador de esta tarjeta 6 está memorizado en el descodificador 2, la lógica de control de acceso 4 acepta funcionar con la tarjeta insertada (etapa 92). En ese caso, el acceso a los programas difundidos es siempre posible, bajo reserva de conformidad de las otras condiciones de acceso unidas a estos programas.

Si el identificador de esta tarjeta 6 no está memorizado en el descodificador 2, la lógica de control de acceso verifica (etapa 86) si el número de identificadores de tarjetas 6 ya memorizados es inferior a un valor máximo NBCA de tarjetas 6 autorizadas por la configuración.

- Si se alcanza ese número NBCA, la lógica de control de acceso 4 rehúsa funcionar con la tarjeta 6 insertada en el lector del descodificador 2, y aplica (etapa 90) la perturbación en el acceso a los datos tal como ha sido definido por el operador. Una perturbación de ese tipo puede consistir en bloquear el acceso a los programas difundidos. Ésta puede ir acompañada de la presentación en una pantalla del terminal al que esté asociado el descodificador 2 de un mensaje que invite al abonado a insertar otra tarjeta 6 en el descodificador 2,

- Si no se alcanza ese número NBCA, el identificador de la tarjeta 6 insertada en el lector del descodificador 2 se añade a la lista de identificadores memorizados (etapa 88). La lógica de control de acceso 4 acepta entonces funcionar con la tarjeta 6 insertada (etapa 92).

Cuando la tarjeta 6 se extrae (etapa 94) del descodificador 2, la lógica de control de acceso 4 pasa a espera de la inserción de una tarjeta 6 (etapa 80).

La perturbación 90 en el acceso a los datos en caso de fallo de emparejamiento puede ser de diferente naturaleza, tal como por ejemplo:

- Parada de audio y de video en los canales encriptados (obtenida por no remitir ECM a la tarjeta para calcular CW);

- Parada de audio y de video en los canales en abierto y analógicos (obtenida mediante mensaje en middleware);

- Envío de un mensaje en middleware desde el terminal (por ejemplo: mensaje Open TV).

Esta perturbación puede ser utilizada asimismo para provocar el bloqueo de descodificadores robados.

En el caso descrito en la figura 2, en donde la lógica de control de acceso 4 se ejecuta en la interfaz amovible 8 conectada a un descodificador 2, el autómata descrito en la figura 4 y el organigrama descrito en la figura 5 se aplican directamente a la lógica de control de acceso incorporada 4 en esta interfaz amovible 8.

REIVINDICACIONES

1.- Procedimiento de emparejamiento de un equipo receptor de datos digitales (2) con una pluralidad de módulos externos de seguridad (6, 8) que tienen, cada uno de ellos, un identificador único destinado a gestionar el acceso a los datos digitales distribuidos por un operador, procedimiento caracterizado por las etapas siguientes:

- transmitir al equipo receptor (2) una señalización que incluye al menos un mensaje de gestión de la memorización del identificador del módulo externo de seguridad (6, 8) y/o un mensaje de gestión de la fase de control que incluye un número NBCA que representa el número máximo de identificadores de tarjetas que un descodificador está autorizado a memorizar,

- conectar un módulo externo de seguridad (6, 8) al equipo receptor,

- memorizar sobre la marcha en el equipo receptor (2) el identificador único del módulo de seguridad (6, 8) conectado,

- verificar si se alcanza o no el número NBCA,

- si se alcanza el número NBCA, prohibir la memorización,

- si no, autorizar la memorización.

2.- Procedimiento según la reivindicación 1, caracterizado porque incluye además una fase de control que consiste en verificar, en cada conexión posterior de un módulo externo de seguridad (6, 8) al equipo receptor (2), si el identificador de dicho módulo está memorizado en ese equipo receptor (2).

3.- Procedimiento según la reivindicación 1, caracterizado porque la citada señalización incluye al menos una de las consignas siguientes:

- autorizar la memorización,

- prohibir la memorización

- eliminar los identificadores ya memorizados en el equipo receptor (2),

- activar o desactivar la fase de control.

4.- Procedimiento según la reivindicación 3, caracterizado porque la citada señalización incluye además una consigna de reconfiguración mediante la que se transmite al equipo receptor (2) una lista actualizada de los identificadores de los módulos externos de seguridad (6, 8) emparejados con el citado equipo receptor (2).

