(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 721 879**

(51) Int. CI.:

H04L 9/08 (2006.01)
G11B 20/00 (2006.01)
H04N 7/167 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.03.2012 E 12157612 (8)**

(97) Fecha y número de publicación de la concesión europea: **20.02.2019 EP 2495906**

(54) Título: **Procedimiento de protección de un contenido multimedia registrado en una red doméstica**

(30) Prioridad:

02.03.2011 FR 1151708

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.08.2019

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche Tour Opéra C
92057 Paris La Défense, FR

(72) Inventor/es:

BOIVIN, MATHIEU;
LAFRANCHI, STÉPHANE y
POCHON, NICOLAS

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento de protección de un contenido multimedia registrado en una red doméstica

La invención se refiere a un procedimiento de protección de un contenido multimedia registrado. La invención tiene igualmente por objeto un procedimiento de transmisión y un procedimiento de registro de un contenido multimedia para la realización del procedimiento de protección. La invención tiene también por objeto un registrador y/o un lector, una cabecera de red y un soporte de registro de informaciones.

El codificado de los contenidos multimedia permite someter el descodificado de estos contenidos multimedia a la adquisición, mediante pago, de un título de acceso cuya validez es comprobada en cada acceso a los contenidos multimedia.

En este contexto, es igualmente necesario proteger los contenidos multimedia transmitidos en forma codificada y luego registrados. En efecto, si se deja la posibilidad de registrar el contenido multimedia sin protección en lectura, entonces éste puede ser indefinidamente reutilizado (releído) por el poseedor de los derechos, y libremente puesto a disposición, y utilizable (leíble) por, otros usuarios que no han adquirido los títulos de acceso requeridos para visualizar el contenido multimedia. Ahora bien, hoy en día, es muy fácil difundir un contenido multimedia registrado a un gran número de personas, particularmente por mediación de redes de partición. Por ejemplo, una red de partición es una red estación a estación más conocida bajo el término inglés de red «peer to peer». En otra alternativa, la partición se realiza utilizando servidores hospedados.

Por consiguiente ya ha sido propuesto registrar contenidos multimedia en forma codificada. Así, el solicitante conoce un procedimiento de protección de un contenido multimedia registrado en el cual:

- una cabecera de red transmite un contenido multimedia codificado y mensajes ECM (Entitlement Control Message) conteniendo criptogramas CW^* de palabras de control CW que permiten cada una descodificar un criptoperiodo respectivo del contenido multimedia codificado,
- un registrador recibe el contenido multimedia codificado y los mensajes ECM, descifra los criptogramas CW^* contenidos en los mensajes ECM recibidos con una clave de abonado K_a y protege en lectura el contenido multimedia codificado con la ayuda de una clave local KH_k cifrando, con la clave local KH_k, las palabras de control descifradas para generar criptogramas CW^{KHk},
- el registrador registra el contenido multimedia codificado y los criptogramas CW^{KHk}.

El solicitante conoce igualmente un procedimiento de protección de un contenido multimedia registrado similar salvo que el registrador protege en lectura el contenido multimedia codificado con la ayuda de una clave local KH_k descodificando el contenido multimedia con las palabras de control descifradas y luego codificando de nuevo el contenido multimedia con al menos una palabra de control CW' y en general un criptograma CW'^{KHk} correspondiente a la palabra de control CW' cifrada con la clave local KH_K.

En la mayoría de los casos, el registrador está implementado en un terminal en el interior del cual está igualmente implementado un lector que permite leer o jugar, en claro, el contenido multimedia registrado.

Por «en claro», se designa el hecho que el contenido multimedia leído es directamente perceptible y comprensible por un ser humano. Dicho de otro modo, el contenido multimedia en claro es el resultado de un descodificado correcto del contenido multimedia codificado.

En estos procedimientos conocidos, la clave local KH_k es generada localmente por el terminal y mantenida secreta en un procesador de seguridad. Así, solo el lector de este terminal puede jugar en claro el contenido multimedia registrado protegido por medio de esta clave. Esto es una buena solución para impedir la partición del contenido multimedia registrado en las redes de partición. Sin embargo, esta solución presenta igualmente inconvenientes.

En efecto, hoy en día, es cada vez más frecuente que un usuario tenga en su hogar varios terminales para descodificar contenidos multimedia recibidos. Ahora bien, con la solución conocida, el contenido multimedia registrado por uno de estos terminales no puede ser leído por otro terminal del mismo hogar incluso si este tiene los títulos de acceso requeridos. Dicho de otro modo, no es posible particionar el contenido multimedia registrado entre los diferentes terminales de un mismo hogar. En efecto, el otro terminal no conoce la clave local KH utilizada para proteger el contenido multimedia registrado.

El estado de la técnica es igualmente conocido por los documentos:

- EP 1 672 831 A1,
- WO 2004/017635 A1,
- EP 1 383 327 A2,
- EP 1 662 788 A1,

- US2009/067622 A1.

La invención trata de remediar este inconveniente impidiendo la partición sin ninguna restricción del contenido multimedia registrado por medio de redes de partición.

La invención tiene por consiguiente por objeto un procedimiento de protección de un contenido multimedia registrado conforme a la reivindicación 1 o 2.

En el procedimiento indicado más arriba, la clave local KH_k es solamente transmitida a los M lectores asociados con el identificador de hogar. Así, solo estos M lectores son capaces de descifrar los criptogramas CW^{KHk} o CW'^{KHk}. Dicho de otro modo, solo los lectores de este grupo son capaces de descifrar el contenido multimedia registrado por el registrador cuando han recibido la clave local KH_k. Por lo tanto, la partición del contenido multimedia registrado entre estos M lectores de este grupo es posible.

Por el contrario, la partición del contenido multimedia registrado con un lector que no pertenece a este grupo se hace imposible. En efecto, un lector que no pertenece a este grupo no recibe la clave KH_k de modo que no puede leer en claro el contenido multimedia registrado.

Así, la partición de un contenido multimedia registrado en un mismo hogar está permitida sin hacer por ello posible una partición sin restricción de este contenido multimedia registrado en redes de partición tales como las redes “peer to peer”.

Por último, transmitir los criptogramas KH_k^{Ki} a los diferentes lectores únicamente cuando este lector solicita la lectura de un contenido multimedia aumenta la seguridad del procedimiento. En efecto, la clave KH_k solo es transmitida a los lectores en el momento en que esta se hace necesaria para leer un contenido multimedia. La misma no está por consiguiente sistemáticamente contenida en cada uno de los lectores del grupo de M lectores del hogar. Eso limita la exposición de la clave KH_k a las tentativas de utilización fraudulenta de esta clave. Además, el criptograma KH_k^{Ki} solo es descifrable por el $i^{-ésimo}$ lector. Así, la intercepción de este criptograma en la red local del hogar no cuestiona la seguridad del procedimiento. En efecto, la clave K_i no es conocida por ninguno de los otros lectores e incluso por el registrador.

Los modos de realización de este procedimiento de protección pueden comprender una o varias de las características de las reivindicaciones dependientes.

Estos modos de realización presentan además las ventajas siguientes:

- la utilización de dos claves locales KH_k y $KH"_k$, así como de un indicador de modo de protección permite limitar la lectura del contenido multimedia registrado en los únicos P lectores del grupo de M lectores que propone un mejor nivel de seguridad;
- la presencia del indicador del modo de protección en el interior del mensaje ECM permite modificar el modo de protección a aplicar en función del contenido multimedia recibido;
- la transmisión de una nueva clave local KH_{k+1} en respuesta a la supresión de un lector del grupo de M lectores permite excluir este lector del grupo a partir de la fecha de esta transmisión;
- la transmisión de una nueva clave local KH_{k+1} en respuesta al aporte de un lector al grupo de M lectores permite incluir este lector al grupo a partir de la fecha de esta transmisión;
- la memorización por los lectores de las diferentes claves locales KH_k recibidas asociadas con su índice k respectivo permite a estos lectores continuar jugando contenidos multimedia registrados antes de la transmisión de una nueva clave KH_{k+1}.

La invención tiene igualmente por objeto un procedimiento de transmisión de un contenido multimedia, conforme a la reivindicación 7, para la realización del procedimiento de protección anteriormente indicado.

La invención tiene igualmente por objeto un procedimiento, conforme a la reivindicación 8, de registro de contenidos multimedia transmitidos según el procedimiento de transmisión anteriormente indicado.

Los modos de realización de este procedimiento de registro pueden comprender las características de una o varias de las reivindicaciones dependientes.

La invención tiene igualmente por objeto un registrados y/o lector conforme a la reivindicación 11.

La invención tiene igualmente por objeto una cabecera de red conforme a la reivindicación 12.

La invención tiene igualmente por objeto un soporte de registro que comprende instrucciones para la ejecución de uno cualquiera de los procedimientos indicados anteriormente cuando estas instrucciones son ejecutadas por un ordenador electrónico.

La invención se comprenderá mejor con la lectura de la descripción que sigue, dada únicamente a título de ejemplo no limitativo y realizada haciendo referencia a los dibujos en los cuales:

- la figura 1 es una ilustración esquemática de un sistema de transmisión y de recepción de contenidos multimedia codificados,
- la figura 2 es un organigrama de un primer modo de realización de un procedimiento de protección de un contenido multimedia registrado,
- la figura 3 es un organigrama de otro modo de realización de un procedimiento de protección de un contenido multimedia registrado.

En estas figuras, las mismas referencias se utilizan para designar los mismos elementos.

En lo que sigue de esta descripción, las características y funciones bien conocidas del experto en la materia no se describen en detalle. Además, la terminología utilizada es la de los sistemas de acceso condicionales a contenidos multimedia. Para más informaciones sobre esta terminología, el lector puede referirse al documento siguiente:

- «Functional Model of Conditional Access System», EBU Review, Technical European Broadcasting Unión, Brussels, BE, nº 266, 21 diciembre 1995.

La figura 1 representa un sistema 2 de emisión y de recepción de contenidos multimedia codificados. Los contenidos multimedia emitidos son contenidos multimedia linealizados. Por ejemplo, un contenido multimedia corresponde a una secuencia de un programa audiovisual tal como una emisión de televisión o una película.

Los contenidos multimedia en claro son generados por una o varias fuentes 4 y transmitidos por una cabecera de red 6. La cabecera de red 6 difunde los contenidos multimedia simultáneamente hacia una multitud de terminales de recepción a través de una red de transmisión de informaciones. Los contenidos multimedia difundidos son, por ejemplo, sincronizados temporalmente los unos con los otros para respetar una parrilla preestablecida de programas.

