(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 339 261**

(51) Int. Cl.:
H04N 7/167 (2006.01)
H04N 5/00 (2006.01)
H04N 7/16 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05728066 .1**
(96) Fecha de presentación : **17.02.2005**
(97) Número de publicación de la solicitud: **1716705**
(97) Fecha de publicación de la solicitud: **02.11.2006**

(54) Título: **Procedimiento de emparejamiento de un número N de terminales receptores con un número M de tarjetas de control de acceso condicional.**

(30) Prioridad: **20.02.2004 FR 04 50324**

(45) Fecha de publicación de la mención BOPI:
18.05.2010

(45) Fecha de la publicación del folleto de la patente:
18.05.2010

(73) Titular/es: **Viaccess**
Les Collines de l'Arche, Tour Opéra C
92057 Paris La Défense Cédex, FR

(72) Inventor/es: **Beun, Frédéric;**
Boudier, Laurence;
Roque, Pierre y
Tronel, Bruno

(74) Agente: **Justo Bailey, Mario de**

DESCRIPCIÓN

Procedimiento de emparejamiento de un número N de terminales receptores con un número M de tarjetas de control de acceso condicional.

Campo técnico

La invención se sitúa en el campo de la protección de datos digitales difundidos y de los equipos receptores destinados a recibir estos datos en una red de distribución de datos y/o servicios y se refiere más específicamente a un procedimiento de emparejamiento de un número N de equipos receptores de datos con un número M de módulos externos de seguridad, estando provisto cada equipo receptor de un identificador único, y teniendo cada módulo externo de seguridad un identificador único.

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

Estado de la técnica anterior

Cada vez más operadores ofrecen datos y servicios en línea accesibles por medio de terminales provistos de procesadores de seguridad. Generalmente, los datos y servicios distribuidos son encriptados en la emisión mediante unas claves secretas y desencriptados en la recepción mediante las mismas claves secretas previamente puestas a disposición del abonado.

Además de las técnicas clásicas de control de acceso basadas en la encriptación en la emisión y la desencriptación en la recepción de los datos distribuidos, los operadores proponen unas 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 los usuarios provistos de un terminal robado o de una tarjeta pirata.

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 y 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 proviene del hecho de que la asociación entre un receptor y el módulo de seguridad al que se empareja se establece *a priori*, y que no permite al operador administrar eficazmente su parque de equipos receptores con el fin de impedir el desvío de este equipo para usos fraudulentos.

Un objeto del procedimiento de emparejamiento según la invención es permitir a cada operador limitar los usos de su parque de material de recepción controlando dinámicamente las configuraciones del equipo receptor y de los módulos externos de seguridad destinados a cooperar con este equipo.

Exposición de la invención

La invención preconiza un procedimiento de emparejamiento de un número N de equipos receptores de datos con un número M de módulos externos de seguridad, estando provisto cada equipo receptor de un identificador único, y teniendo cada módulo externo de seguridad un identificador único, comprendiendo este procedimiento una fase de configuración y una fase de control.

Según la invención, la fase de configuración comprende las siguientes etapas:

- memorizar en cada módulo externo de seguridad una lista de identificadores de equipos receptores,

- memorizar en cada equipo receptor una lista de identificadores de módulos externos de seguridad,

y la fase de control consiste en autorizar el acceso a los datos, si el identificador de un módulo externo de seguridad conectado a un equipo receptor está presente en la lista memorizada en este equipo receptor y si el identificador de dicho equipo receptor está presente en la lista memorizada en dicho módulo externo de seguridad, si no, perturbar el acceso a dichos datos.

Preferentemente, la configuración se pone en marcha únicamente cuando el usuario conecta un módulo externo de seguridad a un equipo receptor.

En un modo preferido de realización, el procedimiento según la invención comprende una etapa en la que el operador transmite al equipo receptor una señalización para administrar la fase de control que comprende al menos una de las siguientes consignas:

- activar la fase de control en una fecha o después de un plazo programados,

- desactivar la fase de control en una fecha o después de un plazo programados,

- especificar una fecha absoluta (respectivamente un plazo) a partir de la cual (respectivamente al cabo del cual) se inicia la activación o la desactivación de la fase de control,

- anular dicha fecha programada (respectivamente dicho plazo programado).

En una primera variante, el operador transmite además al equipo receptor una señalización que comprende un mensaje de supresión de la lista de los identificadores memorizados en el equipo receptor.

Dicho mensaje de señalización se transmite a dicho equipo receptor a través de un mensaje EMM (*Entitlement Management Message*, en inglés) específico de este equipo receptor.

Esta señalización puede ser transmitida a un grupo de equipos receptores a través de un mensaje EMM específico de dicho grupo de equipos receptores.

En una segunda variante, el operador transmite además al módulo externo de seguridad una señalización que comprende un mensaje de supresión de la lista de los identificadores memorizados en este módulo externo de seguridad. Dicho mensaje de señalización se transmite a dicho módulo externo de seguridad a través de un mensaje EMM específico, y puede ser transmitido para un grupo de módulos externos de seguridad a través de un mensaje EMM específico a dicho grupo de módulos externos de seguridad.

Según otra característica del procedimiento según la invención, el operador transmite, por una parte, a un equipo receptor la lista de los M identificadores de los módulos externos de seguridad a través de un mensaje EMM específico a dicho equipo receptor y, por otra parte, a un módulo externo de seguridad la lista de los N identificadores de equipos receptores a través de un mensaje EMM específico a dicho módulo externo de seguridad.

Según otra variante, el operador transmite, por una parte, a un grupo de equipos receptores la lista de los M identificadores de módulos externos de seguridad a través de un mensaje EMM específico a dicho grupo de equipos receptores y, por otra parte, a un grupo de módulos externos de seguridad la lista de los N identificadores de equipos receptores a través de un mensaje EMM específico a dicho grupo de módulos externos de seguridad.

En otra variante de realización, el operador transmite a un grupo de equipos receptores un mensaje de señalización para la fase de control en un flujo privado que se trata mediante un programa dedicado ejecutable en cada equipo receptor en función del identificador de dicho equipo receptor.

Alternativamente, la lista de identificadores de módulos externos de seguridad se transmite en un flujo privado a un grupo de equipos receptores y tratada por un programa dedicado ejecutable en cada equipo receptor en función del identificador de dicho equipo receptor, y la lista de identificadores de equipos receptores se transmite a un grupo de módulos externos de seguridad en un flujo privado que se trata por medio de un programa dedicado ejecutable en cada uno de dichos módulos externos de seguridad o en el equipo receptor al que está conectado uno de dichos módulos externos de seguridad, en función del identificador de dicho módulo externo de seguridad.

En un ejemplo de aplicación del procedimiento según la invención, los datos digitales representan unos programas audiovisuales distribuidos en abierto o en forma encriptada.

Según una característica suplementaria, la lista de los identificadores de los M módulos de seguridad memorizados en un equipo receptor está cifrada, y la lista de los identificadores de los N equipos receptores memorizados en un módulo externo de seguridad está cifrada.