5.- Procedimiento según la reivindicación 4, caracterizado porque la citada lista es transmitida directamente al equipo receptor (2).

6.- Procedimiento según la reivindicación 4, caracterizado porque la citada lista es transmitida a través de un módulo externo de seguridad (6, 8) conectado a dicho equipo receptor (2).

7.- Procedimiento según la reivindicación 2, en el que la citada fase de control incluye un procedimiento que consiste en perturbar el tratamiento de datos si el identificador del módulo externo de seguridad (6, 8) conectado no ha sido previamente memorizado por el equipo receptor (2).

8.- Procedimiento según la reivindicación 1, caracterizado porque los citados datos son distribuidos en abierto o encriptados por medio de una palabra de control cifrada, y porque cada módulo externo de seguridad (6, 8) incorpora los derechos de acceso a los citados datos y un algoritmo de desencriptación de la citada palabra de control.

9.- Procedimiento según la reivindicación 4, caracterizado porque la citada señalización es transmitida a un equipo receptor (2) en un mensaje EMM específico de un módulo externo de seguridad (6, 8) asociado a ese equipo receptor (2).

10.- Procedimiento según la reivindicación 4, caracterizado porque la citada señalización es transmitida a un equipo receptor (2) en un mensaje EMM específico de ese equipo receptor (2).

11.- Procedimiento según la reivindicación 4, caracterizado porque, para un equipo receptor (2) dado, la lista actualizada de los identificadores de los módulos externos de seguridad (6, 8) es transmitida en un mensaje EMM específico a un módulo de seguridad (6, 8) asociado a este equipo receptor (2).

12.- Procedimiento según la reivindicación 4, caracterizado porque la citada señalización es transmitida a un grupo de equipos receptores (2) en un mensaje EMM específico de un grupo de módulos externos de seguridad (6, 8) asociados a los citados equipos receptores (2).

13.- Procedimiento según la reivindicación 4, caracterizado porque la citada señalización es transmitida a un grupo de equipos receptores (2) en un mensaje EMM específico de dicho grupo de equipos receptores (2).

14.- Procedimiento según la reivindicación 4, caracterizado porque, para un grupo de equipos receptores (2) dado, la lista actualizada de los identificadores de los módulos externos de seguridad (6, 8) se transmite en un mensaje EMM específico de un grupo de módulos externos de seguridad (6, 8) asociados a dichos equipos receptores (2).

15.- Procedimiento según la reivindicación 4, caracterizado porque la citada señalización de control es transmitida en un flujo privado a un grupo de equipos receptores (2).

16.- Procedimiento según la reivindicación 4, caracterizado porque, para un grupo de equipos receptores (2) dado, la lista actualizada de los identificadores de los módulos externos de seguridad (6, 8) se transmite en un flujo privado a cada equipo receptor (2).

17.- Procedimiento según la reivindicación 16, caracterizado porque el citado flujo privado es tratado por medio de una lógica dedicada, ejecutable en cada equipo receptor (2) en función del identificador del módulo externo de seguridad (6, 8) asociado al mismo.

18.- Procedimiento según una de las reivindicaciones 9 a 14, caracterizado porque incluye además un mecanismo destinado a impedir la utilización de un EMM transmitido a un mismo módulo externo de seguridad (6, 8) en dos equipos receptores (2) distintos.

19.- Procedimiento según la reivindicación 18, caracterizado porque el citado EMM presenta el formato siguiente:

```
EMM-U_section() {
table_id = 0x88                 8 bits
section_syntax_indicator = 0    1 bit
DVB_reserved                    1 bit
ISO_reserved                    2 bits
EMM-U_section_length            12 bits
unique_address_field            40 bits
para (i=0; i<N; i++) {
        EMM_data_byte           8 bits
        }
}
```

20.- Procedimiento según una de las reivindicaciones 12 a 14, caracterizado porque el citado EMM es específico de todos los módulos externos de seguridad (6, 8) o de todos los equipos receptores (2) y presenta el siguiente formato:

```
EMM-G_section() {
table_id = 0x8A o 0x8B          8 bits
section_syntax_indicator = 0    1 bit
DVB_reserved                    1 bit
ISO_reserved                    2 bits
EMM-G_section_length            12 bits
para (i=0; i<N; i++) {
        EMM_data_byte           8 bits
        }
}
```