La red 8 es típicamente una red de gran distancia de transmisión de informaciones tal como la red Internet o una red por satélite o cualquier otra red de difusión tal como la utilizada para la transmisión de la televisión digital terrestre (TNT).

La cabecera de red 6 comprende un codificador 16 que comprime los contenidos multimedia que recibe. El codificador 16 trata contenidos multimedia digitales. Por ejemplo, este codificador funciona conforme a la norma MPEG2 (Moving Picture Expert Group – 2) o la norma UIT-T H264.

Los contenidos multimedia comprimidos son dirigidos a una entrada de un multiplexor 26. Los mensajes ECM (Entitlement Control Message), EMM (Entitlement Management Message) y los contenidos multimedia comprimidos son multiplexados por el multiplexor 26. Los mensajes ECM y EMM son proporcionados por un sistema 28 de acceso condicional. Después, el flujo multiplexado así creado es codificado por un codificador 22 antes de ser transmitido a la red 8.

El codificador 22 codifica cada flujo multiplexado para acondicionar la visualización de los contenidos multimedia a ciertas condiciones tales como la compra de un título de acceso por los usuarios de terminales de recepción.

El codificador 22 codifica cada flujo multiplexado con la ayuda de palabras de control CW_t que le son proporcionadas, así como por el sistema 28 de acceso condicional, por un generador 32 de claves. Más precisamente, cada flujo multiplexado es dividido es una sucesión de criptoperiodos. Durante todo el tiempo de duración de un criptoperiodo, las condiciones de acceso al contenido multimedia codificado permanecen inalteradas. En particular, durante toda la duración de un criptoperiodo, el contenido multimedia es codificado con la misma palabra de control CW_t. Generalmente, la palabra de control CW_t varía de un criptoperiodo al otro. Además, la palabra de control CW_t es generalmente específica de un contenido multimedia, siendo esta última aleatoria o pseudoaleatoriamente lanzada. El índice t es un número de orden que identifica el criptoperiodo codificado con esta palabra de control CW_t.

Aquí, el conjunto de componentes del contenido multimedia, es decir particularmente el audio, el video, el teletexto, son codificados con la misma palabra de control CW_t. Por ejemplo, los contenidos multimedia son codificados a nivel TS («Transport Stream»).

Típicamente, este codificado es conforme a una norma tal como la norma DVB-CSA («Digital Video Broadcasting – Common Scrambling Algorithm», cuya puesta en práctica se describe en la norma DVB ETR 289), ISMA Cryp (Internet Streaming Media Alliance Encryption and Authentication), SRTP (Secure Real-time Transport Protocol, AES («Advanced Encryption Standard», cuya puesta en práctica se describe en la norma ATIS-0800006), etc.

El sistema 28 es más conocido bajo el acrónimo CAS (Condicional Access System). Para cada canal, el sistema 28 genera mensajes ECM_t (Entitlement Control Message) conteniendo al menos el criptograma CW^*_t de la palabra de control CW_t generada por el generador 32 y utilizada por el codificador 22 para codificar el criptoperiodo t del canal.

El sistema 28 introduce en cada ECM particularmente:

- los criptogramas CW^*_t y CW^*_{t+1} de las palabras de control CW_t y CW_{t+1} que permiten descodificar los criptoperiodos t y t+1 inmediatamente consecutivos del canal,
- las condiciones de acceso CA destinadas para ser comparadas con títulos de acceso adquiridos por el usuario, y
- una firma o una redundancia criptográfica MAC que permite comprobar la integridad del mensaje ECM.

El sistema 28 puede igualmente introducirse en los mensajes ECM:

- un indicador de modo de protección para aplicar en caso de registro del contenido multimedia, o
- una prohibición de registro del contenido multimedia.

El mensaje ECM que contiene el par de criptogramas CW^*_t/CW^*_{t+1} es indicado por ECM_t en lo que sigue de la descripción, donde el índice t es un número de orden que identifica la posición temporal de este mensaje ECM con relación a los otros mensajes ECM diferentes emitidos para descodificar el mismo contenido multimedia.

Aquí, el índice t identifica igualmente el criptoperiodo CP_t descodificable con la ayuda de la palabra de control CW_t contenida en el mensaje ECM_t.

A título de ilustración, aquí, el codificado y el multiplexado de los contenidos multimedia es conforme al protocolo DVB-Simulcrypt (ETSI TS 103 197).

El sistema 28 genera igualmente mensajes EMM (Entitlement Management Message) cuya utilización se describe en la figura 2. Estos mensajes EMM contienen particularmente los títulos de acceso con destino a los terminales de recepción. En la práctica, contrariamente a los mensajes ECM utilizados aquí, los mensajes EMM pueden ser direccionados a un solo terminal de recepción particular entre el conjunto de terminales del sistema 2.

Aquí, los mensajes ECM y EMM responden a la sintaxis definida en la norma DVB ETR 289 («Support for use of scrambling and conditional access within digital broadcasting systems»).

Aquí, el sistema 28 está conectado con una memoria 34 que contiene una tabla 36. La tabla 36 asocia con cada identificador STB-ID de un terminal de recepción diferentes atributos utilizados para su funcionamiento en el registro de un contenido multimedia recibido.

Para simplificar la figura 1, una vista parcial y ampliada de esta tabla 36 está representada en la figura 1 junto a la memoria 34. Con cada identificador STB-ID, esta tabla 36 asocia:

- un identificador de hogar House-Id,
- un campo «Record-A» que contiene una autorización o al contrario una prohibición de registrar los contenidos multimedia,
- un campo «Share-A» que contiene una autorización o al contrario una prohibición de particionar el contenido multimedia registrado con los diferentes terminales del mismo hogar,
- un campo «Life-T» que contiene eventualmente un tiempo de duración para una licencia asociada con un contenido multimedia registrado,
- un campo $KH'^{,Kisoft}$ que contiene un criptograma de una clave local corriente KH'_k cifrada con la clave K_{isoft} propia del terminal identificado por el identificador STB-ID,
- un campo KH''^{Kichip} que contiene un criptograma de una clave local KH''_k cifrada con una clave K_{ichip} propia del terminal identificado por el identificador STB-ID,
- un campo $KH'''^{,Kichip}$ que contiene un criptograma de una clave local KH'''_k cifrada con la clave K_{ichip} propia del terminal de recepción identificado por el identificador STB-ID, y
- un campo «Default-P» que contiene un indicador del modo de protección a aplicar por defecto en el registro de un contenido multimedia.

El identificador House-Id permite identificar un hogar entre todos los hogares del sistema 2. Un hogar alberga típicamente al menos uno y aquí generalmente varios terminales de recepción de contenidos multimedia codificados. Un hogar corresponde generalmente a un domicilio privado tal como un apartamento o una casa. Así, la tabla 36 asocia los diferentes terminales de recepción de un mismo hogar con el mismo identificador House-Id de este hogar.

El sistema 28 es típicamente realizado a partir de un ordenador electrónico programable capaz de ejecutar instrucciones en un soporte de registro de informaciones para la puesta en práctica del procedimiento de las figuras 2 o 3.

Un sistema 38 de gestión de los abonados está asociado con la memoria 34. Este sistema 38 es más conocido bajo el acrónimo de SMS («Subscriber Management System»). El sistema 38 permite particularmente llenar y modificar el contenido de los campos de la tabla 36.

El sistema 2 comprende una multitud de hogares cada uno equipado con uno o varios terminales de recepción. Estos terminales son más conocidos bajo el término inglés de «set-top box». Para simplificar la figura 1, solo tres hogares 40 a 42 han sido representados.

El hogar 40 se describirá en el caso particular en que éste comprenda cuatro terminales 50, 52, 54 y 56 de recepción de contenidos multimedia codificados. Estos terminales están conectados los unos con los otros por mediación de una red doméstica 60. La red 60 es una red local del hogar 40. Esta red 60 está aquí conectada con la red 8 por mediación de un modem ADSL (Asymmetric Digital Subscriber Line) de un proveedor de acceso a Internet. Aquí, este modem ADSL comprende igualmente un router. Generalmente, un hogar comprende como máximo un solo router. La red 60 es una red alámbrica, por ejemplo del tipo Ethernet, y/o una red inalámbrica tal como una red WiFi.

En este modo de realización, cada terminal tiene la capacidad de registrar un contenido multimedia y de leer un contenido multimedia registrado. Además, cada uno de estos terminales tiene generalmente la capacidad de descodificar, a medida que se va recibiendo, un contenido multimedia difundido por la cabecera de red 6 para visualizarlo en claro en una pantalla. Para simplificar la descripción y la figura, se supone aquí que solo algunos terminales son utilizados para registrar un contenido multimedia mientras que solo otros terminales son utilizados para leer el contenido multimedia registrado. A continuación, los terminales utilizados para registrar son llamados «registradores» y los terminales utilizados para leer el contenido multimedia registrado son llamados «lectores».

Para los registradores, solo las características útiles para el registro de un contenido multimedia son descritas. Las características de un registrador para leer un contenido multimedia registrado son por ejemplo idénticas a las descritas para los lectores. De forma recíproca, solo las características de cada lector útiles para leer un contenido multimedia se describen aquí en detalle. Las características de estos lectores para registrar un contenido multimedia son por ejemplo idénticas a las descritas con respecto a los registradores.

Más precisamente, aquí, los terminales 50 y 52 se describen como registradores mientras que los terminales 54 y 56 se describen como lectores.

El registrador 50 está equipado con un ordenador electrónico 64 conectado con un soporte de registro 66. Este ordenador 64 es apto para ejecutar las instrucciones registradas en el soporte 66 para poner en práctica el procedimiento de la figura 2 o 3. A este respecto, el soporte 66 comprende particularmente las instrucciones de un módulo 68 de registro y de un agente 70 de acceso condicional.

El ordenador 64 está igualmente conectado con una memoria de masa 72 destinada para contener los contenidos multimedia registrados. Esta memoria 72 es típicamente un periférico de almacenado de masa tal como un disco duro, una clave USB (Universal Serial Bus) o similares.

El registrador 50 comprende igualmente un procesador de seguridad que trata informaciones confidenciales tales como las claves criptográficas. Para preservar la confidencialidad de estas informaciones, este procesador está concebido para ser lo más robusto posible frente a tentativas de ataque realizadas por piratas informáticos. Por consiguiente, es más robusto frente a estos ataques que los otros componentes del registrador 50. A este efecto, el procesador incorpora su propio ordenador 76 conectado a su propia memoria 78 únicamente accesible por el procesador 76. Típicamente, la memoria 78 es incorporada por el procesador para que esta sea protegida y hecha lo más robusta posible. Aquí, el procesador es un procesador de seguridad amovible tal como una tarjeta de circuito impreso con chip 74.