Ventajosamente, el procedimiento según la invención comprende además un mecanismo destinado a impedir la utilización de un EMM transmitido a un mismo módulo externo de seguridad o a un mismo equipo receptor.

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

```
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_lenght                    12 bits
unique_adress_field                     40 bits
for (i=0; i<N; i++) {
     EMM_data_byte                      8 bits
     }
}
```

Los mensajes EMM que conciernen a todos los módulos externos de seguridad o a todos los equipos receptores presentan el siguiente formato:

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

Los mensajes EMM específicos a un subgrupo de módulos externos de seguridad o a 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_lenght                    12 bits
shared_address_field                    24 bits
Reserved                                6 bits
data_format                             1 bit
ADF_scrambling_flag                     1 bit
```

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

El procedimiento según la invención se pone en marcha en un sistema de control de acceso que comprende una pluralidad de equipos receptores que tienen cada uno un identificador único y susceptibles de cooperar con una pluralidad de módulos externos de seguridad que tienen cada uno un identificador único, comprendiendo cada módulo externo de seguridad unas informaciones relativas a los derechos de acceso de un abonado a unos datos digitales distribuidos por un operador, comprendiendo este sistema igualmente una plataforma de gestión comercial que comunica con dichos equipos receptores y con dichos módulos externos de seguridad. Este sistema comprende además:

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

- y un segundo módulo dispuesto en dichos equipos receptores y los módulos externos de seguridad y destinado a tratar dichas peticiones para preparar una configuración del emparejamiento.

El procedimiento según la invención es utilizable en una arquitectura en la que el equipo receptor comprende un decodificador y el módulo externo de seguridad comprende una tarjeta de control de acceso en la que están memorizadas unas informaciones relativas a los derechos de acceso de un abonado a unos datos digitales distribuidos por un operador. En este caso, el emparejamiento se efectúa entre dicho decodificador y dicha tarjeta.

Alternativamente, el procedimiento según la invención puede ser utilizado en una arquitectura en la que el equipo receptor comprende un decodificador y el modulo externo de seguridad comprende una interfaz de seguridad amovible provista de una memoria no volátil y destinada a cooperar, por una parte, con el decodificador y, por otra parte, con una pluralidad de tarjetas de control de acceso condicional para administrar el acceso a unos datos digitales distribuidos por un operador. En este caso, el emparejamiento se efectúa entre dicho decodificador y dicha interfaz de seguridad amovible.

El procedimiento según la invención puede ser utilizado igualmente en una arquitectura en la que el equipo receptor comprende un decodificador provisto de una interfaz de seguridad amovible que tiene una memoria no volátil y destinada a cooperar, por una parte, con dicho decodificador y, por otra parte, con una pluralidad de tarjetas de control de acceso condicional. En este caso, el emparejamiento se realiza entre dicha interfaz de seguridad amovible y dichas tarjetas de control de acceso.

La invención se refiere igualmente a un equipo receptor susceptible de ser emparejado con una pluralidad de módulos externos de seguridad para administrar el acceso a unos datos digitales distribuidos por un operador. Este equipo receptor comprende:

- una memoria no volátil destinada a memorizar una lista de módulos externos de seguridad,

- unos medios para verificar si el identificador de un módulo externo de seguridad conectado a dicho equipo está presente en la lista memorizada en dicha memoria no volátil.

En un primer modo de realización, este equipo receptor comprende un decodificador y el módulo externo de seguridad es una tarjeta de control de acceso que comprende unas informaciones relativas a los derechos de acceso de un abonado a dichos datos digitales, siendo efectuado el emparejamiento en este caso entre dicho decodificador y dicha tarjeta.

En un segundo modo de realización, este equipo receptor comprende un decodificador y el módulo externo de seguridad es una interfaz de seguridad amovible provista de una memoria no volátil y destinada a cooperar, por una parte, con dicho decodificador y, por otra parte, con una pluralidad de tarjetas de control de acceso condicional, para administrar el acceso a dichos datos digitales, siendo efectuado en este caso el emparejamiento entre dicho decodificador y dicha interfaz de seguridad amovible.

En un tercer modo de realización, este equipo receptor comprende un decodificador provisto de una interfaz de seguridad amovible que tiene una memoria no volátil y destinada a cooperar, por una parte, con dicho decodificador y, por otra parte, con una pluralidad de tarjetas de control de acceso condicional y el emparejamiento se realiza entre dicha interfaz de seguridad amovible y dichas tarjetas de control de acceso.

La invención se refiere igualmente a un decodificador susceptible de cooperar con una pluralidad de módulos externos de seguridad para administrar el acceso a unos programas audiovisuales distribuidos por un operador, teniendo cada módulo externo de seguridad un identificador único y que comprende al menos un algoritmo de tratamiento de datos. Este decodificador comprende:

- una memoria no volátil destinada a memorizar una lista de módulos externos de seguridad,

- unos medios para verificar si el identificador de un módulo externo de seguridad conectado a dicho decodificador está presente en la lista memorizada en dicha memoria no volátil.

En una primera variante, dichos módulos externos de seguridad son unas tarjetas de control de acceso en las que están memorizadas unas informaciones relativas a los derechos de acceso de un abonado a unos datos digitales distribuidos por un operador.

En una segunda variante, dichos módulos externos de seguridad son unas interfaces de seguridad amovibles que comprenden una memoria no volátil y destinadas a cooperar, por una parte, con el decodificador y, por otra parte, con una pluralidad de tarjetas de control de acceso condicional para administrar el acceso a unos datos digitales distribuidos por un operador.

La invención se refiere igualmente a una interfaz de seguridad amovible 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 administrar el acceso a unos datos digitales distribuidos por un operador, teniendo cada tarjeta un identificador único y comprendiendo unas informaciones relativas a los derechos de acceso de un abonado a dichos datos digitales.

Esta interfaz comprende:

- una memoria no volátil destinada a memorizar una lista de tarjetas de abonados,

- unos medios para verificar si el identificador de una tarjeta asociada a dicha interfaz está presente en la lista memorizada en dicha memoria no volátil.

En un primer ejemplo de realización, la interfaz amovible es una tarjeta PCMCIA (de *Personal Computer Memory Card International Association*) que comprende un programa de desencriptación de datos digitales.

En un segundo ejemplo de realización, la interfaz amovible es un programa ejecutable ya sea en el equipo receptor, ya sea en una tarjeta de control de acceso.

El procedimiento se dirige por medio de un programa de ordenador ejecutable en N equipos receptores susceptibles de ser emparejados con M módulos externos de seguridad que tienen cada uno un identificador único y en los que están almacenadas unas informaciones relativas a los derechos de acceso de un abonado a unos datos digitales distribuidos por un operador, este programa comprende unas instrucciones para memorizar en cada módulo externo de seguridad una lista de identificadores de una parte o del conjunto de los N equipos receptores, y unas instrucciones para memorizar en cada equipo receptor una lista de identificadores de una parte o del conjunto de los M módulos externos de seguridad, unas instrucciones para controlar el identificador de un módulo externo de seguridad conectado a un equipo receptor y el identificador de dicho equipo receptor, y unas instrucciones para prohibir el acceso a dichos datos si el identificador del módulo externo de seguridad conectado al equipo receptor no está presente en la lista de identificadores previamente memorizada en este equipo receptor o si el identificador de dicho equipo receptor no está presente en la lista de identificadores previamente memorizada en dicho módulo externo de seguridad.