21.- Procedimiento según una de las reivindicaciones 12 a 14, caracterizado porque el citado EMM es específico de un subgrupo de módulos externos de seguridad (6, 8) o de equipos receptores (2), y presenta el formato siguiente:

```
EMM-S_section() {
table_id = 0x8E                 8 bits
section_syntax_indicator = 0    1 bit
DVB_reserved                    1 bit
ISO_reserved                    2 bits
EMM-S_section_length            12 bits
shared_address_field            24 bits
reserved                        6 bits
```

```
data_format                    1 bit
ADF_scrambling_flag            1 bit
para (i=0; i<N; i++) {
        EMM_data_byte          8 bits
        }
}
```

22.- Procedimiento según la reivindicación 1, caracterizado porque los identificadores de módulos externos de seguridad (6, 8) están agrupados en una lista cifrada.

23.- Procedimiento según una cualquiera de las reivindicaciones 1 a 22, caracterizado porque el equipo receptor (2) incluye un descodificador y el módulo externo de seguridad (6, 8) incluye una tarjeta de control de acceso (6) en la que están memorizadas las informaciones relativas a los derechos de acceso de un abonado a los datos digitales distribuidos por un operador, y porque el emparejamiento se efectúa entre el citado descodificador y la citada tarjeta (6).

24.- Procedimiento según una cualquiera de las reivindicaciones 1 a 22, caracterizado porque el equipo receptor (2) incluye un descodificador y el módulo externo de seguridad (6, 8) incluye una interfaz de seguridad amovible (8) dotada de una memoria no volátil y destinada a cooperar, por una parte, con el descodificador, y por otra parte, con una pluralidad de tarjetas de control (6) de acceso condicional para gestionar el acceso a los datos digitales distribuidos por un operador, y porque el emparejamiento se efectúa entre el citado descodificador y la citada interfaz (8) de seguridad amovible.

25.- Procedimiento según una cualquiera de las reivindicaciones 1 a 22, caracterizado porque el equipo receptor (2) incluye un descodificador dotado de una interfaz de seguridad amovible (8) que tiene una memoria no volátil y está destinada a cooperar, por una parte, con el citado descodificador, y por otra parte, con una pluralidad de tarjetas de control (6) de acceso condicional, y porque el emparejamiento se realiza entre la citada interfaz de seguridad amovible (8) y las citadas tarjetas de control de acceso (6).

26.- Procedimiento según la reivindicación 8, caracterizado porque los datos son programas audiovisuales.

27.- Equipo receptor (2) susceptible de ser emparejado con una pluralidad de módulos externos de seguridad (6, 8), cada uno de los cuales tiene un identificador único para gestionar el acceso a los datos digitales distribuidos por un operador, caracterizado porque incluye:

- medios para memorizar sobre la marcha el identificador de cada módulo externo de seguridad (6, 8) conectado a los mismos,

- medios para verificar si se ha alcanzado o no un número NBCA que representa el número máximo de identificadores de tarjetas que un descodificador está autorizado a memorizar, transmitidos previamente al equipo receptor (2) que representa el número máximo de identificadores de tarjetas que un equipo receptor (2) está autorizado a memorizar,

- medios para prohibir la memorización en caso de que el número NBCA haya sido alcanzado, y

- medios para autorizar la memorización si el número NBCA no ha sido alcanzado.

28.- Equipo según la reivindicación 27, caracterizado porque incluye un descodificador, y porque el módulo externo de seguridad (6, 8) es una tarjeta de control de acceso (6) que incluye informaciones relativas a los derechos de acceso de un abonado a los citados datos digitales, siendo realizado el emparejamiento entre el citado descodificador y la citada tarjeta (6).

29.- Equipo receptor según la reivindicación 28, caracterizado porque incluye un descodificador, y porque el módulo externo de seguridad (6, 8) es una interfaz de seguridad amovible (8) dotada de una memoria no volátil y destinada a cooperar, por una parte, con el citado descodificador, y por otra parte, con una pluralidad de tarjetas de control de acceso condicional (6), para gestionar el acceso a los citados datos digitales, siendo efectuado el emparejamiento entre el citado descodificador y la citada interfaz de seguridad amovible (8).

30.- Equipo receptor según la reivindicación 27, caracterizado porque incluye un descodificador dotado de una interfaz de seguridad amovible (8) que tiene una memoria no volátil y que está destinada a cooperar, por una parte, con el citado descodificador, y por otra parte, con una pluralidad de tarjetas de control (6) de acceso condicional, y porque el emparejamiento se realiza entre la citada interfaz de seguridad amovible (8) y las citadas tarjetas de control de acceso (6).