La memoria 78 comprende particularmente una clave criptográfica K_{isc} propia para la tarjeta de circuito impreso con chip 74 y un identificador SC-ID de esta tarjeta con chip. En esta descripción, se dice que una clave es «propia de» un dispositivo cuando la misma permite identificar de forma única este dispositivo entre el conjunto de dispositivos del sistema 2. La misma es por consiguiente única para este dispositivo. El identificador SC-ID permite identificar la tarjeta de circuito impreso con chip 74 entre el conjunto de tarjetas de circuito impreso con chip del sistema 2.

Solo la tarjeta de circuito impreso con chip 74 del sistema 2 tiene la clave K_{isc}. Típicamente, esta clave K_{isc} es inscrita durante la personalización de la tarjeta de circuito impreso con chip, es decir durante la fabricación de ésta. El índice « i » de la clave K_{isc} identifica el terminal.

El registrador 52 es similar al registrador 50 salvo que el ordenador 64 sea sustituido por un procesador 80 de seguridad.

Este procesador 80 comprende un microprocesador 82 programable apto para ejecutar instrucciones registradas en un soporte de registro de informaciones. A este respecto, el procesador 80 está conectado con una memoria 84 que comprende instrucciones para la puesta en práctica del procedimiento de la figura 2 o 3. Esta memoria 84 comprende particularmente las instrucciones de un módulo 86 de registro y de un agente 88 de acceso condicional. El procesador 80 comprende igualmente varios coprocesadores aptos para ejecutar instrucciones en paralelo a las ejecutadas por el microprocesador 82. Estos coprocesadores están destinados para realizar más rápidamente tareas específicas. Aquí, el procesador 80 comprende al menos un coprocesador criptográfico 96 concebido para ejecutar las operaciones de cifrado y de descifrado.

El coprocesador criptográfico 96 comprende una memoria interna 98 en la cual se registran diferentes informaciones confidenciales. Por ejemplo, una clave $K_{ichip,}$ así como el identificador STB-ID del registrador 52 son registrados en esta memoria 98. La clave K_{ichip} es propia del registrador 52 y no es conocida por ningún otro registrador. Por ejemplo, esta clave K_{ichip} es registrada durante la fabricación del procesador 80. El índice « i » de la clave K_{ichip} identifica el terminal.

El procesador 80 puede comprender otros coprocesadores. Estos otros coprocesadores están designados por el nombre de la función que cumplen. Por ejemplo, aquí, el procesador 80 comprende igualmente los coprocesadores siguientes:

- un desmultiplexor 90,
- un descodificador 92, y
- un codificador 94.

Típicamente, el microprocesador 82 así como el conjunto de estos coprocesadores están realizados en el mismo trozo de silicio llamado igualmente «tarjeta de circuito impreso con chip». Son por consiguiente fabricados al mismo tiempo.

El procesador 80 está igualmente conectado con una memoria de masa 100 destinada a contener los contenidos multimedia registrados. Esta memoria 100 es por ejemplo idéntica a la memoria 72.

El registrador 52 comprende igualmente un procesador de seguridad amovible 102 tal como una tarjeta de circuito impreso con chip. Por ejemplo, estructuralmente, esta tarjeta de circuito impreso con chip 102 es idéntica a la tarjeta de circuito impreso con chip 74. La clave K_{isc} y el identificador SC-ID contenido en su memoria 78 son diferentes de los contenidos en la memoria 78 de la tarjeta de circuito impreso con chip 74.

El lector 54 es capaz de leer un contenido multimedia registrado por uno cualquiera de los registradores 50, 52 y de visualizar este contenido multimedia registrado en claro en un visualizador 110. El visualizador 110 es por ejemplo una pantalla.

El lector 54 comprende un ordenador electrónico 112 programable conectado con una memoria 114. El ordenador 112 es apto para ejecutar instrucciones registradas en la memoria 114 para poner en práctica el procedimiento de la figura 2 o 3. A este respecto, la memoria 114 comprende particularmente las instrucciones:

- de un módulo 116 de lectura de contenido multimedia,
- de un agente 118 de acceso condicional, y
- de un descodificador 120.

El identificador STB-ID así como una clave K_{isoft} de este lector 54 son por ejemplo almacenados en la memoria 114. La clave K_{isoft} es propia del lector 54.

El lector 56 es idéntico al lector 54 salvo que el ordenador 112 sea sustituido por un procesador 130 de seguridad. La estructura de este procesador 130 es similar a la del procesador 80 anteriormente descrito. En particular, comprende un microprocesador 132 capaz de ejecutar instrucciones registradas en una memoria 134 conectada con este procesador 130. Comprende igualmente los coprocesadores siguientes:

- un desmultiplexor 136,
- un decodificador 138,
- un descodificador 140, y
- un coprocesador criptográfico 142 que contiene su propia memoria 144 en el interior de la cual se registran diferentes informaciones confidenciales tales como la clave criptográfica K_{ichip} y el identificador STB-ID del lector 56.

Una clave K_{isoft} propia de este lector es igualmente registrada en la memoria 144.

Aquí, el lector 56 está conectado con un visualizador 146, por ejemplo, idéntico al visualizador 110.

Los otros hogares del sistema 2 tales como los hogares 41 o 42 comprenden uno o varios registradores tales como los registradores 50 y 52 y uno o varios lectores tales como los lectores 54 o 56. Los hogares 41 y 42 corresponden a identificadores de hogar House-Id diferentes del del hogar 40.

Aquí, solo los terminales del hogar 40 están asociados con su identificador House-Id común en la tabla 36.

El funcionamiento del sistema 2 se describirá ahora con respecto al procedimiento de la figura 2 en el caso particular del hogar 40. Lo que se ha descrito para el hogar 40 se aplica a los otros hogares del sistema 2.

Se procede primeramente a una fase de inicialización o de reinicialización 150.

Durante esta fase 150 y más precisamente durante una etapa 152, para cada identificador House-Id, el sistema 28 genera un juego de tres claves locales KH'_k, $KH"_k$ y $KH"'_k$. El índice «k» es el índice de clave e identifica la versión de la clave. En lo que sigue de esta descripción, se designa por «KH_k» una cualquiera de estas tres claves.

Cada una de estas claves corresponde a un modo de protección particular de un contenido multimedia registrado. Aquí, los tres modos de protección siguientes son utilizados yendo del menos robusto al más robusto:

- una protección logicial de las palabras de control,
- una protección material de las palabras de control, y
- una protección mediante nuevo codificado local del contenido multimedia.

Estos tres modos corresponden, en orden, a las claves KH'_k, $KH"_k$ y $KH"'_k$.

La protección material necesita la utilización de un procesador de seguridad protegido por un componente material. Aquí, solo los registradores 50 y 52 y el lector 56 pueden poner en práctica este modo de protección. De igual modo, la protección por nuevo codificado local necesita la utilización de un codificador implementado en un procesador de seguridad material. Aquí, solo el registrador 52 y el lector 56 pueden poner en práctica este modo de protección. A la inversa, la protección logicial no necesita la utilización de procesador de seguridad material. La misma puede por consiguiente ser utilizada por todos los terminales.

En la etapa 152, el índice k de clave es incrementado por un paso predeterminado.

En una etapa 154 para cada terminal asociado con el identificador House-Id del hogar 40 en la tabla 36, el sistema 28 genera un criptograma KH'^{Kisoft}_k con la clave K_{isoft} propia de este terminal. En lo que sigue de esta descripción, se indica «A^B» el criptograma obtenido cifrando el dato A con la ayuda de la clave B.

Para cada terminal asociado con el identificador House-Id del hogar 40 y equipado con un procesador de seguridad material apto para quitar una protección material, y únicamente para aquellos, el sistema 28 genera un criptograma $KH"^{Kichip}_k$ con la clave K_{ichip} de este terminal. Por último, para cada terminal asociado con el identificador House-Id del hogar 40 y equipado con un procesador de seguridad material apto para poner en práctica una protección mediante nuevo codificado local, y únicamente para aquellos, el sistema 28 genera un criptograma $KH"'^{Kichip}_k$ con la clave K_{ichip} de este terminal.

Los criptogramas KH'^{Kisoft}_k, $KH"^{Kichip}_k$ y $KH"'^{Kichip}_k$ son registrados, respectivamente, en los campos KH'^{Kisoft}, $KH"^{Kichip}$ y $KH"'^{Kichip}$ de la tabla 36 en la columna correspondiente al identificador STB-ID de este terminal. Si uno de los criptogramas no ha sido generado pues el terminal no es capaz de poner en práctica este modo de protección, entonces el campo queda vacío.

Durante una etapa 156, para cada terminal cuyo contenido del campo «Record-A» de la tabla 36 indica que está autorizado para registrar contenidos multimedia, la cabecera de red 6 transmite un mensaje EMM que comprende el contenido de los campos «Record-A», «Default-P», «Life-T», «Share-A», «KH'^{Kisoft}», «$KH"^{Kichip}$», «$KH"'^{Kichip}$» así como el índice de clave k.

Durante esta etapa 156, la cabecera de red 6 transmite igualmente a cada tarjeta de circuito impreso con chip de los terminales del hogar 40 las claves locales KH'_k y $KH"_k$ por intermedio de los agentes de acceso condicional. Más precisamente, la cabecera de red 6 transmite únicamente los criptogramas KH'^{Kisc}_k y $KH"^{Kisc}_k$ obtenidos con la clave K_{isc} de esta tarjeta de circuito impreso. El contenido del campo «Default-P» asociado con el identificador STB-ID del terminal en el cual es introducida le es igualmente transmitido. Durante esta transmisión, el campo «Default-P» está protegido con la ayuda de un secreto propio de la tarjeta de circuito impreso con chip.

Durante una etapa 158, en respuesta a la recepción de estos mensajes EMM, cada agente de acceso condicional de los terminales 50, 52, 54 y 56 registra la configuración recibida y los criptogramas KH_k^{Ki} que le han sido transmitidos, así como el índice k de la clave local.

Durante esta etapa 158, las tarjetas de circuito impreso con chip 74 y 102 descifran los criptogramas recibidos para obtener las claves locales KH'_k y KH''_k y registran estas claves en sus memorias respectivas 78. El contenido del campo «Default-P» es igualmente registrado.

La fase 150 se termina entonces.

Durante una etapa 162, la cabecera de red 6 difunde un flujo multimedia codificado en el cual el contenido multimedia es multiplexado con los mensajes ECM_t correspondientes. Los mensajes ECM_t correspondientes son los mensajes ECM_t que contienen los criptogramas de las palabras de control que permiten descodificar este contenido multimedia.