Breve descripción de los dibujos

Otras características y ventajas de la invención se desprenderán de la descripción que va a seguir, tomada a título de ejemplo no limitativo en referencia a las figuras adjuntas en las que:

- la figura 1 representa una primera arquitectura de sistema para la puesta en marcha del emparejamiento según la invención,

- la figura 2 representa una segunda arquitectura de sistema para la puesta en marcha del emparejamiento según la invención,

- la figura 3 representa una tercera arquitectura de sistema para la puesta en marcha del emparejamiento según la invención,

- la figura 4 representa la estructura de los mensajes EMM_decodificador de configuración y de utilización de las funcionalidades de emparejamiento según la invención,

- la figura 5 representa la estructura de los mensajes EMM_tarjeta de configuración de las funcionalidades de emparejamiento según la invención,

- la figura 6 es un diagrama funcional que representa esquemáticamente los estados de la función de emparejamiento preinstalada en un equipo receptor,

- la figura 7 representa un organigrama que ilustra un modo particular de puesta en marcha del emparejamiento según la invención.

Exposición detallada de modos de realización particulares

La invención va a describirse ahora en el marco de una aplicación en la que un operador que difunde unos programas audiovisuales pone en marcha el procedimiento según la invención para limitar la utilización de su parque de equipos receptores a sus propios abonados.

El procedimiento puede ser puesto en marcha en tres arquitecturas distintas ilustradas respectivamente por las figuras 1, 2 y 3. Los elementos idénticos en estas tres arquitecturas serán designados por unas referencias idénticas.

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

En la primera arquitectura, ilustrada por la figura 1, el equipo receptor comprende un decodificador 2 en el que se instala un programa 4 de control de acceso, y el módulo externo de seguridad es una tarjeta 6 de control de acceso que comprende unas informaciones relativas a los derechos de acceso de un abonado a los programas audiovisuales difundidos. En este caso, el emparejamiento se realiza entre el decodificador 2 y la tarjeta 6.

En la segunda arquitectura ilustrada por la figura 2, el equipo receptor comprende un decodificador 2, no dedicado al control de acceso, y el módulo externo de seguridad es una interfaz 8 de seguridad amovible provista de una memoria no volátil y en la que se instala el programa 4 de control de acceso. Esta interfaz 8 coopera, por una parte, con dicho decodificador 2 y, por otra parte, con una tarjeta 6 entre una pluralidad de tarjetas de control de acceso condicional, para administrar el acceso a dichos programas audiovisuales.

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

En la tercera arquitectura, ilustrada por la figura 3, el equipo receptor comprende un decodificador 2 en el que se instala un programa 4 de control de acceso y que se conecta a una interfaz 8 de seguridad amovible que tiene una memoria no volátil y destinada a cooperar, por una parte, con dicho decodificador 2 y, por otra parte, con una tarjeta 6 entre una pluralidad de tarjetas de control de acceso condicional.

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

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

La descripción que sigue se refiere a la puesta en práctica de la invención en el caso de emparejamiento de N decodificadores dedicados 2 con M tarjetas 6. Las etapas puestas en marcha se aplican a las tres arquitecturas descritas anteriormente.

A la salida de fábrica de los N decodificadores 2, como después de una telecarga del programa 4 de control de acceso en cada decodificador 2, todos los tratamientos del emparejamiento están inactivos. En particular:

- ningún identificador de tarjeta está memorizado en los decodificadores 2,

- el control por los decodificadores 2 de los identificadores de las tarjetas 6 no está activo,

- el control por los decodificadores 2 de la presencia de su propio identificador en las tarjetas 6 no está activo.

Igualmente, a la salida de fabrica de las M tarjetas 6, ningún identificador de decodificador 2 está memorizado en las tarjetas 6.

El emparejamiento puede entonces ser configurado y utilizado en los N decodificadores 2 y en las M tarjetas 6 por una petición del operador a través de la plataforma 1 de gestión que emite:

- Hacia los N decodificadores 2, mensajes EMM_decodificador dedicados al emparejamiento.

- Hacia las M tarjetas 6, mensajes EMM_tarjeta dedicados al emparejamiento. Estos mensajes EMM_tarjeta son emitidos hacia las tarjetas 6 directamente o integrados en unos mensajes EMM_decodificador.

Los mensajes EMM_decodificador permiten efectuar las siguientes tareas:

- Activar en los N decodificadores 2 la función de emparejamiento. En este caso cada decodificador verifica si el identificador de una tarjeta insertada 6 en el lector de tarjeta del decodificador forma parte de los identificadores que ha memorizado y que el identificador de este decodificador 2 forma parte de los identificadores de decodificadores memorizados en esta tarjeta 6. Si no es el caso, se aplica una perturbación en el acceso a los datos.

- Desactivar en los N decodificadores 2 la función de emparejamiento. En este caso, cada decodificador 2 no controla ni su identificador ni el de la tarjeta.

- Cargar en los N decodificadores 2 la lista de los M identificadores de tarjetas 6 emparejados a estos decodificadores.

- Borrar los identificadores de tarjetas 6 ya memorizados en los N decodificadores 2.

Los mensajes EMM_tarjeta permiten:

- Cargar en las M tarjetas 6 la lista de N identificadores de decodificadores 2 emparejados a estas tarjetas.

- Borrar los identificadores de los decodificadores 2 ya memorizados en las M tarjetas 6.

Direccionamiento de los mensajes EMM

Los mensajes EMM que permiten la configuración y la utilización de las funcionalidades unidas al emparejamiento según el procedimiento de la invención se emiten en una vía EMM de un múltiplexor digital tal como se define por el estándar MPEG2/Sistema y estándares DVB/ETSI.

Esta vía puede difundir unos EMM que hacen referencia a una dirección de tarjeta/s que permite destinarlos directamente:

- a una tarjeta particular,

- a las tarjetas de un grupo particular,

- a todas las tarjetas.

Esta vía puede difundir igualmente unos EMM que hacen referencia a una dirección de decodificador/es que permite destinarlos directamente:

- a un decodificador particular,

- a un grupo particular de decodificadores,

- a todos los decodificadores.

Los mensajes destinados a una tarjeta particular o a un decodificador particular son unos EMM-U que presentan la siguiente estructura:

```
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_lenght                     12 bits
unique_adress_field                      40 bits
for (i=0; i<N; i++) {
     EMM_data_byte                       8 bits
     }
}
```

El parámetro unique_address_field es la dirección única de una tarjeta en un EMM-U de tarjeta o la dirección única de un decodificador en un EMM-U de decodificador.

Los mensajes destinados a unas tarjetas de un grupo particular de tarjetas o a unos decodificadores de un grupo particular de decodificadores son unos EMM-S que presentan la siguiente estructura:

```
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_lenght                     12 bits
shared_address_field                     24 bits
Reserved                                 6 bits
data_format                              1 bit
ADF_scrambling_flag                      1 bit
for (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 de tarjeta o la dirección del grupo de decodificadores en un EMM-S de decodificador. Se hace referencia a un decodificador de un grupo o una tarjeta de un grupo por medio del mensaje si además es explícitamente designado en un campo ADF contenido en EMM_data_byte y que puede ser cifrado según la información ADF_scrambling_flag.