31.- Interfaz de seguridad amovible (8) que incluye una memoria no volátil y que está destinada a cooperar, por una parte, con un equipo receptor (2), y por otra parte, con una pluralidad de tarjetas de control de acceso (6)

condicional, para gestionar el acceso a los datos digitales distribuidos por un operador, teniendo cada tarjeta (6) un identificador único e incluyendo informaciones relativas a los derechos de acceso de un abonado a los citados datos digitales, estando la interfaz caracterizada porque incluye:

- medios para memorizar sobre la marcha el identificador de cada módulo externo de seguridad (6, 8) conectado a los mismos;

- medios para verificar si se ha alcanzado o no un número NBCA que representa el número máximo de identificadores de tarjetas que un descodificador está autorizado a memorizar, transmitidos previamente al equipo receptor (2), que representan el número máximo de identificadores de tarjetas que un equipo receptor (2) está autorizado a memorizar,

- medios para prohibir la memorización en caso de que haya alcanzado el número NBCA, y

- medios para autorizar la memorización si el número NBCA no ha sido alcanzado.

32.- Interfaz según la reivindicación 31, caracterizada porque la misma consiste en una tarjeta PCMCIA que incluye una lógica de descodificación de datos digitales.

33.- Interfaz según la reivindicación 32, caracterizada porque consiste en un módulo lógico.

34.- Programa de ordenador ejecutable en un equipo receptor (2) susceptible de cooperar con una pluralidad de módulos externos de seguridad (6, 8) que tienen, cada uno de ellos, un identificador único y en los que están almacenadas informaciones relativas a los derechos de acceso de un abonado a los datos digitales distribuidos por un operador, caracterizado porque incluye:

- instrucciones para memorizar sobre la marcha el identificador de cada módulo externo de seguridad (6, 8) al que esté conectado,

- instrucciones para verificar si se ha alcanzado o no un número NBCA que representa el número máximo de identificadores de tarjetas que un equipo receptor (2) está autorizado a memorizar, transmitidos previamente al equipo receptor (2), que representa el número máximo de identificadores de tarjetas que un equipo receptor (2) está autorizado a memorizar,

- instrucciones para prohibir la memorización en caso de que se haya alcanzado el número NBCA, y

- medios para autorizar la memorización si el número NBCA no se ha alcanzado.

35.- Programa de ordenador según la reivindicación 34, caracterizado porque incluye, además, instrucciones destinadas a generar localmente parámetros de control del emparejamiento del equipo receptor (2) con un módulo externo de seguridad (6, 8) en función de una señalización transmitida a dicho equipo receptor (2) por el operador.

36.- Sistema que incluye una pluralidad de equipos receptores (2) según la reivindicación 27, conectados a una red de difusión de datos y/o servicios, siendo cada equipo receptor (2) susceptible de ser emparejado con una pluralidad de módulos externos de seguridad (6, 8), incluyendo el citado sistema además una plataforma de gestión comercial (1) que comunica con los equipos receptores (2) y con los citados módulos externos de seguridad (6, 8), caracterizado porque incluye además:

- un primer módulo dispuesto en la citada plataforma de gestión comercial (1), y destinado a generar peticiones de emparejamiento, y

- un segundo módulo dispuesto en los citados equipos receptores (2) y destinado a tratar las citadas peticiones para preparar una configuración del emparejamiento y para controlar el emparejamiento.