Cuando el usuario lo desea, este comanda uno de los registradores 50 o 52 para registrar el contenido multimedia actualmente difundido por la cabecera de red 6. Aquí, dos fases 170 y 172 de registro distintas serán descritas.

La fase 170 corresponde a un registro del contenido multimedia con una protección logicial o material. Por ejemplo, esta fase 170 es realizada por el registrador 50.

La fase 170 comienza por una etapa 173 de adquisición de un control de registro del contenido multimedia actualmente difundido.

En respuesta, durante una etapa 174, el módulo 68 recibe y desmultiplexa el flujo multimedia recibido para extraer un flujo SPTS (Single Program Transport Stream) que contiene las componentes de video, audio y teletexto de un solo contenido multimedia. El módulo 68 extrae igualmente de este flujo multimedia los mensajes ECM_t que corresponden al contenido multimedia a registrar y los transmite al agente 70 de acceso condicional.

Durante una etapa 176, el agente 70 procede a diferentes comprobaciones. Por ejemplo, comprueba que el registrador 50 esté autorizado para registrar contenidos multimedia. Esta comprobación se realiza por ejemplo con la ayuda del contenido del campo «Record-A» anteriormente recibido. Comprueba igualmente durante esta etapa que el mensaje ECM_t correspondiente al contenido multimedia no comprende ninguna prohibición de registro. La incorporación en los mensajes ECM_t de una prohibición de registro permite impedir el registro de algunos contenidos multimedia recibidos, por ejemplo, para respetar los derechos de autor.

Por último, comprueba igualmente si el mensaje ECM_t impone un modo de protección para este contenido multimedia en su registro. Si así es el caso, el agente 70 comprueba que este modo de protección está soportado por el registrador 50. Por ejemplo, en el caso del registrador 50, este soporta los modos de protección logicial y material, pero no es capaz de realizar la protección por un nuevo codificado local.

Si por uno de los motivos mencionados anteriormente, el registro del contenido multimedia no es posible, entonces el procedimiento vuelve a la etapa 173. En el caso contrario, el agente 70 procede a una etapa 178.

Durante la etapa 178, el agente 70 determina el modo de protección a poner en práctica. Si el modo de protección es forzado por una instrucción contenida en los mensajes ECM_t, este modo de protección impuesto es seleccionado. Si ningún modo de protección es impuesto por el contenido de los mensajes ECM_t, el agente 70 selecciona el modo de protección por defecto contenido en el campo «Default-P». Conocer el modo de protección a aplicar permite al agente 70 determinar a que procesador de seguridad deben dirigirse los mensajes ECM_t recibidos. Por ejemplo, si el modo de protección logicial o material debe aplicarse, entonces los mensajes ECM_t son transmitidos a la tarjeta de circuito impreso con chip introducida en este terminal. Si la protección mediante nuevo codificado local debe ser realizada, los mensajes ECM_t son directamente dirigidos hacia el procesador de seguridad 80 de este terminal. Dentro del marco de la fase 170, se supone que es la protección logicial o material la que debe ser aplicada.

A continuación, siempre durante esta etapa 178, genera un identificador RECORD-ID que permite identificar el contenido multimedia registrado. Por ejemplo, este identificador RECORD-ID es función de la fecha de comienzo de registro así como del identificador STB-ID del registrador 50.

Durante una etapa 180, el agente 70 envía el identificador RECORD-ID al módulo 68 y cada mensaje ECM_t recibido a la tarjeta de circuito impreso con chip 74.

Durante una etapa 182, la tarjeta de circuito impreso con chip 74 procede a diferentes comprobaciones y determina el modo de protección a aplicar. Aquí, la tarjeta de circuito impreso con chip 74 comprueba las condiciones siguientes:

- el mensaje ECM_t correspondiente al contenido multimedia no comprende ninguna prohibición de registro;
- cuando un modo de protección es impuesto por los mensajes ECM_t, este modo de protección está soportado por el registrador 50 comprobando la presencia de la clave KH'_k o KH''_k necesaria para este modo de protección en la memoria 78,
- los títulos de acceso que contiene corresponden a los derechos de acceso contenidos en los mensajes ECM_t.

Si una de estas condiciones no es satisfactoria, el registro se inhibe y el procedimiento vuelve a la etapa 173.

Si todas estas condiciones son satisfactorias, la tarjeta de circuito impreso con chip selecciona el modo de protección a aplicar. Esta selección se realiza como la descrita para el agente 70 salvo que el campo «Default-P» utilizado es el registrado en la memoria 78. El hecho de determinar de nuevo el modo de protección a aplicar en la tarjeta de circuito impreso con chip hace más difícil cualquier tentativa de falsificación del modo de protección a aplicar.

Seguidamente, durante una etapa 184, la tarjeta de circuito impreso con chip descifra los criptogramas CW^*_t y CW^*_{t+1} contenidos en los mensajes ECM_t recibidos para obtener las palabras de control CW_t y CW_{t+1} en claro. Este descifrado se realiza con la ayuda de la clave de abonado K_a. La clave K_a es una clave que es transmitida por la cabecera de red, por mensaje EMM, a los terminales que han suscrito un abono que permite descodificar el contenido multimedia. Típicamente, esta clave K_a es renovada todos los meses. La clave K_a es la misma para todos los terminales autorizados para descodificar el contenido multimedia incluso si estos terminales pertenecen a hogares diferentes.

Durante una etapa 186, la tarjeta de circuito impreso con chip 74 protege el contenido multimedia registrado. A este efecto, aquí, cifra las palabras de control CW_t y CW_{t+1} con la clave local KH_k correspondiente al modo de protección seleccionado para obtener los criptogramas CW_t^{KHk} y CW_{t+1}^{KHk}. Por ejemplo, si el modo de protección seleccionado es la protección logicial, la clave local utilizada es KH'_k. Si el modo de protección seleccionado es la protección material, la clave local utilizada es KH''_k. Seguidamente, los criptogramas CW_t^{KHk} y CW_{t+1}^{KHk} son transmitidos al agente 70.

Durante la etapa 190, en respuesta, el agente 70 elabora una licencia para la lectura del contenido multimedia registrado. Más precisamente, durante la etapa 190, el agente 70 asocia con cada criptograma CW_t^{KHk} un índice temporal $ECM\text{-}REF_t$. El índice temporal $ECM\text{-}REF_t$ identifica el criptoperiodo CP_t del contenido multimedia que debe ser descodificado con la palabra de control CW_t. Por ejemplo, el índice temporal $ECM\text{-}REF_t$ es un contador temporal incrementado por un paso predeterminado en cada recepción de un nuevo mensaje ECM_t.

Seguidamente, el agente 70 registra cada criptograma CW_t^{KHk} asociado con su índice temporal $ECM\text{-}REF_t$ en un bloque de palabras de control.

De preferencia, el agente 70 introduce igualmente el nivel moral requerido y el modo de protección del contenido multimedia registrado. Por último, durante la etapa 190, el agente 70 determina el tiempo de duración de la licencia añadiendo a la fecha actual, el tiempo de duración contenido en el campo « Life-T » recibido. El índice k de la clave local KH_k utilizada para cifrar las palabras de control es igualmente introducido en la licencia.

Una vez elaborada esta licencia, durante una etapa 192, el módulo 68 registra el contenido multimedia codificado en la memoria 72 asociado con la licencia elaborada por el agente 70.

Se apreciará que durante la fase 170, el contenido multimedia registrado no es descodificado y luego codificado de nuevo. El registro del contenido multimedia en modo de protección material de las palabras de control se realiza de forma idéntica a lo que ha sido anteriormente descrito salvo que la clave KH''_k es seleccionada por la tarjeta de circuito impreso con chip 74 durante la etapa 186.

La fase 172 corresponde al registro de un contenido multimedia con una protección por nuevo codificado local. Esta se 172 es aquí realizada por el registrador 52 pues el registrador 50 está desprovisto de esta capacidad.

La fase 172 comienza por las mismas etapas 173 a 178 que las anteriormente descritas salvo que las mismas son realizadas por el módulo 86 y el agente 88. Durante la etapa 178, se supone que el modo de protección seleccionado es el nuevo codificado local.

Seguidamente, durante una etapa 200, el agente 88 de acceso condicional calcula implícitamente una palabra de control CW' generando una clave, es decir obteniendo un número aleatorio, que se considera como que proporciona el valor del criptograma $CW'^{KH'''k}$. Luego, transmite este criptograma $CW'^{KH'''k}$ al procesador 80.

Durante una etapa 202, el coprocesador criptográfico 96 descifra el criptograma $CW'^{KH'''k}$ con su clave KH'''_k para obtener una palabra de control CW'. La clave KH'''_k es utilizada pues aquí la protección por un nuevo codificado local

ha sido seleccionada en la etapa 178. Durante esta etapa, el agente 88 construye igualmente una licencia como se ha descrito en relación con la etapa 190 salvo que el bloque de palabras de control sea sustituido por el criptograma $CW'^{KH'''k}$.

Durante una etapa 204, el agente 88 envía cada mensaje ECM_t recibido a la tarjeta de circuito impreso con chip.

Durante una etapa 206, la tarjeta de circuito impreso con chip 102 comprueba si la misma tiene los títulos de acceso que permiten descodificar este contenido multimedia.

Si la tarjeta de circuito impreso con chip 102 tiene los títulos de acceso que le dan derecho a descodificar el contenido multimedia recibido, durante una etapa 208, la tarjeta de circuito impreso con chip 102 descifra los criptogramas CW^*_t contenidos en el mensaje ECM_t con la ayuda de la clave de abonado K_a. La misma obtiene entonces las palabras de control en claro CW_t.

Durante una etapa 210, el ordenador 76 cifra estas palabras de control CW_t en claro con la ayuda de una clave de sesión secreta K_s para obtener criptogramas CW_t^{Ks}. Estos criptogramas son enviados al procesador 80.

Durante una etapa 212, el coprocesador criptográfico 94 descifra los criptogramas CW_t^{Ks} para obtener las palabras de control en claro CW_t. La utilización de la clave de sesión K_s permite por consiguiente asegurar la transmisión de las palabras de control entre la tarjeta de circuito impreso con chip 102 y el procesador 80. Esta clave K_s es diferente de las claves K_{isoft} y K_{ichip} del procesador 80.

Durante una etapa 214, el descodificador 92 descodifica el contenido multimedia recibido con la ayuda de las palabras de control CW_t para obtener el contenido multimedia en claro.

Seguidamente, durante una etapa 216, el codificador 94 codifica este contenido multimedia en claro con la ayuda de la palabra de control CW'. Para el codificado del contenido multimedia registrado, una sola palabra de control CW' es aquí utilizada. En efecto, se supone aquí que el algoritmo de cifrado utilizado es lo suficientemente robusto para que una sola palabra de control baste. Por ejemplo, el algoritmo de cifrado utilizado es el algoritmo AES (Advanced Encryption Standard).