Los mensajes destinados a todas las tarjetas o a todos los decodificadores son unos EMM-G que presentan la siguiente estructura:

```
table_id = 0x8A ó 0x8B                  8 bits
section_syntax_indicator = 0            1 bit
DVB_reserved                            1 bit
ISO_reserved                            2 bits
EMM-G_section_lenght                    12 bits
for (i=0; i<N; i++) {
      EMM_data_byte                     8 bits
      }
}
```

Contenido de los mensajes EMM_decodificador

La figura 4 ilustra esquemáticamente el contenido de los datos EMM_data_byte de un mensaje EMM_decodificador de emparejamiento. Este contenido depende de la función a ejecutar por un decodificador 2 para la configuración o utilización del emparejamiento.

Los datos EMM_data_byte incluyen los siguientes parámetros funcionales:

- ADF 20: complemento de dirección de un decodificador en un grupo de decodificadores; este parámetro es útil en caso de direccionamiento por grupo si no puede ser omitido; puede ser cifrado;

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

- OPID/NID 24: identificación del parque de decodificadores y de la señal del operador;

- TIME 26: datos de sellado de tiempo de la emisión del mensaje; este parámetro se utiliza para evitar la repetición del mensaje por un mismo decodificador;

- CRYPTO 28: identificación de las funciones de protección criptográfica aplicadas a los parámetros FUNCTIONS 32; los parámetros FUNCTIONS pueden ser cifrados y protegidos por una redundancia criptográfica 30;

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

- STBID 34: dirección única del decodificador concernido por el mensaje. Este parámetro está presente en un EMM-U de decodificador, si no puede ser omitido.

Los parámetros funcionales anteriores son organizados libremente en los datos EMM_data_byte de un mensaje EMM_codificador. Una implementación preferida es la combinación de estos parámetros por estructura TLV (tipo-longitud-valor).

Contenido de los mensajes EMM_tarjeta

La figura 5 ilustra esquemáticamente el contenido de los datos EMM_data_byte de un mensaje EMM_tarjeta de emparejamiento. Este contenido permite inscribir, modificar o borrar una lista de los identificadores de terminales.

Los datos EMM_data_byte incluyen los siguientes parámetros funcionales:

- SOID 40: identificación del operador;

- ADF 42: complemento de direccionamiento de una tarjeta en un grupo de tarjetas; este parámetro es útil en caso de direccionamiento por grupo, si no, puede ser omitido; puede ser cifrado;

- CRYPTO 44: identificación de las funciones de protección criptográfica aplicadas al parámetro LDA 48 y a los otros parámetros 50; los parámetros 48 y 50 pueden ser cifrados y protegidos por una redundancia criptográfica 46.

- LDA 48 (Lista de decodificadores autorizados): este parámetro contiene la lista de los identificadores de decodificadores con los que la tarjeta puede funcionar.

Los datos EMM_data_byte pueden además contener otros parámetros 50 que se refieren a otras funciones de la tarjeta que el emparejamiento.

Los parámetros presentes en los datos EMM_data_byte son organizados libremente en estos datos de un mensaje EMM_tarjeta. Una implementación preferida es la combinación de estos parámetros por estructura TLV (tipo-longitud-valor).

Configuración y utilización del emparejamiento

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

- MODE: este parámetro activa, desactiva o reinicializa la solución de emparejamiento según la invención. Después de la desactivación, el decodificador no controla el identificador de una tarjeta insertada pero conserva la lista de los identificadores memorizados. Después de la reinicialización, el decodificador no controla el identificador de una tarjeta insertada y ya no tiene identificadores de tarjetas memorizados.

- LCA (Lista de tarjetas autorizadas): este parámetro carga en un decodificador la lista de los identificadores de tarjetas con los que puede funcionar;

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

- Fecha/Plazo: este parámetro caracteriza la fecha o el plazo de activación o de desactivación del emparejamiento.

Los parámetros funcionales anteriores son organizados libremente en el conjunto de parámetros FUNCTIONS 32. Una implementación preferida es la combinación de estos parámetros por estructura TLV (tipo-longitud-valor).

Además, en ciertos tipos de servicio tales como una forma de emparejamiento de un decodificador con una tarjeta, un EMM_decodificador puede transportar uno o varios EMM_tarjeta. En este caso, el EMM_tarjeta (los EMM_tarjeta) está/n incluido/s en el conjunto de parámetros FUNCTIONS 32 de forma claramente identificable por el decodificador que podrá extraer y suministrar a la tarjeta insertada el/los EMM_tarjeta. Una implementación preferida de inclusión de EMM_tarjeta en el conjunto de parámetros FUNCTIONS 32 de un EMM_decodificador es el uso de una estructura TLV particular que contiene el/los EMM_tarjeta con todos los datos de direccionamiento correspondientes.

Otra utilización de EMM_tarjeta en un EMM_decodificador permite memorizar en la tarjeta que este EMM_decodificador ya ha sido tratado por el decodificador, con el fin de evitar la repetición en otro decodificador y permitiendo el tratamiento único de este EMM por un solo decodificador; semánticamente estos datos significan “ya tratado” y son verificados por el programa 4 de control de acceso del decodificador 2 cuando trata este EMM. Una realización preferida de este mecanismo antirepetición es la inscripción de estos datos en un bloque de datos FAC (*Facilities Data Block* en inglés) de la tarjeta.

Funcionamiento

El funcionamiento del emparejamiento según la invención va a ser descrito ahora en referencia a las figuras 6 y 7.

La figura 6 es un diagrama funcional que ilustra esquemáticamente los estados de la función de emparejamiento del programa 4 de control de acceso preinstalado en un decodificador 2.

La función de emparejamiento está en estado inactivo 60 cuando el programa 4 de control de acceso acaba de ser instalado o telecargado 61 o cuando ha recibido de la plataforma 1 de gestión una orden de desactivación del emparejamiento 62 o de reinicialización del emparejamiento 64. En este estado el programa 4 de control de acceso acepta funcionar con una tarjeta insertada 6 en el decodificador 2 sin verificar su emparejamiento con esta tarjeta.