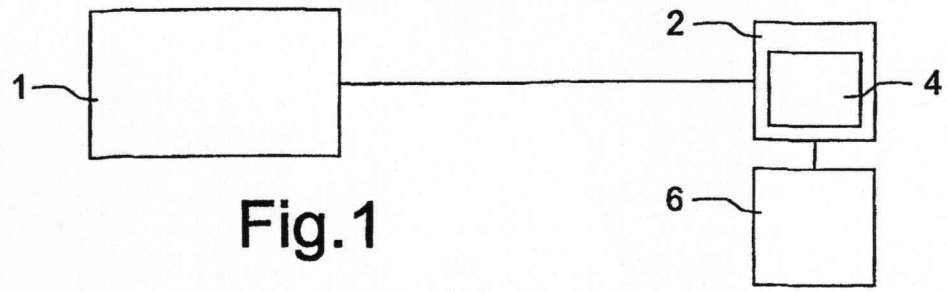

Fig.1

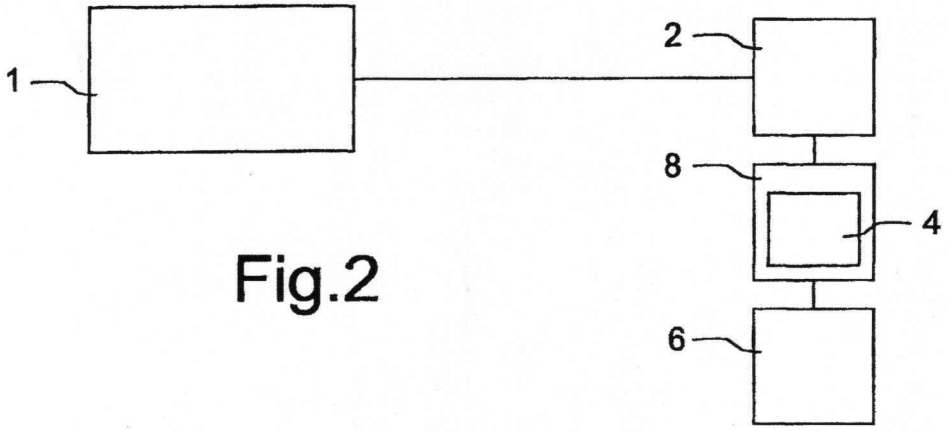

Fig.2

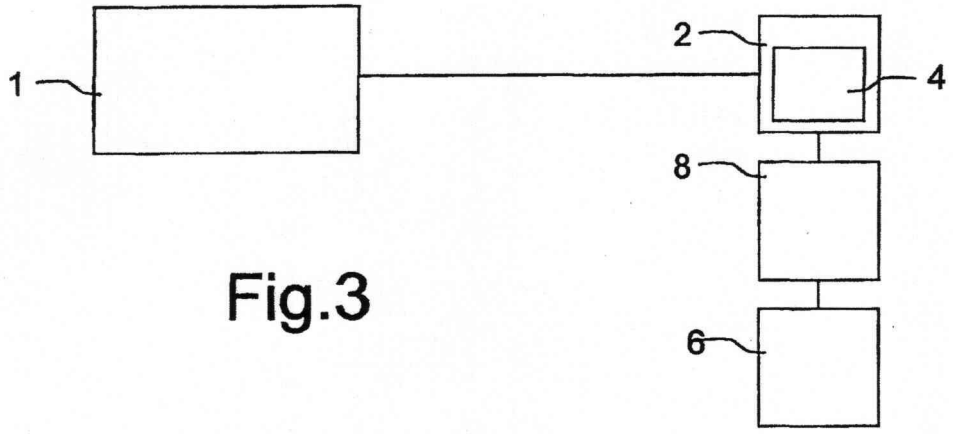

Fig.3