Una vez codificado de nuevo, durante una etapa 218, el contenido multimedia y la licencia elaborada son registrados por el módulo 86 en la memoria 100.

Se observará que para la protección por recodificado local, la utilización del índice temporal $ECM\text{-}REF_t$ se vuelve inútil pues una sola palabra de control CW' es utilizada para codificar todos los criptoperiodos del contenido multimedia registrado.

Las fases 170 y 172 pueden ser ejecutadas al mismo tiempo o una después de la otra y en el mismo terminal o en terminales diferentes.

Los contenidos multimedia registrados en las fases 170 o 172 pueden ser leídos por otro lector del hogar mecánicamente independiente del registrador. Tres procedimientos de lectura son posibles en función del modo de protección utilizado en el registro del contenido multimedia. Cada uno de estos procedimientos de lectura corresponde a una de las fases de lectura descritas ahora.

Durante una fase 230, un contenido multimedia registrado con una protección logicial es leído. Esta fase 230 se describe en el caso particular donde el lector sea el lector 54.

Al comienzo de la fase 230, durante una etapa 232, un usuario selecciona un contenido multimedia registrado por uno de los registradores del hogar 40. Por ejemplo, durante esta etapa 232, un catálogo de los diferentes contenidos multimedia registrados por los registradores del hogar 40 es visualizado. Este catálogo contiene típicamente el nombre, el tiempo de duración, el número de la cadena en la cual ha sido registrado el contenido multimedia, el identificador del registrador que ha registrado este contenido multimedia así como el identificador del contenido multimedia RECORD-ID. Durante esta etapa 132, se supone que un contenido multimedia registrado en la memoria 72 del registrador 50 es seleccionado.

Durante una etapa 234, el lector comprueba si está autorizado o no para leer un contenido multimedia. Aquí, se supone que un lector está autorizado para leer un contenido multimedia registrado a partir del momento en que éste ha recibido igualmente la autorización de registrar los contenidos multimedia. Así, esta comprobación se realiza a partir del contenido del campo «Record-A». En el caso negativo, el procedimiento vuelve a la etapa 232.

Durante una etapa 236, si está autorizado para leer, el agente 118 envía una demanda de licencia al registrador 50 identificado a partir del identificador STB-ID contenido en el catálogo de contenidos multimedia. Esta demanda incluye particularmente el identificador RECORD-ID del contenido multimedia seleccionado.

Durante una etapa 238, en respuesta a esta demanda, el registrador 50 comprueba a partir del contenido de su campo «Share-A» si está autorizado para particionar un contenido multimedia registrado. En caso afirmativo, el agente 70 transmite la licencia del contenido multimedia asociado al identificador RECORD-ID. En el caso contrario, el procedimiento vuelve a la etapa 232. Aquí, se supone que la partición está autorizada.

El agente 118 recibe esta licencia y comprueba, durante una etapa 240:

- si el tiempo de duración de la licencia ha expirado, y
- si el modo de protección del contenido multimedia es accesible para el lector 54.

En particular, durante la etapa 240, el agente 118 comprueba que está en posesión del criptograma $KH'_k{}^{Kisoft}$ correspondiente al modo de protección y al índice k de clave local contenidos en la licencia. En caso negativo, el procedimiento vuelve a la etapa 232.

En caso afirmativo, durante una etapa 242, el agente 118 descifra el criptograma $KH'_k{}^{Kisoft}$ con su clave K_{isoft}. El criptograma es seleccionado, por el agente 118, en función del nivel de protección y del índice k de clave local demandados en la licencia entre el conjunto de criptogramas de claves locales memorizados en el lector 54. Al término de la etapa 242, la clave local KH'_k es obtenida.

Seguidamente, durante una etapa 244, el registrador 50 transmite, por ejemplo en lectura de flujo, el contenido multimedia registrado y los índices temporales $ECM\text{-}REF_t$ al lector 54 a partir de la memoria 72. La transmisión en lectura de flujo es igualmente más conocida bajo el término inglés de «streaming».

Durante una etapa 246, el módulo 116 proporciona el índice temporal $ECM\text{-}REF_t$ del criptoperiodo a descodificar al agente 118.

En respuesta, durante una etapa 248, el agente 118 busca el criptograma $CWt^{KH'k}$ asociado con el índice temporal $ECM\text{-}REF_t$ recibido en el bloque de palabras de control de la licencia recibida.

Seguidamente, el agente 118 descifra este criptograma encontrado con la clave local KH'_k para obtener la palabra de control CW_t en claro. Al final de la etapa 248, la palabra de control CW_t en claro es transmitida al descodificador 120.

Durante una etapa 250, el descodificador 120 descodifica el contenido multimedia registrado con la ayuda de las palabras de control en claro CW_t recibidas. El contenido multimedia en claro es entonces visualizado de forma directamente perceptible y comprensible por un ser humano en la pantalla 110.

La lectura de un contenido multimedia registrado con una protección material será ahora descrita con referencia a una fase 260 de lectura. La fase 260 es por ejemplo realizada por el lector 56 ya que éste está equipado con un procesador de seguridad 130. La fase 260 comienza por las mismas operaciones 232 a 240 que las ya descritas en relación con la fase 230.

Seguidamente, durante una etapa 262, el procesador 130 selecciona el criptograma $KH''_k{}^{Kichip}$ en función del nivel de protección y del índice de clave k contenidos en la licencia recibida. Este criptograma es transmitido al coprocesador 142 que lo descifra con su propia clave K_{ichip} contenida, por ejemplo, en la memoria 144.

Seguidamente, se procede a las etapas 264, 266, 268 y 270 idénticas, respectivamente, a las etapas 244, 246, 248 y 250 a excepción del hecho de que son ejecutadas por el procesador de seguridad 130 y no por los módulos y agente logiciales 116, 118 y 120 y que la clave KH''_k es utilizada en lugar de la clave KH'_k. En particular, el descodificado se realiza por el descodificador 140.

Durante una fase 280, el lector 56 es utilizado para leer un contenido multimedia registrado con una protección por recodificado local.

La fase 280 comienza por las mismas etapas 232 a 240 que las descritas en relación con la fase 230.

Seguidamente, durante una etapa 282, el procesador 130 selecciona el criptograma $KH'''_k{}^{Kichip}$ en función del nivel de protección y del índice k de clave local contenidos en la licencia. Durante esta etapa, el coprocesador criptográfico 142 descifra este criptograma $KH'''_k{}^{Kichip}$ con la ayuda de su clave K_{ichip} para obtener la clave local KH'''_k.

Seguidamente, durante una etapa 284, el criptograma $CW'^{KH'''k}$ es extraído, por el procesador 130, de la licencia recibida y luego descifrado con la ayuda de su clave KH'''_k. Obtiene entonces la palabra de control CW' en claro.

Durante una etapa 286, el descodificador 140 descodifica el contenido multimedia codificado con la palabra de control CW' en claro para obtener el contenido multimedia descodificado.

Finalmente, durante una etapa 288, el contenido multimedia descodificado es transmitido al visualizador 146 de forma que sea visualizado de manera perceptible y directamente comprensible por un ser humano.

El procedimiento anteriormente indicado permite activar y desactivar fácilmente la partición de contenido multimedia registrado con un terminal particular del hogar 40. Por ejemplo, para desactivar la partición con los otros terminales del hogar de nuevos contenidos multimedia susceptibles de ser registrados, la cabecera de red 6 envía un mensaje EMM a este terminal para cambiar el contenido del campo «Share-A» y prohibir la partición.

Resulta igualmente posible suprimir de una tarjeta de circuito impreso con chip las claves locales KH'_k y KH''_k para limitar el funcionamiento del terminal. Se pueden suprimir todas las claves locales de la tarjeta de circuito impreso con chip para impedir completamente a este registrador particionar los nuevos contenidos multimedia registrados con los otros lectores del hogar. Se puede igualmente suprimir solo una clave para permitir el registro de contenido multimedia particionable únicamente con un modo de protección específico.

De forma similar, para impedir la lectura de contenido multimedia registrado por uno de los lectores del hogar 40, la cabecera de red 6 envía un mensaje EMM que contiene instrucciones para borrar los criptogramas $KH'_k{}^{Kisoft}$, $KH''_k{}^{Kichip}$, $KH'''_k{}^{Kichip}$.

El contenido del campo «Record-A» puede igualmente ser modificado gracias al envío de un nuevo mensaje EMM para cambiar las autorizaciones de registro.

Por motivos de seguridad o para añadir o revocar un terminal en el hogar, las claves locales KH'_k, KH''_k y KH'''_k son renovadas. En estas condiciones, una nueva fase 150 de inicialización es reiterada. Durante esta nueva fase 150, nuevas claves locales KH'_{k+1}, KH''_{k+1} y KH'''_{k+1} son generadas para el hogar 40. El índice de clave k es igualmente incrementado. En respuesta a la recepción de este nuevo juego de claves locales, las tarjetas de circuito impreso con chip borran el antiguo juego de claves locales y lo sustituyen por el nuevo juego de claves locales. En efecto, las claves locales contenidas en las tarjetas de circuito impreso con chip son únicamente utilizadas para registrar los nuevos contenidos multimedia. La tarjeta de circuito impreso con chip no tiene por consiguiente necesidad de registrar las antiguas claves locales utilizadas.

Por el contrario, los agentes de acceso condicional de los diferentes terminales del hogar 40 registran los nuevos criptogramas $KH'_{k+1}{}^{Kisoft}$, $KH''_{k+1}{}^{Kichip}$ y $KH'''_{k+1}{}^{Kichip}$ y no borran los criptogramas $KH'_k{}^{Kisoft}$, $KH''_k{}^{Kichip}$ y $KH'''_k{}^{Kichip}$. En efecto, estos antiguos criptogramas son útiles para leer un contenido multimedia registrado antes de la renovación de las claves locales. En cada lectura de un contenido multimedia, la clave local correcta es seleccionada gracias al índice de clave k asociado con la licencia del contenido multimedia registrado. La renovación de las claves KH'_k, KH''_k y KH'''_k permite revocar un terminal del hogar. En efecto, el terminal revocado ya no está asociado con el identificador House-Id del hogar en la tabla 36. Por consiguiente, no recibe los criptogramas $KH'_{k+1}{}^{Kisoft}$, $KH''_{k+1}{}^{Kichip}$ y $KH'''_{k+1}{}^{Kichip}$. No puede por consiguiente leer o registrar un contenido multimedia protegido con una de las claves KH'_{k+1}, KH''_{k+1} y KH'''_{k+1} y por consiguiente particionar este contenido multimedia con los demás terminales del hogar. A la inversa la renovación de las claves KH'_k, KH''_k y KH'''_k permite añadir un nuevo terminal al hogar. En este caso, el identificador STB-ID del nuevo terminal debe ser asociado con el identificador House-Id del hogar en la tabla 36 antes del lanzamiento de la fase 150 de reinicialización.