Para efectuar la activación del emparejamiento entre M decodificadores 2 y N tarjetas 6, el operador activa a través de la plataforma 1 de gestión:

- un tratamiento 70 para definir el modo de emparejamiento (=activo), y el tipo de perturbación aplicable en el acceso a los datos en caso de fracaso del emparejamiento,

- un tratamiento 72 para definir la lista LCA a cargar en estos N decodificadores de los identificadores de las M tarjetas autorizadas,

- un tratamiento 74 para definir la lista LDA para cargar en estas M tarjetas unos identificadores de los N decodificadores autorizados.

En función de estas informaciones la plataforma 1 de gestión genera y emite (flecha 76):

- al menos un mensaje EMM_decodificador para cargar en la memoria no volátil de los N decodificadores 2 la lista LCA de las tarjetas autorizadas 6,

- al menos un mensaje EMM_tarjeta para cargar en la memoria no volátil de las M tarjetas 6 la lista LDA de los decodificadores autorizados,

- al menos un mensaje EMM_decodificador para cargar los parámetros de configuración en la memoria no volátil de los N decodificadores 2.

La función de emparejamiento en un decodificador 2 pasa al estado activo 78.

Durante una activación de la función de emparejamiento en un decodificador 2 con carga de la lista LCA de las tarjetas autorizadas 6 y/o de la lista LDA de los decodificadores autorizados 2, la consideración efectiva por un decodificador 2 de los parámetros de configuración puede ser diferida en el tiempo según el parámetro Fecha/Plazo para garantizar la carga efectiva de la lista LCA de las tarjetas autorizadas 6 en un decodificador 2 y de la lista LDA de los decodificadores autorizados 2 en una tarjeta 6.

Durante una reactivación de la función de emparejamiento en un decodificador 2, si la lista LCA de las tarjetas autorizadas 6 y/o la lista LDA de los decodificadores autorizados 2 no necesita modificación, los EMM correspondientes no son ni generados ni emitidos.

El operador puede desactivar (etapa 80) el emparejamiento en un decodificador 2, a partir de la plataforma 1 de gestión que genera y emite (flecha 82) un mensaje EMM que direcciona el o los decodificadores 2 concernidos y que contiene una orden de desactivación sin borrado del contexto del emparejamiento 62 o una orden de RAZ del contexto de emparejamiento 64.

La función de emparejamiento en un decodificador 2 pasa al estado inactivo 60.

La consideración efectiva por un decodificador 2 de la orden de desactivación puede ser diferida en el tiempo según el parámetro Fecha/Plazo.

Sea cual sea el estado inactivo 60 o activo 78 de la función de emparejamiento, puede recibir de la plataforma 1 de gestión una lista de tarjetas autorizadas 6 LCA por decodificador de EMM (etapa 72) o una lista de decodificadores autorizados 2 LDA (etapa 74).

La consideración de una de las M tarjetas 6 por la función de emparejamiento de uno de los N decodificadores 2 se describe en el organigrama de la figura 7.

En la inserción (etapa 100) de una tarjeta 6 en el decodificador 2, el programa 4 de control de acceso preinstalado en el decodificador prueba (etapa 102) si la función de emparejamiento está en el estado activo 78.

Si la función de emparejamiento en el decodificador está en el estado inactivo 60, el decodificador acepta funcionar con la tarjeta insertada (108).

Si la función de emparejamiento en el decodificador está en el estado activo 78, el programa de control de acceso:

- enciende el identificador de la tarjeta insertada y verifica (etapa 104) si este identificador está en la lista de las tarjetas autorizadas 6 memorizadas en el decodificador 2,

- enciende en la tarjeta insertada la lista de los decodificadores autorizados y verifica (etapa 106) si el identificador del decodificador 2 está presente en esta lista.

Las pruebas 104 y 106 pueden ser ejecutadas sin que importe el orden.

Si los resultados de estas dos pruebas 104 y 106 de identificadores son positivos, el programa 4 de control de acceso acepta funcionar con la tarjeta insertada 6 (etapa 108). Entonces es posible el acceso a los programas difundidos, bajo reserva de conformidad de las otras condiciones de acceso unidas a estos programas.

Si el resultado de al menos una de las pruebas 104 y 106 no es positivo, el programa 4 de control de acceso rechaza funcionar con la tarjeta insertada 6 y aplica (etapa 110) la perturbación en el acceso a los datos tal como se define por el operador. Tal perturbación puede consistir en bloquear el acceso a los programas difundidos. Puede ser acompañada de la presentación visual en la pantalla del terminal al que está asociado el decodificador de un mensaje que invita al abonado a insertar otra tarjeta 6 en el decodificador 2.

Cuando se extrae la tarjeta 2 (etapa 112) del decodificador 2, el programa de control de acceso pasa a estar en espera de la inserción de una tarjeta (etapa 100).

La perturbación aplicada a la etapa 110 en el acceso a los datos en caso de fallo de emparejamiento puede ser de diferente naturaleza tal como:

- interrupción del audio y vídeo en las cadenas cifradas (obtenido por no sumisión de los EMC en la tarjeta para cálculo de los CW);

- interrupción del audio y vídeo en las cadenas en abierto y analógicas (obtenido por mensaje al middleware);

- envío de un mensaje al middleware del terminal (ejemplo: mensaje Open TV).

Esta perturbación puede ser utilizada igualmente para provocar el bloqueo de decodificadores robados.

En el caso descrito en la figura 2 en el que el programa 4 de control de acceso se ejecuta en la interfaz amovible 8 conectada a un decodificador 2, el autómata descrito en la figura 4 y el organigrama descrito en la figura 5 se aplican directamente al programa 4 de control de acceso preinstalado en esta interfaz amovible 8.

REIVINDICACIONES

1. Procedimiento de emparejamiento de un número N de equipos receptores (2) de datos con un número M de módulos externos (6, 8) de seguridad, estando provisto cada equipo receptor (2) de un identificador único, y teniendo cada módulo externo (6, 8) de seguridad un identificador único, procedimiento **caracterizado** porque comprende una fase de configuración que comprende las siguientes etapas:

- memorizar en cada módulo externo (6, 8) de seguridad una lista de identificadores de equipos receptores (2),

- memorizar en cada equipo receptor (2) una lista de identificadores de módulos externos (6, 8) de seguridad,

y una fase de control que consiste en autorizar el acceso a los datos si el identificador de un módulo externo (6, 8) de seguridad conectado a un equipo receptor (2) está presente en la lista memorizada en este equipo receptor (2), y si el identificador de dicho equipo receptor (2) está presente en la lista memorizada en dicho módulo externo (6, 8) de seguridad, si no, perturbar el acceso a dichos datos.

2. Procedimiento según la reivindicación 1, **caracterizado** porque la configuración se pone en marcha únicamente cuando el usuario conecta un módulo externo (6, 8) de seguridad a un equipo receptor (2).

3. Procedimiento según la reivindicación 1, **caracterizado** porque comprende además una etapa en la que el operador transmite al equipo receptor (2), una señalización para administrar la fase de control que comprende al menos una de las siguientes consignas:

- activar la fase de control en una fecha o después de un plazo programados,

- desactivar la fase de control en una fecha o después de un plazo programados,

- especificar una fecha absoluta (respectivamente un plazo) a partir de la cual (respectivamente al cabo del cual) se inicia la activación o la desactivación de la fase de control,

- anular dicha fecha programada (respectivamente dicho plazo programado).