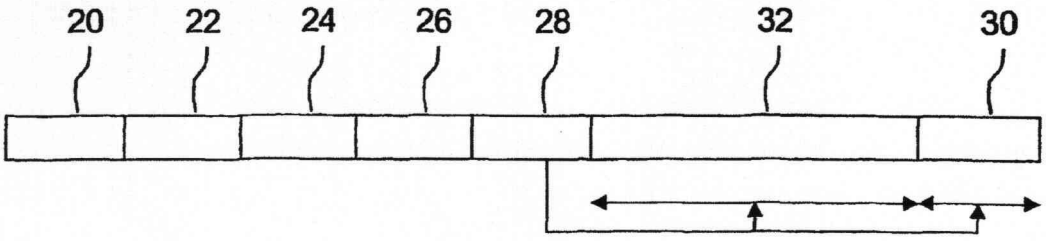

Fig.4

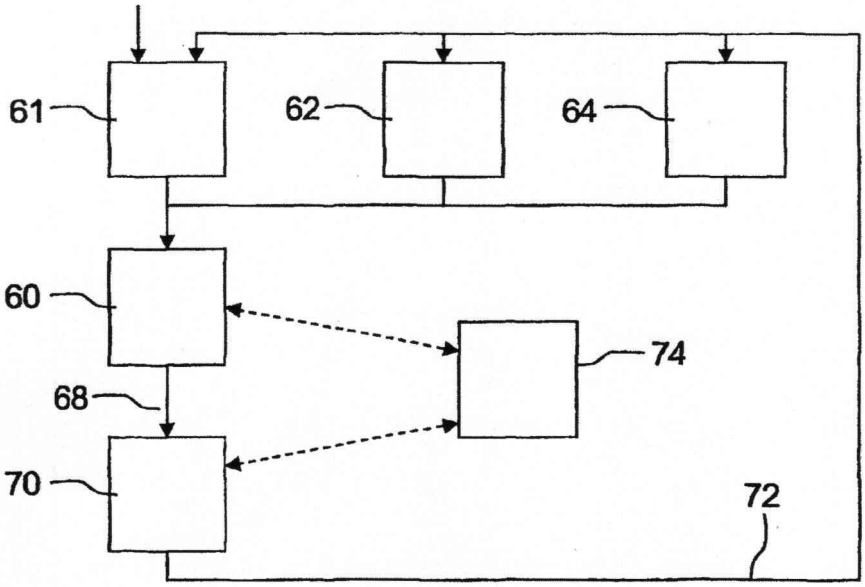

Fig.5

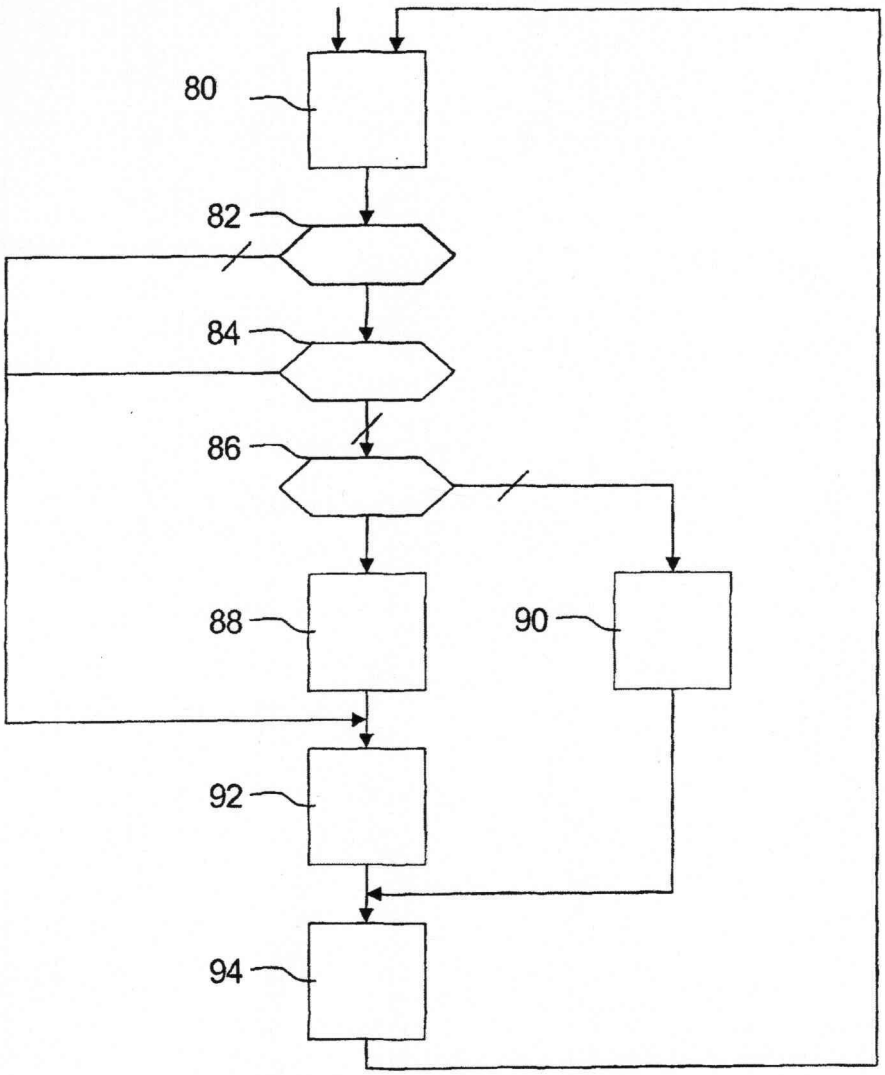

Fig.6