En el caso particular del aporte de un terminal al hogar, puede estar previsto que desde que un nuevo identificador STB-ID está asociado con el identificador House-Id, la cabecera de red transmite a este terminal los criptogramas de las claves KH'_k, KH''_k y KH'''_k para el índice k actual pero igualmente las versiones precedentes KH'_{k-j}, KH''_{k-j} y KH'''_{k-j} de estas claves, donde j es un número entero natural que varía entre 1 y k. Así, el nuevo terminal del hogar puede leer contenidos multimedia protegidos con una versión precedente de las claves KH'_k, KH''_k y KH'''_k.

La figura 3 representa otro procedimiento de funcionamiento del sistema 2. Se describe en el caso particular del hogar 40. En este procedimiento, los criptogramas $KH'_k{}^{Kisoft}$, $KH''_k{}^{Kichip}$ y $KH'''_k{}^{Kichip}$ no son directamente transmitidos desde la cabecera de red 6 a todos los lectores sino transmitidos a los lectores por mediación de los registradores.

El procedimiento comienza por una fase 300 de inicialización. La fase 300 es por ejemplo idéntica a la fase 150 a excepción del hecho de que la etapa 156 es sustituida por una etapa 302. Durante la etapa 302, los criptogramas $KH'_k{}^{Kisoft}$, $KH''_k{}^{Kichip}$ y $KH'''_k{}^{Kichip}$ generados para los diferentes lectores del hogar 40 son únicamente transmitidos a los registradores y no directamente a los lectores. Los registradores memorizan estos criptogramas asociados con el identificador STB-ID del lector correspondiente. De preferencia, los criptogramas $KH'_k{}^{Kisoft}$, $KH''_k{}^{Kichip}$ y $KH'''_k{}^{Kichip}$ para el agente de acceso condicional y los criptogramas $KH'_k{}^{Kisc}$ y $KH''_k{}^{Kisc}$ para la tarjeta de circuito impreso con chip son transmitidos en un mismo mensaje EMM.

La transmisión de los contenidos multimedia así como las fases de registro son idénticas a las anteriormente descritas.

Seguidamente, el lector 54 procede a una fase 310 de lectura de un contenido multimedia registrado con una protección logicial. Esta fase 310 es por ejemplo idéntica a la fase 230 salvo que las etapas 236 y 238 son sustituidas por las etapas 312 y 314.

Durante la etapa 312, la solicitud de licencia incluye igualmente el identificador STB-ID del lector 50.

Durante la etapa 314, si la partición de contenido multimedia registrado es autorizada, el registrador personaliza la licencia transmitida al lector en función del identificador STB-ID recibido en la solicitud. Más precisamente, el registrador integra en la licencia el criptograma KH'_k^{Kisoft} asociado con el identificador STB-ID del lector. Esta licencia personalizada es entonces transmitida al lector.

Durante la etapa 242, el lector recupera por consiguiente el criptograma KH'_k^{Kisoft} directamente de la licencia recibida y no de un mensaje EMM.

El resto de las etapas es idéntico a las descritas en relación con la fase 230. Así, en este modo de realización, el criptograma KH'_k^{Kisoft} solo es transmitido al lector en el momento de la solicitud de lectura y no sistemáticamente durante una fase de inicialización.

Resulta igualmente posible proceder a las fases 320 y 322 de lectura de un contenido multimedia registrado, respectivamente, con una protección material y con una protección por recodificado local. Estas fases 320 y 322 son respectivamente idénticas a las fases 260 y 280 anteriormente descritas salvo que el criptograma KH''_k^{Kichip} o el criptograma KH'''_k^{Kichip} esté contenido en la licencia transmitida por el registrador y no haya sido recibido antes durante la fase de inicialización. Este modo de realización evita una desincronización entre el índice de las claves utilizadas por el registrador y el índice de las claves utilizadas por el lector. Por ejemplo, dicha desincronización puede aparecer si el lector estuviera apagado en el momento en que los criptogramas KH^{ki} le han sido transmitidos, es decir durante la fase de inicialización.

Numerosos otros modos de realización son posibles. Por ejemplo, los contenidos multimedia son intercambiados entre el registrador y un lector bien sea por lectura de flujo o por telecarga.

El contenido multimedia registrado puede ser telecargado a partir de la memoria de otro terminal que el terminal que la ha registrado. Por ejemplo, el lector 54 puede recibir y registrar localmente un contenido multimedia registrado inicialmente por el registrador 50 y particionar este contenido multimedia registrado con el lector 56.

En variante, la gestión de los índices k de clave puede ser omitida. En otra variante, un solo modo de protección es posible. El procedimiento es por consiguiente simplificado de forma consecuente.

En otra variante, la autorización o no de registrar un contenido multimedia se deduce de los títulos de acceso de los terminales. Por ejemplo, estos títulos de acceso son comparados con los derechos de acceso contenidos en los mensajes ECM recibidos para deducir la autorización y, alternativamente, la prohibición de registrar el contenido multimedia.

La palabra de control CW' puede ser generada por el procesador de seguridad y no por el agente de acceso condicional. Varias palabras de controles CW' pueden ser generadas para codificar los criptoperiodos respectivos del contenido multimedia registrado.

También es posible generar una incertidumbre indicada por CW'^{kb} y luego descifrar esta incertidumbre con una clave K_b para obtener la palabra de control CW'. Seguidamente, el coprocesador 94 cifra esta palabra de control CW' con su clave KH'''_k para obtener el criptograma $CW'^{KH'''k}$ que está integrado en la licencia. La clave K_b puede ser la clave K_{ichip} del procesador 80 u otra clave.

Las claves locales KH de un hogar pueden ser generadas por uno de los registradores de este hogar y luego transmitidas a la cabecera de red 6 que crea entonces los criptogramas KH'_k^{Kisoft}, KH''_k^{Kichip} y KH'''_k^{Kichip} antes de transmitirlos al lector. En variante, el registrador no genera las claves KH en su totalidad pero genera una información que es transmitida a la cabecera de red y luego la cabecera de red genera las claves KH a partir de esta información.

El codificado de los contenidos multimedia puede ser realizado de distinto modo. Por ejemplo, el codificado es realizado a otro nivel del nivel TS como se ha propuesto en la especificación Ismacryp. Los diferentes componentes del contenido multimedia, tales como el video y el audio, no son necesariamente codificados con la misma palabra de control.

Lo que ha sido descrito anteriormente, se aplica también en el caso en que los terminales de un mismo hogar estén repartidos en varios sitios distintos tales como la vivienda principal y la vivienda secundaria.

El registro de un contenido multimedia puede ser programado por el usuario.

Cuando un contenido multimedia es registrado con un modo de protección logicial, no es necesario que el lector esté provisto de un procesador de seguridad material, amovible o no. Es por ejemplo el caso del lector 54.

En variante, los terminales equipados con un procesador de seguridad material para la realización de la protección por recodificado local no tienen necesariamente necesidad de estar también equipado con una tarjeta de circuito impreso con chip. Por ejemplo, la tarjeta de circuito impreso con chip 102 del terminal 52 puede ser omitida. En este caso, los criptogramas CW_t^{Ks} son generados por la cabecera de red y directamente transmitidos al procesador 80 del terminal 52.

Cuando algunos parámetros, como el contenido del campo «Default-P» o «Life-T», son necesariamente idénticos para todos los terminales de un mismo hogar, estos pueden estar directamente asociados con el identificador House-Id en una tabla suplementaria. En este caso, los campos tales como «Default-P» y «Life-T» son omitidos de la tabla 36.

No es necesario que cuando un terminal tiene la autorización de registrar, tenga igualmente la autorización de leer un contenido multimedia registrado. Así, en otro modo de realización, además del campo «Record-A», la tabla 36 comprende un campo «Read-A» asociado con cada identificador STB-ID. Este campo «Read-A» contiene una autorización y, alternativamente, una prohibición de leer un contenido multimedia registrado. Un terminal puede leer un contenido multimedia únicamente si el contenido del campo «Read-A» asociado con su identificador STB-ID lo autoriza.

REIVINDICACIONES

1. Procedimiento de protección de un contenido multimedia registrado, en el cual:

- una cabecera de red transmite (162) un contenido multimedia codificado y mensajes ECM (Entitlement Control Message) conteniendo criptogramas CW^* de palabras de control CW que permiten cada una descodificar un criptoperiodo respectivo del contenido multimedia codificado,
- un registrador recibe el contenido multimedia codificado y los mensajes ECM, descifra (184) los criptogramas CW^* contenidos en los mensajes ECM recibidos con una clave de abonado K_a y protege (186) en lectura el contenido multimedia codificado con la ayuda de una clave local KH_k cifrando, con la clave local KH_k, las palabras de control descifradas para generar criptogramas CW^{KHk},
- el registrador registra (192) el contenido multimedia codificado y los criptogramas CW^{KHk},

en el cual el procedimiento comprende también:

- la provisión (152, 154) de una tabla que asocia con un identificador de hogar
  - el registrador, y
  - un grupo de M lectores distintos seleccionados entre un conjunto de N lectores aptos para descifrar, cuando han recibido la clave local KH_k, los criptogramas CW^{KHk}, y luego para descodificar el contenido multimedia registrado con las palabras de control CW así descifradas para leer el contenido multimedia en claro, donde M es un número entero superior o igual a dos y estrictamente inferior a N, y

- una etapa durante la cual la cabecera de red transmite la clave KH_k a los lectores que están asociados con el mismo identificador de hogar en la tabla y no transmite la clave KH_k a los lectores que no están asociados con este identificador de hogar en esta tabla,

caracterizado por que la etapa durante la cual la cabecera de red transmite la clave KH_k a los lectores se desarrolla en dos subetapas:

- una subetapa durante la cual la cabecera de red transmite (302) al registrador, para cada lector del grupo de M lectores, un criptograma KH_k^{Ki} obtenido cifrando la clave local KH_k con una clave K_i conocida solamente por el i-ésimo lector del grupo de M lectores entre el conjunto de los N lectores,

- una subetapa durante la cual, en respuesta a una demanda de lectura del contenido multimedia por el i-ésimo lector, el registrador transmite (314) a este lector el criptograma KH_k^{Ki}, y el i-ésimo lector descifra el criptograma KH_k^{Ki} con su clave K_i para obtener la clave local KH_k que permite descodificar el contenido multimedia registrado.