4. Procedimiento según la reivindicación 1, **caracterizado** porque el operador transmite además al equipo receptor (2) una señalización que comprende un mensaje de supresión de la lista de los identificadores memorizados en el equipo receptor (2).

5. Procedimiento según la reivindicación 1, **caracterizado** porque el operador transmite además al módulo externo (6, 8) de seguridad una señalización que comprende un mensaje de supresión de la lista de los identificadores memorizados en este módulo externo (6, 8) de seguridad.

6. Procedimiento según la reivindicación 1, **caracterizado** porque el operador transmite a un equipo receptor (2) la lista de los M identificadores de los módulos externos (6, 8) de seguridad a través de un mensaje EMM específico a dicho equipo receptor (2).

7. Procedimiento según la reivindicación 1, **caracterizado** porque el operador transmite a un módulo externo (6, 8) de seguridad la lista de los N identificadores de equipos receptores (2) a través de un mensaje EMM específico a dicho módulo externo (6, 8) de seguridad.

8. Procedimiento según la reivindicación 1, **caracterizado** porque el operador transmite a un grupo de equipos receptores (2) la lista de los M identificadores de módulos externos (6, 8) de seguridad a través de un mensaje EMM específico a dicho grupo de equipos receptores (2).

9. Procedimiento según la reivindicación 1, **caracterizado** porque el operador transmite a un grupo de módulos externos (6, 8) de seguridad la lista de los N identificadores de equipos receptores (2) a través de un mensaje EMM específico a dicho grupo de módulos externos (6, 8) de seguridad.

10. Procedimiento según las reivindicaciones 3 ó 4, **caracterizado** porque el operador suministra a un equipo receptor (2) dicho mensaje de señalización a través de un mensaje EMM específico a dicho equipo receptor (2).

11. Procedimiento según las reivindicaciones 3 ó 4, **caracterizado** porque el operador suministra a un grupo de equipos receptores (2) dicho mensaje de señalización a través de un mensaje EMM específico a dicho grupo de equipos receptores (2).

12. Procedimiento según la reivindicación 5, **caracterizado** porque el operador suministra a un módulo externo de seguridad dicho mensaje de señalización a través de un mensaje EMM específico a dicho módulo externo (2) de seguridad.

13. Procedimiento según la reivindicación 5, **caracterizado** porque el operador suministra a un grupo de módulos externos (6, 8) de seguridad dicho mensaje de señalización a través de un mensaje EMM específico a dicho grupo de módulos externos (6, 8) de seguridad.

14. Procedimiento según las reivindicaciones 3 ó 4, **caracterizado** porque el operador transmite a un grupo de equipos receptores (2) en un flujo privado un mensaje de señalización para la fase de control, siendo tratado dicho flujo privado por un programa dedicado ejecutable en cada equipo receptor (2) en función del identificador de dicho equipo receptor (2).

15. Procedimiento según la reivindicación 1, **caracterizado** porque la lista de identificadores de módulos externos (6, 8) de seguridad se transmite en un flujo privado a un grupo de equipos receptores (2) y tratada por un programa dedicado ejecutable en cada equipo receptor (2) en función del identificador de dicho equipo receptor (2).

16. Procedimiento según la reivindicación 1, **caracterizado** porque la lista de identificadores de equipos receptores (2) se transmite a un grupo de módulos externos (6, 8) de seguridad en un flujo privado que se trata por medio un programa dedicado ejecutable en cada uno de dichos módulos externos (6, 8) de seguridad o en el equipo receptor (2) al que está conectado cada uno de dichos módulos externos (6, 8) de seguridad, en función del identificador de dicho módulo externo (6, 8) de seguridad.

17. Procedimiento según la reivindicación 1, **caracterizado** porque los datos digitales se distribuyen en abierto o en forma encriptada.

18. Procedimiento según la reivindicación 17, **caracterizado** porque los datos digitales representan unos programas audiovisuales.

19. Procedimiento según la reivindicación 1, **caracterizado** porque la lista de los identificadores de los M módulos de seguridad memorizados en un equipo receptor (2) está cifrada.

20. Procedimiento según la reivindicación 1, **caracterizado** porque la lista de los identificadores de los N equipos receptores (2) memorizados en un módulo externo (6, 8) de seguridad está cifrada.

21. Procedimiento según una de las reivindicaciones 6 a 13, **caracterizado** porque comprende además un mecanismo destinado a impedir la utilización de un EMM transmitido a un mismo módulo externo (6, 8) de seguridad o a un mismo equipo receptor (2).

22. Procedimiento según las reivindicaciones 6, 7, 10 ó 12, **caracterizado** porque dicho EMM presenta el siguiente formato:

```
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_lenght                     12 bits
unique_adress_field                      40 bits
for (i=0; i<N; i++) {
     EMM_data_byte                       8 bits
     }
}
```

23. Procedimiento según las reivindicaciones 8, 9, 11 ó 13, **caracterizado** porque dicho mensaje EMM se refiere a todos los módulos externos (6, 8) de seguridad o todos los equipos receptores (2) y presenta el siguiente formato:

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

24. Procedimiento según las reivindicaciones 8, 9, 11 ó 13, **caracterizado** porque dicho mensaje EMM es específico a un subgrupo de módulos externos (6, 8) de seguridad o un subgrupo de equipos receptores (2) y presenta 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_lenght                    12 bits
shared_address_field                    24 bits
Reserved                                6 bits
data_format                             1 bit
ADF_scrambling_flag                     1 bit
for (i=0; i<N; i++) {
      EMM_data_byte                     8 bits
      }
}
```

25. Procedimiento según una cualquiera de las reivindicaciones 1 a 24, **caracterizado** porque el equipo receptor (2) comprende un decodificador y el módulo (6, 8) de seguridad externo comprende una tarjeta (6) de control de acceso en la que están memorizadas unas informaciones relativas a los derechos de acceso de un abonado a unos datos digitales distribuidos por un operador, y porque el emparejamiento se efectúa entre dicho decodificador y dicha tarjeta (6).

26. Procedimiento de una cualquiera de las reivindicaciones 1 a 24, **caracterizado** porque el equipo receptor (2) comprende un decodificador y el módulo externo (6, 8) de seguridad comprende una interfaz (8) de seguridad amovible provista de una memoria no volátil y destinada a cooperar, por una parte, con el decodificador y, por otra parte, con una

pluralidad de tarjetas (6) de control de acceso condicional para administrar el acceso a unos datos digitales distribuidos por un operador, y porque el emparejamiento se efectúa entre dicho decodificador y dicha interfaz (8) de seguridad amovible.

27. Procedimiento de una cualquiera de las reivindicaciones 1 a 24, **caracterizado** porque el equipo receptor (2) comprende un decodificador provisto de una interfaz (8) de seguridad amovible que tiene una memoria no volátil y destinada a cooperar, por una parte, con dicho decodificador y, por otra parte, con una pluralidad de tarjetas (6) de control de acceso condicional, y porque el emparejamiento se realiza entre dicha interfaz (8) de seguridad amovible y dichas tarjetas (6) de control de acceso.

28. Equipo receptor susceptible de ser emparejado con una pluralidad de módulos externos (6, 8) de seguridad para administrar el acceso a unos datos digitales distribuidos por un operador, **caracterizado** porque comprende:

- una memoria no volátil destinada a memorizar una lista de módulos externos (6, 8) de seguridad,

- unos medios para verificar si el identificador de un módulo externo (6, 8) de seguridad conectado a dicho equipo está presente en la lista memorizada en dicha memoria no volátil.

29. Equipo según la reivindicación 28, **caracterizado** porque comprende un decodificador y porque el módulo externo (6, 8) de seguridad es una tarjeta (6) de control de acceso que comprende unas informaciones relativas a los derechos de acceso de un abonado a dichos datos digitales, efectuándose el emparejamiento entre dicho decodificador y dicha tarjeta (6).

30. Equipo según la reivindicación 28, **caracterizado** porque comprende un decodificador y porque el módulo externo (6, 8) de seguridad es una interfaz (8) de seguridad amovible provista de una memoria no volátil y destinada a cooperar, por una parte, con dicho decodificador y, por otra parte, con una pluralidad de tarjetas (6) de control de acceso condicional, para administrar el acceso a dichos datos digitales, siendo efectuado el emparejamiento entre dicho decodificador y dicha interfaz (8) de seguridad amovible.

31. Equipo según la reivindicación 28, **caracterizado** porque comprende un decodificador provisto de una interfaz (8) de seguridad amovible que tiene una memoria no volátil y destinada a cooperar, por una parte, con dicho decodificador y, por otra parte, con una pluralidad de tarjetas (6) de control de acceso condicional, y porque el emparejamiento se realiza entre dicha interfaz (8) de seguridad amovible y dichas tarjetas (6) de control de acceso.

32. Decodificador susceptible de cooperar con una pluralidad de módulos externos (6, 8) de seguridad para administrar el acceso a unos programas audiovisuales distribuidos por un operador, teniendo cada módulo externo (6, 8) de seguridad un identificador único y comprendiendo al menos un algoritmo de tratamiento de datos, decodificador **caracterizado** porque comprende:

- una memoria no volátil destinada a memorizar una lista de módulos externos (6, 8) de seguridad,

- unos medios para verificar si el identificador de un módulo externo (6, 8) de seguridad conectado a dicho decodificador está presente en la lista memorizada en dicha memoria no volátil.

33. Decodificador según la reivindicación 32, **caracterizado** porque dichos módulos externos (6, 8) de seguridad son unas tarjetas (6) de control de acceso en las que están memorizadas unas informaciones relativas a los derechos de acceso de un abonado a unos datos digitales, distribuidas por un operador.

34. Decodificador según la reivindicación 32, **caracterizado** porque dichos módulos externos (6, 8) de seguridad son unas interfaces (8) de seguridad amovibles que comprenden una memoria no volátil y están destinadas a cooperar, por una parte, con el decodificador y, por otra parte, con una pluralidad de tarjetas (6) de control de acceso condicional para administrar el acceso a unos datos digitales distribuidos por un operador.

35. Interfaz de seguridad amovible destinada a cooperar, por una parte, con un equipo receptor (2) y, por otra parte, con una pluralidad de tarjetas (6) de control de acceso condicional, para administrar el acceso a unos datos digitales distribuidos por un operador, teniendo cada tarjeta un identificador único y comprendiendo unas informaciones relativas a los derechos de acceso de un abonado a dichos datos digitales, interfaz **caracterizada** porque comprende:

- una memoria no volátil destinada a memorizar una lista de tarjetas de abonados,

- unos medios para verificar si el identificador de una tarjeta asociada a dicha interfaz está presente en la lista memorizada en dicha memoria no volátil.

36. Interfaz según la reivindicación 35, **caracterizada** porque consiste en una tarjeta PCMCIA que comprende un programa de desencriptación de datos digitales.

37. Interfaz según la reivindicación 35, **caracterizada** porque consiste en un programa.

38. Sistema de control de acceso que comprende una pluralidad de equipos receptores (2) que tienen cada uno un identificador único y son susceptibles de cooperar con una pluralidad de módulos externos (6, 8) de seguridad que tienen cada uno un identificador único, comprendiendo cada módulo externo (6, 8) de seguridad unas informaciones relativas a los derechos de acceso de un abonado a unos datos digitales distribuidos por un operador, comprendiendo dicho sistema igualmente una plataforma (1) de gestión comercial que comunica con dichos equipos receptores (2) y con dichos módulos externos (6, 8) de seguridad, **caracterizado** porque comprende además:

- un primer módulo dispuesto en dicha plataforma comercial (1) y destinado a generar unas peticiones de emparejamiento,

- y un segundo módulo dispuesto en dichos equipos receptores (2) y en dichos módulos externos (6, 8) de seguridad y destinado a tratar dichas peticiones para preparar una configuración del emparejamiento.

39. Programa de ordenador ejecutable en N equipos receptores (2) susceptibles de cooperar con M módulos (6, 8) de seguridad que tienen cada uno un identificador único y en los que están almacenadas unas informaciones relativas a los derechos de acceso de un abonado a unos datos digitales distribuidos por un operador, **caracterizado** porque comprende unas instrucciones para memorizar en cada módulo externo (6, 8) de seguridad una lista de identificadores de un parte o del conjunto de los N equipos receptores (2), y unas instrucciones para memorizar en cada equipo receptor (2) una lista de identificadores de una parte o del conjunto de los M módulos (6, 8) de seguridad, unas instrucciones para controlar el identificador de un módulo de seguridad conectado a un equipo receptor (2) y el identificador de dicho equipo receptor (2), y unas instrucciones para prohibir el acceso a dichos datos si el identificador del módulo (6, 8) de seguridad conectado al equipo receptor (2) no está presente en la lista de identificadores previamente memorizada en este equipo receptor (2) o si el identificador de dicho equipo receptor (2) no está presente en la lista de identificadores previamente memorizada en dicho módulo externo (6, 8) de seguridad.

Fig.1

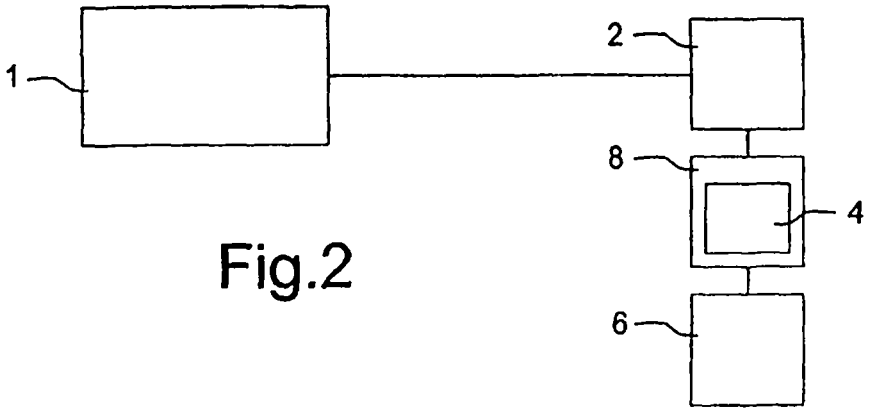

Fig.2

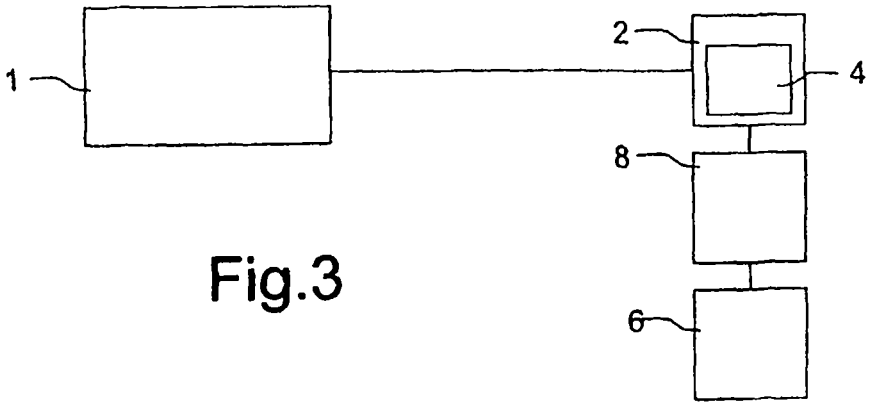

Fig.3

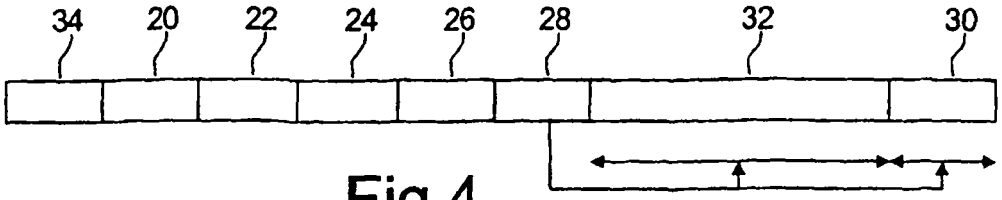

Fig.4

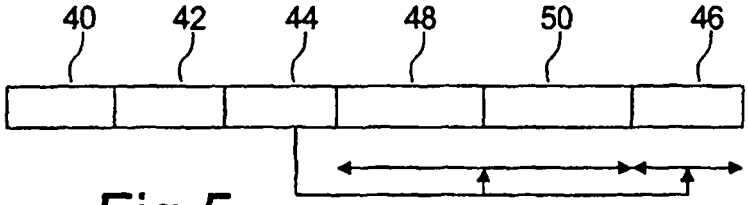

Fig.5

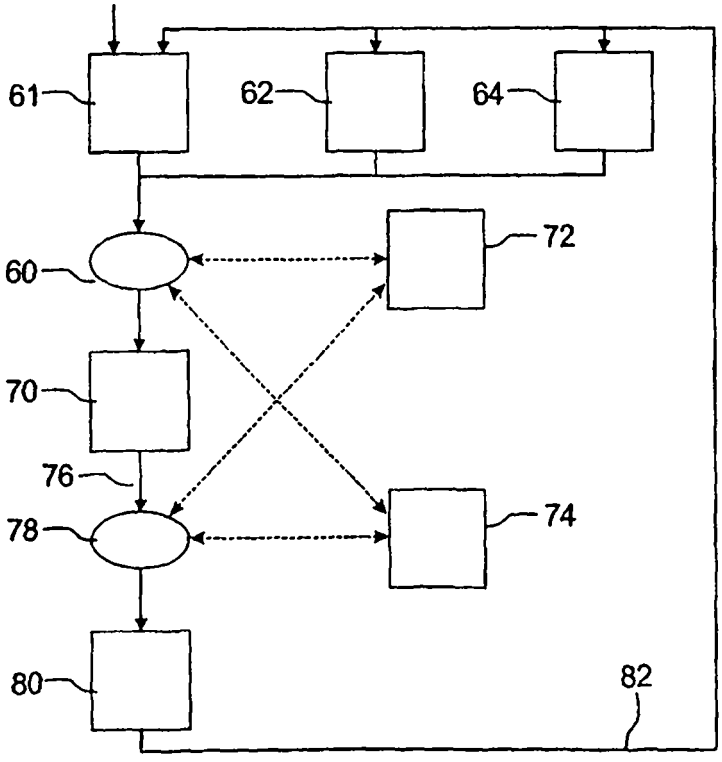

Fig.6

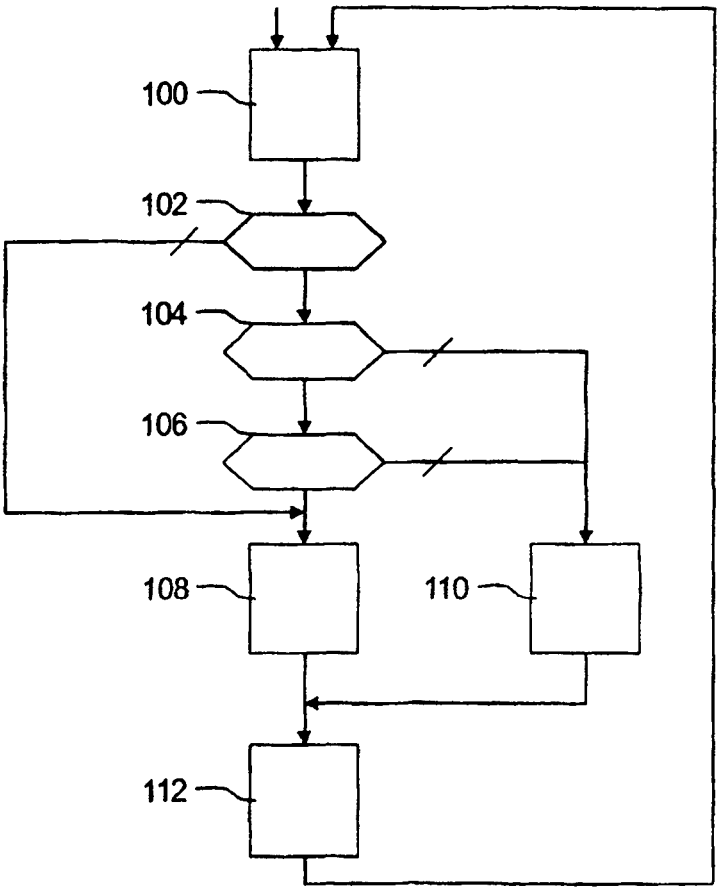

Fig.7