2. Procedimiento de protección de un contenido multimedia registrado, en el cual:

- una cabecera de red transmite (162) un contenido multimedia codificado y mensajes ECM (Entitlement Control Message) que contienen criptogramas CW^* de palabras de control CW que permiten cada una descodificar un criptoperiodo respectivo del contenido multimedia codificado,

- un registrador recibe el contenido multimedia codificado y los mensajes ECM, descifra (208) los criptogramas CW^* contenidos en los mensajes ECM recibidos con una clave de abonado K_a y protege (186) en lectura el contenido multimedia codificado con la ayuda de una clave local KH_k, descodificando (214) el contenido multimedia con las palabras de control descifradas y luego codificando (216) de nuevo el contenido multimedia con al menos una palabra de control CW' generando (200) un criptograma CW'^{KHk} correspondiente a la palabra de control CW' cifrada con la clave local KH_k,

- el registrador registra (218) el contenido multimedia codificado y el criptograma CW'^{KHk},

en el cual el procedimiento comprende también:

- la provisión (152, 154) de una tabla que asocia con un identificador de hogar:

  - el registrador, y

  - un grupo de M lectores distintos seleccionados entre un conjunto de N lectores aptos para descifrar, cuando han recibido la clave local KH_k, el criptograma CW'^{KHk}, y luego en descodificar el contenido multimedia registrado con la palabra de control CW' así descifrados para leer el contenido multimedia en claro, donde M es un número entero superior o igual a dos y estrictamente inferior a N, y

- una etapa durante la cual la cabecera de red transmite la clave KH_k a los lectores que están asociados con el mismo identificador de hogar en la tabla y no transmite la clave KH_k a los lectores que no están asociados con este identificador de hogar en esta tabla,

caracterizado por que la etapa durante la cual la cabecera de red transmite la clave KH_k a los lectores se desarrolla en dos subetapas:

● una subetapa durante la cual la cabecera de red transmite (302) al registrador, para cada lector del grupo de M lectores, un criptograma KH_k^{Ki} obtenido cifrando la clave local KH_k con una clave K_i conocida solamente por el i-ésimo lector del grupo de M lectores entre el conjunto de los N lectores,

● una subetapa durante la cual, en respuesta a una demanda de lectura del contenido multimedia por el i-ésimo lector, el registrador transmite (314) a este lector el criptograma KH_k^{Ki}, y el i-ésimo lector descifra el criptograma KH_k^{Ki} con su clave K_i para obtener la clave local KH_k que permite descodificar el contenido multimedia registrado.

3. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual el procedimiento comprende:

- el suministro (152, 154) de otra clave local $KH"_k$ a los solo lectores de un subgrupo de P lectores seleccionados entre el grupo de M lectores, siendo estos P lectores los únicos del grupo de M lectores de poner en práctica un modo de protección más robusto del contenido multimedia registrado, donde P es un número entero superior o igual a uno y estrictamente inferior a M,

- el registrador selecciona (186, 202) alternativamente, la clave local KH_k y la clave local $KH"_k$ en función de un indicador de modo de protección a utilizar y protege en lectura el contenido multimedia codificado únicamente con la ayuda de la clave local seleccionada.

4. Procedimiento según la reivindicación 3, en el cual el registrador recibe un mensaje ECM que contiene, además de los criptogramas CW^*, el indicador del modo de protección a aplicar durante el registro del contenido multimedia codificado con la ayuda de las palabras de control CW^* contenidas en este mensaje ECM.

5. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el cual en respuesta al aporte o a la supresión de un lector asociado con el identificador de hogar, la cabecera de red transmite una nueva clave local KH_{k+1} a los lectores que están asociados con este identificador de hogar en la tabla y no transmite esta nueva clave local KH_{k+1} a los lectores que no están asociados con este identificador de hogar en esta tabla.

6. Procedimiento según la reivindicación 5, en el cual:

- el registrador asocia (190) con cada contenido multimedia registrado un índice k de la clave local utilizada para proteger este contenido multimedia registrado,

- cada lector memoriza la clave local KH_k y KH_{k+1} asociada con su índice k respectivo, y

- el lector selecciona (240) la clave local entre las claves KH_k y KH_{k+1}, para eliminar la protección del contenido multimedia, en función del índice k de clave local asociado con este contenido multimedia registrado.

7. Procedimiento de transmisión de contenido multimedia para la puesta en práctica de un procedimiento de protección conforme a una cualquiera de las reivindicaciones anteriores, en el cual una cabecera de red:

- transmite (162) un contenido multimedia codificado y mensajes ECM (Entitlement Control Message) que contienen criptogramas CW^* de palabras de control CW que permiten cada una descodificar un criptoperiodo respectivo del contenido multimedia codificado,

- transmite la clave local KH_k a los lectores que están asociados con el mismo identificador de hogar en la tabla y no transmite la clave local KH_k a los lectores que no están asociados con este identificador de hogar en esta tabla,

caracterizado por que la etapa durante la cual la cabecera de red transmite la clave KH_k a los lectores comprende una subetapa durante la cual la cabecera de red transmite (302) al registrador, para cada lector del grupo de M lectores, un criptograma KH_k^{Ki} obtenido cifrando la clave local KH_k con una clave K_i conocida solamente del i-ésimo lector del grupo de M lectores entre el conjunto de los N lectores.

8. Procedimiento de registro de contenido multimedia transmitido según un procedimiento conforme a la reivindicación 7, en el cual:

- un registrador recibe el contenido multimedia codificado y los mensajes ECM, descifra (184) los criptogramas CW^* contenidos en los mensajes ECM recibidos con una clave de abonado K_a y protege en lectura el contenido multimedia codificado con la ayuda de una clave local KH_k,

- el registrador registra (192, 218) el contenido multimedia codificado protegido con la clave KH_k,

caracterizado por que:

- el registrador recibe (158) de la cabecera de red, para cada lector del grupo de M lectores, un criptograma KH_k^{Ki} obtenido cifrando la clave local KH_k con una clave K_i conocida solamente por el i-ésimo lector del grupo de M lectores entre el conjunto de los N lectores, y
- en respuesta a una demanda de lectura del contenido multimedia por el i-ésimo lector, el registrados transmite (314) a este lector el criptograma KH_k^{Ki}.

9. Procedimiento según la reivindicación 8, en el cual:

- el registrador lanza (200) de forma aleatoria o pseudo aleatoria al menos un criptograma CW'^{Kb}, luego

- un procesador de seguridad del registrador descifra (202) el criptograma CW'^{Kb} con una clave K_b para obtener la palabra de control CW' en claro, luego codifica (216) de nuevo el contenido multimedia, anteriormente descodificado, con la palabra de control así obtenida.

10. Procedimiento según una cualquiera de las reivindicaciones 8 a 9, en el cual el registrador inhibe sistemáticamente (176) y, alternativamente, permite el registro del contenido multimedia codificado en función de una autorización o de una prohibición de registro contenida en los mensajes ECM que contienen las palabras de control CW^* necesarias para descodificar este contenido multimedia.

11. Registrador y/o lector para la puesta en práctica de un procedimiento conforme a una cualquiera de las reivindicaciones anteriores, caracterizado por que este registrador y/o lector comprende:

- un ordenador electrónico programable, y

- un soporte de registro de informaciones que contienen instrucciones para la puesta en práctica de un procedimiento conforme a una cualquiera de las reivindicaciones anteriores cuando estas instrucciones son ejecutadas por el ordenador electrónico.

12. Cabecera de red para la realización de un procedimiento conforme a una cualquiera de las reivindicaciones 1 a 7, comprendiendo esta cabecera de red un sistema (28) de acceso condicional, caracterizado por que el sistema (28) de acceso condicional comprende:

- un ordenador electrónico programable, y

- un soporte de registro de informaciones que contienen instrucciones para la realización de un procedimiento conforme a una cualquiera de las reivindicaciones 1 a 7 cuando estas instrucciones son ejecutadas por el ordenador electrónico, y

- la tabla (36) que asocia con un identificador de hogar

  ● el registrador, y

  ● un grupo de M lectores distintos seleccionados entre un conjunto de N lectores aptos para descifrar, cuando han recibido la clave local KH_k, los criptogramas CW^{KHk} o el criptograma CW'^{KHk} luego en descodificar el contenido multimedia registrado con las palabras de control CW o la palabra de control CW' así descifradas para leer el contenido multimedia en claro, donde M es un número entero superior o igual a dos y estrictamente inferior a N.

13. Soporte de registro de informaciones, caracterizado por que comprende instrucciones para la realización de un procedimiento conforme a una cualquiera de las reivindicaciones 1 a 10, cuando estas instrucciones son ejecutadas por un ordenador electrónico.

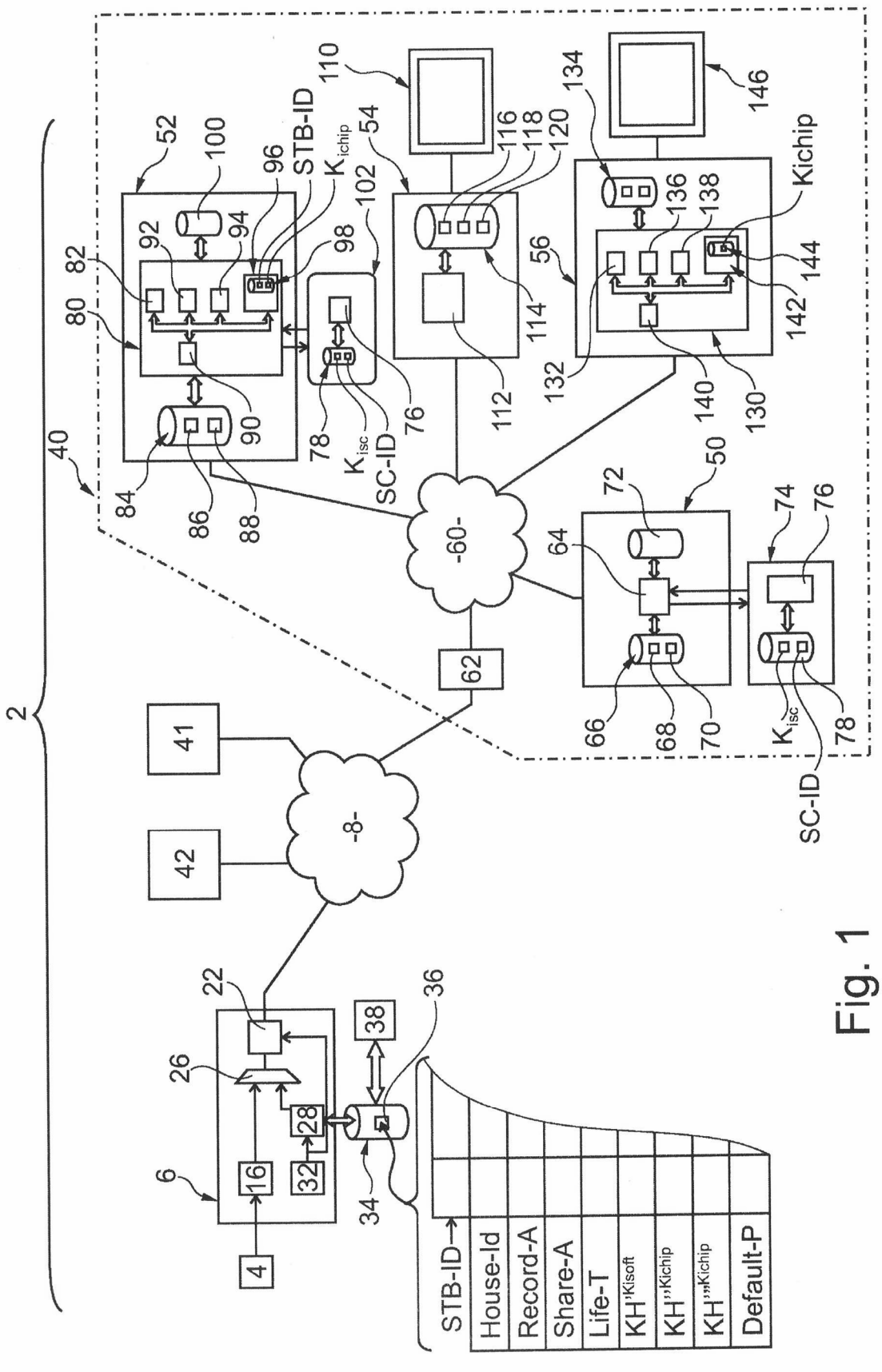
2
40
41
42
-8-
-60-
62
50
72
64
66
68
70
74
76
78
SC-ID
K_{isc}
52
100
96
STB-ID
K_{ichip}
54
110
116
118
120
134
146
Kichip
92
94
98
102
82
80
90
84
86
88
78
K_{isc}
SC-ID
76
112
114
56
136
138
144
142
132
140
130
22
26
28
32
38
36
34
6
4
16
STB-ID
House-Id
Record-A
Share-A
Life-T
$KH^{'Kisoft}$
$KH^{''Kichip}$
$KH^{'''Kichip}$
Default-P

Fig. 1

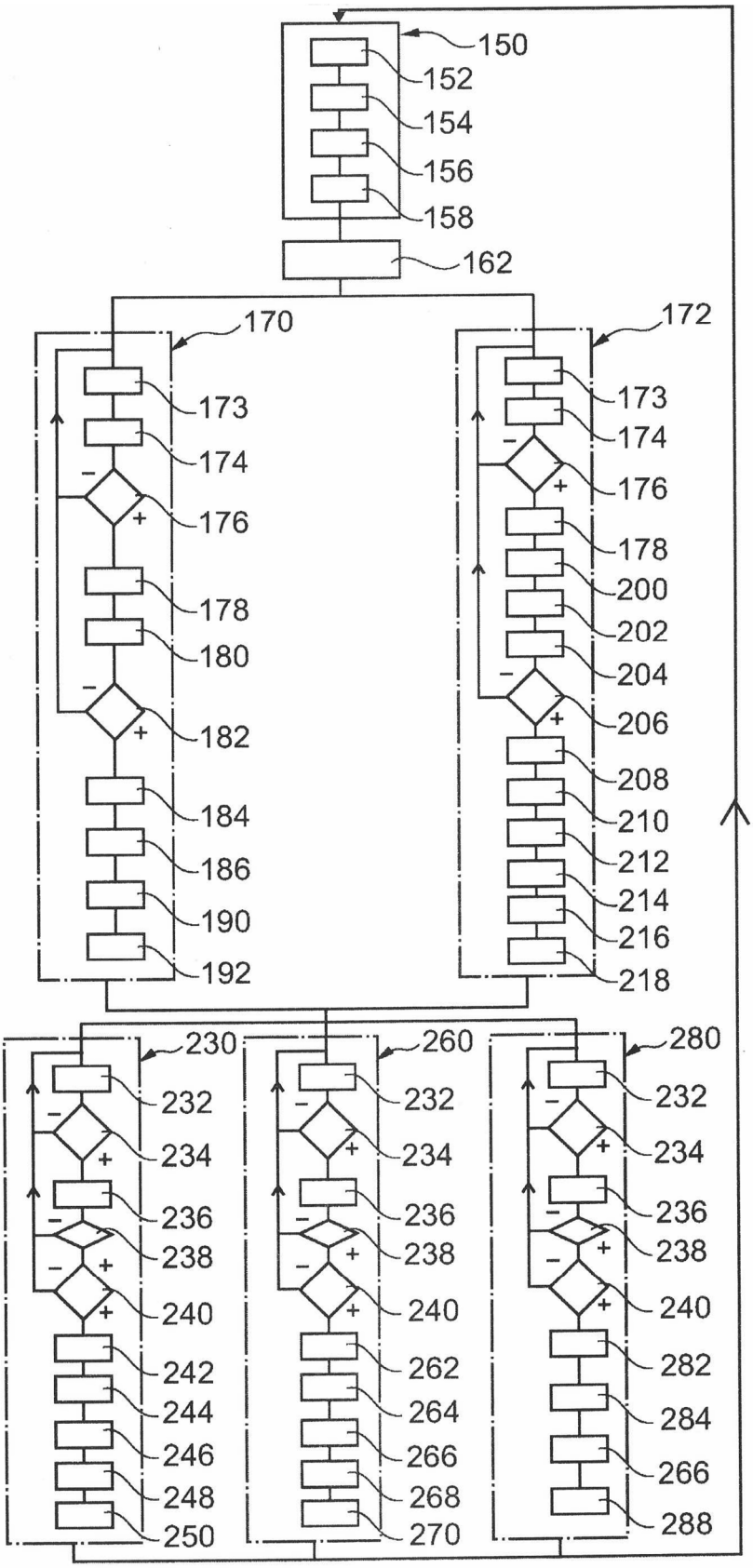
150
152
154
156
158
162
170
172
173
174
176
178
180
182
184
186
190
192
173
174
176
178
200
202
204
206
208
210
212
214
216
218
230
260
280
232
234
236
238
240
242
244
246
248
250
232
234
236
238
240
262
264
266
268
270
232
234
236
238
240
282
284
266
288

Fig. 2

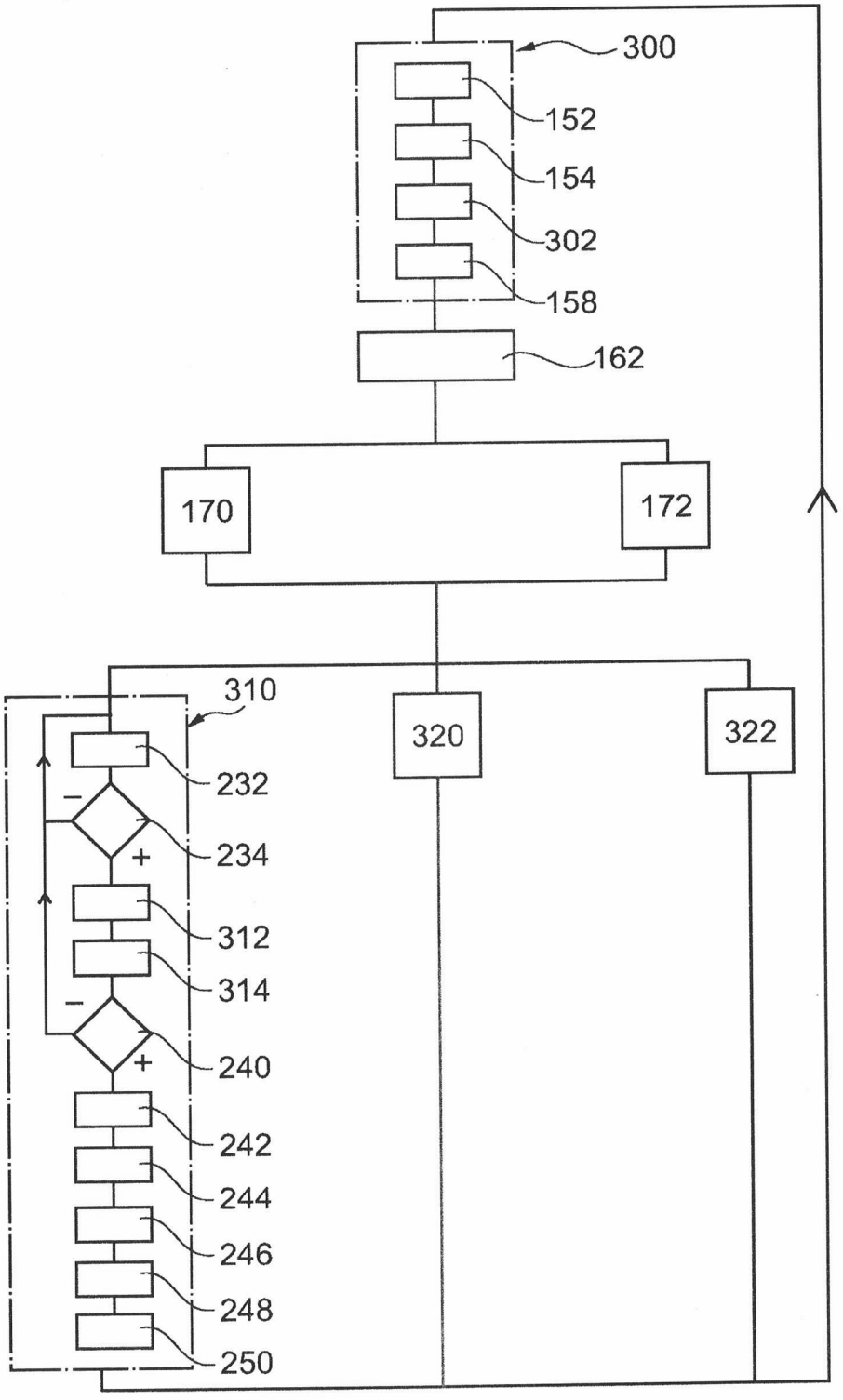
300
152
154
302
158
162
170
172
310
320
322
232
234
312
314
240
242
244
246
248
250
–
+
–
+

Fig. 3